

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

---

In re: The Home Depot, Inc., Customer  
Data Security Breach Litigation

This document relates to:

CONSUMER CASES

---

)  
)  
)  
)  
)  
)  
)

Case No.: 1:14-md-02583-TWT

**CONSUMER PLAINTIFFS' CONSOLIDATED  
CLASS ACTION COMPLAINT**

Plaintiffs identified below (collectively “Consumer Plaintiffs”), individually and on behalf of the Classes defined below of similarly situated persons, allege the following against Home Depot U.S.A., Inc. and The Home Depot, Inc. (collectively “Home Depot” or “Defendants”) based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

**NATURE OF THE CASE**

1. Between approximately April 1, 2014 and September 18, 2014, Home Depot was subject to one of the largest retailer data breaches in U.S. history, when hackers acquired the personal and financial information of up to 56 million Home Depot customers located in every state in the nation (the “Home Depot breach” or

“Home Depot data breach”). Home Depot management’s attitude towards data security in the years and months leading up to the breach can best be described as willfully dismissive. Notwithstanding the warnings and pleas of many of its employees who recognized the vulnerability of millions of customers’ sensitive information stored in Home Depot’s systems, Home Depot management refused to upgrade its security systems, refused to follow recommendations of information technology (“IT”) employees and experts, and suffered from ineffective leadership in key IT security positions within the organization. Home Depot customers across the United States have suffered real and imminent harm as a direct consequence of Home Depot’s conduct, which includes (a) refusing to take adequate and reasonable measures to ensure its data systems were protected; (b) refusing to take available steps to prevent the breach from happening; (c) failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers’ personal and financial information; and (d) failing to provide timely and adequate notice of the Home Depot data breach.

2. As a result of the Home Depot data breach, the payment card data and personal information of 56 million Home Depot customers has been exposed to criminals for misuse. Remarkably, Home Depot would not have even discovered the breach when it did except for an Internet blog post by a data security watchdog that reported massive batches of Home Depot customers’ payment cards were

offered for sale on online black markets to be purchased by criminals across the globe. The injuries suffered by Consumer Plaintiffs and the proposed Classes as a direct result of the Home Depot data breach include:

- a. unauthorized charges on their debit and credit card accounts;
- b. theft of their personal and financial information;
- c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- d. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;
- e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Home Depot data breach;
- f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their payment card and personal information being placed in the hands of criminals and already misused via the sale of Consumer Plaintiffs' and Class members' information on the Internet black market;
- g. damages to and diminution in value of their personal and financial information entrusted to Home Depot for the sole purpose of purchasing products and services from Home Depot and with the mutual understanding that Home Depot would safeguard

Consumer Plaintiffs' and Class members' data against theft and not allow access to and misuse of their information by others;

- h. money paid for products and services purchased at Home Depot stores during the period of the Home Depot data breach in that Consumer Plaintiffs and Class members would not have shopped at Home Depot had Home Depot disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information and had Home Depot provided timely and accurate notice of the Home Depot data breach;
- i. continued risk to their financial and personal information, which remains in the possession of Home Depot and which is subject to further breaches so long as Home Depot fails to undertake appropriate and adequate measures to protect Consumer Plaintiffs' and Class members' data in its possession.

3. Examples of these harms caused to Home Depot customers as a direct and foreseeable consequence of Home Depot's conduct include the experiences of the following representative Consumer Plaintiffs, as well as the experiences of the other representative Consumer Plaintiffs in this Complaint:

4. Plaintiff Bruce Holdridge is a resident of Cave Creek, Arizona and was an Arizona resident during the period of the Home Depot breach. Plaintiff Holdridge shopped at a Home Depot retail store in Arizona between April 1 and September 18, 2014 by swiping his Home Depot credit card through Home Depot point-of-sale devices to make payment. Plaintiff Holdridge learned of the Home Depot breach on or about September 15, 2014 when, after seeing media coverage, he called Home Depot and discovered fraudulent charges for approximately \$8,500 reflected on his Home Depot credit card account. Plaintiff Holdridge then opened a

fraud investigation with Home Depot and closed his credit card account. Home Depot's fraud investigation took approximately three months to conclude. Since experiencing those fraudulent charges, Plaintiff Holdridge has received approximately 65 letters from the three credit bureaus showing repeated fraudulent attempts to use his name and credit history to open credit lines. Due to identity thieves submitting fraudulent credit applications in his name, Plaintiff Holdridge also has spent considerable time responding to numerous calls from would-be lenders seeking validation of his identity. In addition, since on or about September 16, 2014, Plaintiff Holdridge regularly receives phishing scam calls attempting to trick him into providing additional personal and financial information. Plaintiff Holdridge filed a report regarding the identity theft with the Phoenix, Arizona police department and paid to have a seven-year freeze placed on his credit reports with all three credit bureaus (requiring that he provide a police report) in an effort to prevent or mitigate additional identity theft activity. As a result of the Home Depot breach, Plaintiff Holdridge has spent over 320 hours trying to resolve these ongoing identity theft and financial problems.

5. Plaintiff Nathaniel Newton is a resident of Indio, California and was a California resident during the period of the Home Depot data breach. Plaintiff Newton shopped at a Home Depot retail store in California between April 1 and September 18, 2014 by swiping his debit or credit cards through Home Depot

point-of-sale devices to make payment. Since the commencement of the Home Depot breach, Plaintiff Newton has been the target of numerous instances of identity theft and fraud. With the information obtained from Home Depot, criminals used Plaintiff Newton's identity to fraudulently seek lines of credit from numerous financial institutions in Spokane, Washington. Plaintiff Newton also received a call from a telephone service provider that eight new telephone lines were opened under his name in Chattanooga, Tennessee. Plaintiff Newton's identity was also fraudulently used to open a \$10,000 line of credit at a motorcycle shop in Cleveland, Tennessee. Those acts of identity theft caused Plaintiff Newton's credit score to be lowered and he was consequently denied refinancing on the mortgage of his house. Plaintiff Newton now pays approximately \$40 per month for credit monitoring and identity theft protection in an effort to prevent or mitigate further harm to his credit and finances. On or about November 6, 2014, Plaintiff Newton received an e-mail notification from Home Depot regarding the breach. As a result of the Home Depot data breach, Plaintiff Newton expended approximately 40 hours, and continues to expend significant time, addressing issues arising from the breach and monitoring for fraud.

6. Plaintiff Ronald Castleberry, a retired law enforcement official, is a resident of Tallahassee, Florida and was a Florida resident during the period of the Home Depot data breach. Plaintiff Castleberry shopped at a Home Depot retail

store in Florida between April 1 and September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. On or about October 18, 2014, Plaintiff Castleberry's credit card was declined while he was attempting to make a purchase. Plaintiff Castleberry's financial institution had placed a security hold on his credit card account after fraudulent purchases on an international travel website totaling approximately \$1,800 were identified on his account. Due to the Home Depot data breach, Plaintiff Castleberry lost access to his line of credit for several weeks. In addition, throughout the first three months of 2015, Plaintiff Castleberry was targeted by identity thieves who made several attempts to open fraudulent lines of credit, financial assistance accounts, and bank accounts in Plaintiff Castleberry's name. As a result of the Home Depot data breach, Plaintiff Castleberry spent approximately 30 hours addressing issues arising from the breach and monitoring his credit card and other accounts for fraud. Plaintiff Castleberry never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

7. Plaintiffs Martha and Brandyon Brantley are a married couple residing in Dallas, Georgia and were Georgia residents during the period of the Home Depot breach. Mr. Brantley shopped at a Home Depot retail store in Georgia between April 1 and September 18, 2014 by swiping his debit card through Home Depot point-of-sale devices to make payment through the Brantleys' joint debit

card account. On or about September 19, 2014, Mrs. Brantley received an electronic communication from her bank indicating their debit account had been overdrawn and had a negative balance. Mrs. Brantley immediately reviewed their debit account activity and discovered fraudulent charges totaling more than \$500. Although the bank eventually reimbursed the Brantleys for these stolen funds, the process took approximately one week. As a result, the Brantleys were compelled to borrow money to pay bills while their debit card was frozen. The Brantleys' bank is a small financial institution with limited hours of operation, making it difficult for them to travel there in person to fill out paperwork and obtain cash. As a result of the Home Depot data breach, Mrs. Brantley has spent approximately 10 hours addressing issues arising from the breach. The Brantleys never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

8. Plaintiffs Luis and Kitaisha Araujo are a married couple residing in Lansing, Kansas and were Kansas residents during the period of the Home Depot data breach. Mr. Araujo shopped at a Home Depot retail store in Kansas between April 1 and September 18, 2014 by swiping his debit card through Home Depot point-of-sale devices to make payment. In September 2014, the Araujos identified \$1,144.54 in fraudulent charges on their debit account statement, which caused their debt account to be overdrawn and to incur \$150 in overdraft fees. Mr. and



Mrs. Araujo experienced significant inconveniences over a nearly two-week period while they waited for Mr. Araujo's replacement card to be issued. Although the fraudulent charges and overdraft fees were ultimately reimbursed to the Araujos' debit account, they were without access to their funds for a period of time and had to borrow money just to get by and provide for their children. The bank imposed a temporary spending limit of \$300 per transaction without notifying Mr. and Mrs. Araujo, which resulted in Mrs. Araujo's card being declined at the grocery store. Mr. and Mrs. Araujo had to juggle one card between the two of them and Mr. Araujo had to skip lunch on a couple of occasions because he did not have cash or access to their debit funds. On or about November 9, 2014, Mr. Araujo received an e-mail notification from Home Depot regarding the breach. Mr. and Mrs. Araujo incurred unreimbursed late and/or declined payment fees as a result of failed automatic bill payments tied to their debit account. They also spent approximately seven hours dealing directly with their bank and approximately eight additional hours on other matters arising from the Home Depot breach.

9. Plaintiff Paula Ridenti is a resident of Somerville, Massachusetts and was a Massachusetts resident during the period of the Home Depot breach. Plaintiff Ridenti shopped at a Home Depot retail store in Massachusetts between April 1 and September 18, 2014 by swiping her credit card through Home Depot point-of-sale devices to make payment. Plaintiff Ridenti learned of the Home

Depot breach on or about October 30, 2014, when she received a letter from her financial institution indicating fraudulent activity on her account. When Plaintiff Ridenti contacted the financial institution, she was informed the fraudulent activity—a \$480.93 charge at a wholesale store on October 29, 2014—was related to the Home Depot breach. She was further informed that a male individual used a fake credit card with her account number to make the fraudulent purchase. Plaintiff Ridenti's line of credit was frozen and not reinstated until reversal of the fraudulent charges on or about December 11, 2014. Plaintiff Ridenti was subsequently denied credit as a result of this fraudulent activity on her credit report. She has since paid the credit bureaus to place a freeze on her credit report to, among other things, limit or mitigate further damage to her ability to obtain credit. Plaintiff Ridenti incurred unreimbursed expenses and spent over 30 hours addressing issues arising from the Home Depot breach related to her finances and credit.

10. Plaintiff Catherine Adams, a widow who served as a 12-year U.S. Army veteran staff sergeant, now a retired receptionist and volunteer Sunday school teacher living on a fixed income, is a resident of Charlotte, North Carolina and was a North Carolina resident during the period of the Home Depot breach. Plaintiff Adams shopped at a Home Depot retail store in North Carolina between April 1 and September 18, 2014 by swiping her debit card through Home Depot point-of-sale devices to make payment. On or about January 31, 2015, Plaintiff

Adams went on a trip to Winston-Salem to visit her aunt in hospice care. On her drive home, she attempted to purchase gas and her debit card was declined. She was stranded without access to her funds to purchase the fuel she needed, and had to borrow money from strangers to make it home. Plaintiff Adams later called her bank, which informed her that a new debit card had been issued because of the Home Depot data breach. She soon discovered that someone had fraudulently used her debit account information to charge \$337.89 at a grocery store in Orlando, Florida. When she went to Home Depot to report the fraud, Home Depot denied any issue and said it was only an issue with her bank. Plaintiff Adams subsequently received alerts from the three major credit bureaus that six fraudulent credit applications were made in her name, and showed up on her credit reports, including a fraudulent application made at a Lexus car dealership. Further, as a result of the freeze on her bank account that prevented timely automatic payment, Plaintiff Adams' auto insurance provider informed her that her policy would be cancelled for nonpayment of premium "at 12:01 a.m." the same night, and that she had to take immediate action to prevent cancellation. Because her account was frozen, Plaintiff Adams had to borrow money to pay her auto insurance premium. Also, delivery of Plaintiff Adams' blood pressure medication was delayed by approximately one week because her account was frozen and other automatic bill payments were rejected. As a result of the Home Depot breach, Plaintiff Adams

spent over 50 hours addressing issues arising from the breach and checking her account for additional fraud. Plaintiff Adams never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

11. Plaintiff John Simon is a resident of Whitewright, Texas and was a Texas resident during the period of the Home Depot breach. Plaintiff Simon shopped at a Home Depot retail store in Texas between April 1 and September 18, 2014 by swiping his debit card through Home Depot point-of-sale devices to make payment. On or about September 23, 2014, Plaintiff Simon received an e-mail notification from Home Depot regarding the breach. On or about September 25, 2014, Plaintiff Simon received a call from his credit union's fraud department and learned that over \$2,000 was fraudulently charged to his debit card account. The stolen funds were not reimbursed to Plaintiff Simon's account until October 7, 2014. Plaintiff Simon lost access to the balance of the stolen funds during the credit union's fraud investigation. Plaintiff Simon also had to cancel a business meeting in order to visit his credit union and fill out paperwork related to the fraud investigation. As a result of the Home Depot breach, Plaintiff Simon purchased credit monitoring and identity theft prevention and paid approximately \$10 per month for several months after the breach, which was not reimbursed. Plaintiff

Simon incurred unreimbursed expenses and spent over 20 hours addressing issues arising from the Home Depot breach.

12. Consumer Plaintiffs retain a significant interest in ensuring that their information is protected from further breaches, and seek to remedy the harms they have suffered on behalf of themselves and similarly situated consumers whose personal and financial information was stolen as a result of the Home Depot data breach. Consumer Plaintiffs assert claims against Home Depot for violations of state consumer protection statutes, state data breach statutes, negligence, breach of implied contract and unjust enrichment, and seek a declaratory judgment as to Home Depot's deficient data security practices. Consumer Plaintiffs, on behalf of themselves and similarly situated consumers, seek to recover damages, including actual and statutory damages, and equitable relief, including injunctive relief to prevent a recurrence of the data breach and resulting injury, restitution, disgorgement and reasonable costs and attorneys' fees.

### **JURISDICTION AND VENUE**

13. This Consolidated Complaint is intended to serve as a superseding complaint as to all other complaints that have been consolidated in this multi-district litigation. As set forth herein, this Court has general jurisdiction over Home Depot and original jurisdiction over Consumer Plaintiffs' claims.

14. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million exclusive of interest and costs. At least one Consumer Plaintiff and Defendant are citizens of different states. There are more than 100 putative class members.

15. This Court has personal jurisdiction over Defendants because they maintain their principal place of business in Georgia, regularly conduct business in Georgia, and have sufficient minimum contacts in Georgia. Defendants intentionally avail themselves of this jurisdiction by marketing and selling products and services from Georgia to millions of consumers nationwide.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a) because Defendants' principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Consumer Plaintiffs' claims occurred in this District.

### **PARTIES**

17. Consumer Plaintiffs reallege the parties set forth in paragraphs 4-11, as if set forth fully herein.

18. Plaintiff Danny Champion is a resident of Prattville, Alabama and was an Alabama resident during the period of the Home Depot breach. Plaintiff Champion shopped at a Home Depot retail store in Alabama between April 1 and

September 18, 2014 by swiping his debit card through Home Depot point-of-sale devices to make payment. Plaintiff Champion spent about five hours addressing issues arising from the Home Depot breach. Plaintiff Champion never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

19. Plaintiff Kim Barrett is a resident of Anchorage, Alaska and was an Alaska resident during the period of the Home Depot breach. Plaintiff Barrett shopped at a Home Depot retail store in Alaska between April 1 and September 18, 2014 by swiping her credit card through Home Depot point-of-sale devices to make payment. Plaintiff Barrett spent about two hours addressing issues arising from the Home Depot breach. Plaintiff never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

20. Plaintiff Michael Snow is a resident of Little Rock, Arkansas and was an Arkansas resident during the period of the Home Depot breach. Plaintiff Snow shopped at a Home Depot retail store in Arkansas between April 1 and September 18, 2014 by swiping his debit card through Home Depot point-of-sale devices to make payment. Subsequent to using his debit card at a Home Depot store to make transactions reference above, on or about June 6, 2014, Plaintiff Snow reviewed his bank statement and discovered an unauthorized charge. Ultimately he learned that

a criminal in Florida made a fraudulent purchase on June 2, 2014 for approximately \$75 using his debit card information. After experiencing these fraudulent charges, Plaintiff Snow lost access to his funds for approximately three days and had to borrow money from family members. As a result of the Home Depot breach, Plaintiff Snow spent 30 to 35 hours attempting to resolve his finances and checking for additional fraudulent charges. Plaintiff Snow never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

21. Plaintiff Shonna Earls is a resident of Richmond, California and was a California resident during the period of the Home Depot breach. Plaintiff Earls shopped at a Home Depot retail store in California between April 1 and September 18, 2014 by swiping her credit card through Home Depot point-of-sale devices to make payment. Plaintiff Earls learned of the Home Depot breach on or about September 5, 2014 when her financial institution called to inform her of fraudulent charges on her credit card totaling approximately \$540. Due to these fraudulent charges, Plaintiff Earls' credit account was closed and she lost access to her line of credit for approximately one week until she received her replacement card. As a result of the Home Depot breach, Plaintiff Earls spent over eight hours attempting to resolve her finances. Plaintiff Earls now pays approximately \$9 per month for credit card monitoring services in an effort to prevent or mitigate additional



identity theft activity. Plaintiff Earls never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

22. Plaintiff Glenda Fuller is a resident of Gardena, California and was a California resident during the period of the Home Depot breach. Plaintiff Fuller shopped at a Home Depot retail store in California between April 1 and September 18, 2014 by swiping her debit and credit cards through Home Depot point-of-sale devices to make payment. Subsequent to her referenced Home Depot transactions, criminals used Plaintiff Fuller's debit card information to make eight fraudulent purchases; on September 12, 2014, fraudulent purchases were made in the amounts of \$76.00 and \$24.50. Three days later, five fraudulent purchases were made totaling \$320.35. On September 16, an additional fraudulent purchase was made in the amount of \$101.82. Although her bank eventually reimbursed her for these fraudulent charges, reimbursement took approximately one month. Plaintiff Fuller was assessed late and/or declined payment fees totaling \$130 as a result of failed automatic bill payments tied to her debit account. As a result of the Home Depot breach, Plaintiff Fuller spent approximately 20 to 25 hours resolving her finances. Plaintiff Fuller never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

23. Plaintiff Jasmin Gonzalez is a resident of Long Beach, California and was a California resident during the period of the Home Depot breach. Plaintiff Gonzalez shopped at a Home Depot retail store in California between April 1 and September 18, 2014 by swiping her debit and credit cards through Home Depot point-of-sale devices to make payment. In or around September or October 2014, Plaintiff Gonzalez received a letter from her bank indicating that her debit card was compromised in the Home Depot breach. Plaintiff Gonzalez spent over two hours addressing issues arising from the Home Depot breach. Plaintiff Gonzalez never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

24. Plaintiff Edda Hernandez is a resident of Chula Vista, California and was a California resident during the period of the Home Depot breach. Plaintiff Hernandez shopped at a Home Depot retail store in California between April 1 and September 18, 2014 by swiping her debit and credit cards through Home Depot point-of-sale devices to make payment. Subsequent to her referenced Home Depot transactions, in September 2014 Plaintiff Hernandez received an automated call from her credit union seeking confirmation of several purchases that she did not make. After a live credit union representative joined the call, Plaintiff Hernandez confirmed that the charges, totaling approximately \$200, were fraudulent and the representative informed her that the fraudulent use of her debit card information

was related to the Home Depot breach. Although Plaintiff Hernandez was reimbursed for these fraudulent charges, reimbursement took approximately seven to 10 business days, during which time she had to borrow money from her family. As a result of the Home Depot breach, Plaintiff Hernandez has spent approximately five to seven hours attempting to resolve her finances and monitoring her accounts for fraud. Plaintiff Hernandez never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

25. Plaintiff John Holt, Sr. is a resident of Chowchilla, California and was a California resident during the period of the Home Depot breach. Plaintiff Holt shopped at a Home Depot retail store in California between April 1 and September 18, 2014 by swiping his debit card through Home Depot point-of-sale devices to make payment. In or around November 2014, the fraud department at Plaintiff Holt's credit union contacted him regarding potential fraudulent activity on his account and that it needed to replace his debit card. Plaintiff Holt spent approximately three hours addressing issues arising from the Home Depot breach and monitoring his accounts for fraud. Plaintiff Holt never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

26. Plaintiff Walid Khalaf is a resident of San Diego, California and was a California resident during the period of the Home Depot breach. Plaintiff Khalaf shopped at a Home Depot retail store in California between April 1 and September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. Plaintiff Khalaf spent approximately 10 hours addressing issues arising from the Home Depot breach. Plaintiff Khalaf never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

27. Plaintiff Julian Metter is a resident of Los Angeles, California and was a California resident during the period of the Home Depot breach. Plaintiff Metter shopped at a Home Depot retail store in California between April 1 and September 18, 2014 by swiping his debit card through Home Depot point-of-sale devices to make payment. Subsequent to his referenced Home Depot transactions, on or about September 11, 2014, over \$280 in fraudulent charges appeared on Plaintiff Metter's debit account. Plaintiff Metter informed his financial institution of the fraudulent charges, but ultimately the financial institution refused to reimburse the stolen funds to his debit account. Thereafter, Plaintiff Metter withdrew his remaining funds from that debit account and began banking with a different financial institution. As a result of the Home Depot breach, Plaintiff Metter spent approximately 24 hours attempting to resolve his finances. Plaintiff Metter never

received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

28. Plaintiff Joseph Moran is a resident of Oceanside, California and was a California resident during the period of the Home Depot breach. Plaintiff Moran shopped at a Home Depot retail store in California between April 1 and September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. Subsequent to his referenced Home Depot transactions, in or around August of 2014, suspicious international charges appeared on his credit card account, and unbeknownst to Plaintiff Moran caused his credit union to place a security hold on his account. When Plaintiff Moran attempted to use his credit card to pay for \$1,500 worth of car repairs, it was declined. Plaintiff Moran was unable to pay for repairs on his car and therefore unable to get his car back from the repair shop because without a replacement card, he did not have access to his line of credit. Plaintiff Moran eventually paid for the repairs using alternative funding sources, but was unable to reap the benefits of the substantial reward points associated with his compromised credit card. As a result of the Home Depot breach, Plaintiff Moran spent approximately 15 hours attempting to resolve his finances. Plaintiff Moran never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

29. Plaintiff Steve O'Brien ("S. O'Brien") is a resident of San Diego, California and was a California resident during the period of the Home Depot breach. Plaintiff S. O'Brien shopped at a Home Depot retail store in California between April 1 and September 18, 2014 by swiping his debit card through Home Depot point-of-sale devices to make payment. Plaintiff S. O'Brien spent approximately six hours addressing issues arising from the Home Depot breach and monitoring his account for fraud. Plaintiff S. O'Brien never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

30. Plaintiff Joshua Michener is a resident of Castle Rock, Colorado and was a Colorado resident during the period of the Home Depot breach. Plaintiff Michener shopped at Home Depot retail stores in Colorado between April 1 and September 18, 2014 by swiping his debit and credit cards through Home Depot point-of-sale devices to make payment. On or about September 23, 2014, Plaintiff Michener received an e-mail notification from Home Depot regarding the breach. On or about December 3, 2014, fraudulent charges appeared on Plaintiff Michener's debit account totaling approximately \$275, which caused funds from his savings account to automatically transfer to his checking/debit account to cover the charges. Although his bank ultimately reimbursed him for these fraudulent charges, Plaintiff Michener's debit account was not reimbursed for approximately

seven days and he temporarily lost access to those funds. As a result of the Home Depot breach, Plaintiff Michener spent at least 70 hours attempting to resolve his finances and monitoring his accounts for fraudulent activity.

31. Plaintiff Bridgette Moody is a resident of Thornton, Colorado and was a Colorado resident during the period of the Home Depot breach. Plaintiff Moody shopped at a Home Depot retail store in Colorado between April 1 and September 18, 2014 by swiping her debit card through Home Depot point-of-sale devices to make payment. On or about September 30, 2014, Plaintiff Moody received an e-mail from her credit union, which indicated her debit card was compromised in the Home Depot breach. Plaintiff Moody was assessed late and/or declined payment fees as a result of failed automatic bill payments tied to her debit card. On or about October 30, 2014, an unauthorized person hacked into Plaintiff Moody's e-mail account. As a result of the Home Depot breach compromising her debit card and e-mail account, Plaintiff Moody now pays approximately \$30 per month for credit monitoring and identity theft prevention and approximately \$15 per month for e-mail monitoring. Plaintiff Moody spent over 70 hours, not including her daily monitoring of accounts, addressing issues arising from the Home Depot breach. Plaintiff Moody never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

32. Plaintiff Raina Rothbaum is a resident of Westminster, Colorado and was a Colorado resident during the period of the Home Depot breach. Plaintiff Rothbaum shopped at Home Depot retail stores in Colorado between April 1 and September 18, 2014 by swiping her debit card through Home Depot point-of-sale devices to make payment. Plaintiff Rothbaum learned of the Home Depot breach on or about October 5, 2014 when she received a text alert from her bank regarding a fraudulent purchase on her debit card of \$407.13 at a Home Depot retail store in Colorado. Plaintiff Rothbaum contacted Home Depot to confirm that the charge was fraudulent, but she was given another number to call that provided general information regarding the breach. Even though her bank eventually reimbursed her for the fraudulent charge, Plaintiff Rothbaum had to transfer funds from her savings and make trips to the bank for cash while waiting for a replacement debit card. Plaintiff Rothbaum spent approximately 10 to 12 hours addressing issues arising from the Home Depot breach. Plaintiff Rothbaum never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

33. Plaintiff Stephen Sadler is a resident of Parker, Colorado and was a Colorado resident during the period of the Home Depot breach. Plaintiff Sadler shopped at a Home Depot retail store in Colorado between April 1 and September 18, 2014 by swiping his debit card through Home Depot point-of-sale devices to



make payment. Subsequent to his referenced Home Depot transactions, a criminal attempted to make fraudulent international charges on Plaintiff Sadler's debit account, but his bank flagged and stopped the charges before they went through. After his debit card was deactivated and a replacement card was issued, Plaintiff Sadler lost access to his funds for approximately three days. Plaintiff Sadler spent approximately five hours addressing issues arising from the Home Depot breach. Plaintiff Sadler never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

34. Plaintiff Brion Reilly is a resident of Wilmington, Delaware and was a Delaware resident during the period of the Home Depot breach. Plaintiff Reilly shopped at a Home Depot retail store in Delaware between April 1 and September 18, 2014 by swiping his debit card through Home Depot point-of-sale devices to make payment. On or about November 9, 2014, Plaintiff Reilly received an e-mail notification from Home Depot regarding the breach. As a result of the Home Depot breach, Plaintiff Reilly has expended and continues to expend time monitoring his debit account for fraud.

35. Plaintiff Charles Chorman is a resident of Fleming Island, Florida and was a Florida resident during the period of the Home Depot breach. Plaintiff Chorman shopped at a Home Depot retail store in Florida between April 1 and September 18, 2014 by swiping his debit card through Home Depot point-of-sale

devices to make payment. Subsequent to his referenced Home Depot transactions, on or about September 5, 2014, Plaintiff Chorman received an e-mail from his credit union alerting him to suspicious ATM withdrawals and other purchases on his debit account totaling approximately \$1,800. After contacting his credit union and confirming the suspicious transactions were fraudulent, the credit union cancelled Plaintiff Chorman's debit card. Plaintiff Chorman waited approximately one week to receive his replacement card. Plaintiff Chorman had to transfer funds from his savings account to cover the stolen funds, although the credit union eventually reimbursed him for the fraudulent charges. Plaintiff Chorman spent over 10 hours addressing issues arising from the Home Depot breach, including time spent reporting the identity theft to law enforcement. Plaintiff Chorman never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

36. Plaintiff Gary Gilchrist is a resident of Palm Harbor, Florida and was a Florida resident during the period of the Home Depot breach. Plaintiff Gilchrist shopped at a Home Depot retail store in Florida between April 1 and September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. Subsequent to his referenced Home Depot transactions, on or about July 24, 2014, Plaintiff Gilchrist discovered a fraudulent charge for \$125 when reviewing his credit card statement. Plaintiff Gilchrist expended time to contact his

financial institution to investigate and reverse the fraudulent charge. Plaintiff Gilchrist never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

37. Plaintiff Pamela Lee is a resident of West Palm Beach, Florida and was a Florida resident during the period of the Home Depot breach. Plaintiff Lee shopped at a Home Depot retail store in Florida between April 1 and September 18, 2014 by swiping her debit cards through Home Depot point-of-sale devices to make payment. On or about September 18, 2014, Plaintiff Lee's credit union sent her an e-mail notification that one of her debit cards was compromised in the Home Depot breach. Due to the change in her debit account, Plaintiff Lee was assessed late and/or declined payment fees as a result of failed automatic bill payments tied to her debit cards. Plaintiff Lee spent over 20 hours addressing issues arising from the Home Depot breach and monitoring for fraud. Plaintiff Lee never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

38. Plaintiff Sandra McQuiag is a resident of Lake City, Florida and was a Florida resident during the period of the Home Depot breach. Plaintiff McQuiag shopped at a Home Depot retail store in Florida between April 1 and September 18, 2014 by swiping her debit card through Home Depot point-of-sale devices to make payment. Subsequent to her referenced Home Depot transactions, on or

about September 9, 2014, Plaintiff McQuiag received a call from her credit monitoring agency indicating her debit card was fraudulently charged and that, as a result, her debit account was frozen. In order to have the bank reimburse the stolen funds and issue a replacement debit card, Plaintiff McQuiag made at least three separate trips to her bank to fill out paperwork relating to the fraudulent purchases. Plaintiff McQuiag's debit account was frozen and she did not have access to her funds for approximately three days during the fraud investigation. Plaintiff McQuiag spent approximately eight hours addressing issues arising from the Home Depot breach. Plaintiff McQuiag never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

39. Plaintiff Inocencio Valencia is a resident of Valrico, Florida and was a Florida resident during the period of the Home Depot breach. Plaintiff Valencia shopped at a Home Depot retail store in Florida between April 1 and September 18, 2014 by swiping his debit and credit cards through Home Depot point-of-sale devices to make payment. Plaintiff Valencia received an e-mail notification from Home Depot regarding the breach in early September 2014. Plaintiff Valencia then reviewed his debit account statement and discovered fraudulent charges on the account. Plaintiff Valencia reported the fraudulent purchases to his credit union and was required to make a trip to the credit union to complete paperwork for a fraud investigation. The fraud investigation and reimbursement of stolen funds to

his debit account took approximately one to two weeks. During that time, Plaintiff Valencia's debit account was frozen and he did not have access to approximately \$3,000 of his funds. As a result, Plaintiff Valencia was unable to make timely bill payments scheduled to be paid through his debit card account. To date, Plaintiff Valencia has spent approximately four hours resolving issues arising from the Home Depot breach.

40. Plaintiff Claude Garner is a resident of Sautee Nacoochee, Georgia and was a Georgia resident during the period of the Home Depot breach. Plaintiff Garner shopped at a Home Depot retail store in Georgia between April 1 and September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. Subsequent to his referenced Home Depot transactions, on or about August 8, 2014, while reviewing his account activity online, Plaintiff Garner discovered fraudulent charges totaling approximately \$450 and reported the fraudulent charges to his financial institution. Plaintiff Garner's financial institution closed his account and, after several weeks, reversed the fraudulent charges. During that time, Plaintiff Garner had to wait for his replacement card to arrive and, until the fraudulent charges were resolved, his line of credit was limited. Since the Home Depot breach, in an effort to prevent or mitigate further harm, Plaintiff Garner has subscribed to a credit monitoring program that costs him approximately \$17 per month. Plaintiff Garner spent approximately six hours

addressing issues arising from the Home Depot breach. Plaintiff Garner never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

41. Plaintiff Matthew Forrester is a resident of Watkinsville, Georgia and was a Georgia resident during the period of the Home Depot breach. Plaintiff Forrester shopped at a Home Depot retail store in Georgia between April 1 and September 18, 2014 by swiping his debit card through Home Depot point-of-sale devices to make payment. Subsequent to his referenced Home Depot transactions, on or about September 2, 2014, Plaintiff Forrester's bank called and informed him that a criminal had attempted to use his debit account information to make a fraudulent charge of approximately \$100. Plaintiff Forrester's debit account was temporarily frozen by his bank and he had to wait approximately four days for a replacement card to be issued, during which time it was difficult for him to make trips to the bank to obtain cash. In addition, Plaintiff Forrester's wife's web domain was cancelled when an automatic payment scheduled to be paid with his debit card account was declined. Plaintiff Forrester spent approximately 12 hours addressing issues arising from the Home Depot breach. Plaintiff Forrester never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

42. Plaintiff Royce Kitchens is a resident of Sugar Hill, Georgia and was a Georgia resident during the period of the Home Depot breach. Plaintiff Kitchens shopped at a Home Depot retail store in Georgia between April 1 and September 18, 2014 by swiping his debit card through Home Depot point-of-sale devices to make payment. In or around early October 2014, Plaintiff Kitchens' bank automatically cancelled his debit card and mailed a replacement card to him. Around that same time, Plaintiff Kitchens received a letter notification from Home Depot regarding the breach. Plaintiff Kitchens had to wait approximately one week for the replacement card to arrive, during which time he had to make almost ten trips to the bank to withdraw cash. Plaintiff Kitchens spent over 10 hours addressing issues arising from the Home Depot breach.

43. Plaintiff William Lambert is a resident of Woodstock, Georgia and was a Georgia resident during the period of the Home Depot breach. Plaintiff Lambert shopped at a Home Depot retail store in Georgia between April 1 and September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. Plaintiff Lambert learned of the Home Depot breach on or about September 27, 2014 when his financial institution contacted him after it detected fraudulent activity on his credit card account. An investigation revealed several fraudulent charges to Plaintiff Lambert's credit card account at an auto-parts store totaling over \$800. Thereafter, Plaintiff Lambert lost access to his line

of credit until a replacement card arrived in early October 2014, and he was forced to withdraw money from a savings account to cover his living expenses and bill payments during that time. As a result of the Home Depot breach, Plaintiff Lambert has spent over ten hours addressing issues arising from the breach. Plaintiff Lambert never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

44. Plaintiff Kristine Larson is a resident of Atlanta, Georgia and was a Georgia resident during the period of the Home Depot breach. Plaintiff Larson shopped at a Home Depot retail store in Georgia between April 1 and September 18, 2014 by swiping her credit card through Home Depot point-of-sale devices to make payment. To date, Plaintiff Larson has spent over an hour addressing issues arising from the Home Depot breach, including resetting saved payment information tied to her credit card. Plaintiff Larson never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

45. Plaintiffs Carlton and Sandra Smith are a married couple residing in Murrayville, Georgia and were Georgia residents during the period of the Home Depot breach. Mr. Smith shopped at a Home Depot retail store in Georgia between April 1 and September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. Subsequent to his referenced Home Depot



transactions, on or about September 10, 2014, Mr. and Mrs. Smith's financial institution contacted Mrs. Smith regarding a fraudulent charge in China that was attempted on their credit card account. Mr. and Mrs. Smith spent about two hours addressing issues arising from the Home Depot breach and monitoring their account for fraud. Mr. and Mrs. Smith never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

46. Plaintiff Ivonda Washington is a resident of Stone Mountain, Georgia and was a Georgia resident during the period of the Home Depot breach. Plaintiff Washington shopped at a Home Depot retail store in Georgia between April 1 and September 18, 2014 by swiping her credit card through Home Depot point-of-sale devices to make payment. Plaintiff Washington spent approximately 20 hours addressing issues arising from the Home Depot breach, including dealing with the inconvenience of awaiting replacement cards and checking her accounts regularly for fraud. Plaintiff Washington never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

47. Plaintiff Brenda Blough is a resident of Oswego, Illinois and was an Illinois resident during the period of the Home Depot breach. Plaintiff Blough shopped at a Home Depot retail store in Illinois between April 1 and September 18, 2014 by swiping her credit card through Home Depot point-of-sale devices to

make payment. Subsequent to her referenced Home Depot transactions, Plaintiff Blough learned that her credit card account was breached on or about July 18, 2014, when she reviewed her credit card statement and discovered two fraudulent charges made at a Tennessee gas station on or about July 13, 2014, totaling approximately \$275. To report and seek reversal of the fraudulent charges, Plaintiff Blough was required to fill out and submit paperwork to her financial institution, but she was not reimbursed until months later, on or about September 11, 2014. Plaintiff Blough's credit card was deactivated and she had to wait nearly two weeks for a replacement card during which time she did not have access to her line of credit. Plaintiff Blough spent approximately six hours addressing issues arising from the Home Depot data breach. Plaintiff Blough never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

48. Plaintiff Mary Hope Griffin is a resident of River Forest, Illinois and was an Illinois resident during the period of the Home Depot breach. Plaintiff Griffin shopped at a Home Depot retail store in Illinois between April 1 and September 18, 2014 by swiping her credit card through Home Depot point-of-sale devices to make payment. As a result of the Home Depot breach, Plaintiff Griffin spent several hours checking her credit account for fraud. Plaintiff Griffin never

received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

49. Plaintiff Michael Marko is a resident of Godfrey, Illinois and was an Illinois resident during the period of the Home Depot breach. Plaintiff Marko shopped at a Home Depot retail store in Illinois between April 1 and September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. Plaintiff Marko has spent time and money addressing issues arising from the Home Depot breach and having his statements reviewed for fraud. Plaintiff Marko never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

50. Plaintiff Vincent Murphy is a resident of Crystal Lake, Illinois and was an Illinois resident during the period of the Home Depot breach. Plaintiff Murphy shopped at a Home Depot retail store in Illinois between April 1 and September 18, 2014 by swiping his debit card through Home Depot point-of-sale devices to make payment. As a result of the Home Depot breach, Plaintiff Murphy spent approximately one hour resetting his automatic bill payments tied to his debit card. Plaintiff Murphy never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

51. Plaintiff Kelsey O'Brien ("K. O'Brien") is a resident of West Dundee, Illinois and was an Illinois resident during the period of the Home Depot breach.

Plaintiff K. O'Brien shopped at a Home Depot retail store in Illinois between April 1 and September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. In early October 2014, fraudulent charges totaling approximately \$300 to a Wisconsin-based vacation broker were identified on Plaintiff K. O'Brien's credit card account statement. After reporting the fraudulent charges to his bank, Plaintiff K. O'Brien lost access to his line of credit and the \$300 in fraudulent charges were not reversed for about one week. Plaintiff K. O'Brien incurred unreimbursed costs, including paying for his credit reports, and spent approximately 15 to 20 hours addressing issues arising from the Home Depot breach. Plaintiff K. O'Brien never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

52. Plaintiff Richard Bergeron is a resident of Indianapolis, Indiana and was an Indiana resident during the period of the Home Depot breach. Plaintiff Bergeron shopped at a Home Depot retail store in Indiana between April 1 and September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. Plaintiff Bergeron never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

53. Plaintiff Linda Werak is a resident of Wichita, Kansas and was a Kansas resident during the period of the Home Depot breach. Plaintiff Werak

shopped at a Home Depot retail store in Kansas between April 1 and September 18, 2014 by swiping her debit card through Home Depot point-of-sale devices to make payment. On or about September 22, 2014, Plaintiff Werak's credit union contacted her to check her transaction history because of the Home Depot data breach. Plaintiff Werak spent over two hours addressing issues arising from the Home Depot breach and checking for fraud. Plaintiff Werak never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

54. Plaintiff Todd Burris is a resident of Lexington, Kentucky and was a Kentucky resident during the period of the Home Depot breach. Plaintiff Burris shopped at a Home Depot retail store in Kentucky between April 1 and September 18, 2014 by swiping his debit and credit cards through Home Depot point-of-sale devices to make payment. On or about September 21, 2014, Plaintiff Burris received an e-mail notification from Home Depot regarding the breach. On or about November 8, 2014, Plaintiff Burris received another e-mail from Home Depot indicating his e-mail address had been compromised in the breach. Plaintiff Burris spent approximately 12 hours addressing issues arising from the Home Depot breach and monitoring for fraud.

55. Plaintiff Kelli LoBello is a resident of Darrow, Louisiana and was a Louisiana resident during the period of the Home Depot breach. Plaintiff LoBello

shopped at a Home Depot retail store in Louisiana between April 1 and September 18, 2014 by swiping her debit card through Home Depot point-of-sale devices to make payment. Plaintiff LoBello attempted to file her tax return in February 2015 and it was rejected because a fraudulent tax return was already filed using her identity. The IRS recommended that Plaintiff LoBello contact her bank; when she did, her bank told her there were multiple fraudulent attempts on her debit account as a result of the Home Depot breach. Since that time, Plaintiff LoBello also received a significant number of calls from blocked telephone numbers phishing for her personal and financial information. Plaintiff LoBello spent at least 10 hours addressing issues arising from the Home Depot breach including financial and tax issues, and will likely need to file her taxes in paper format as opposed to online going forward. Plaintiff LoBello also paid approximately \$20 per month to the credit bureaus for her credit report since the breach, which has not been reimbursed.

56. Plaintiff Allen Mazerolle is a resident of Falmouth, Maine and was a Maine resident during the period of the Home Depot breach. Plaintiff Mazerolle shopped at a Home Depot retail store in Maine between April 1 and September 18, 2014 by swiping his debit and credit cards through Home Depot point-of-sale devices to make payment. Plaintiff Mazerolle had to wait approximately one week for replacement cards from his financial institution, during which time he had to go

to his bank to get cash. Plaintiff Mazerolle spent over 40 hours addressing issues arising from the Home Depot breach and monitoring for fraud. Plaintiff Mazerolle never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

57. Plaintiff James Burden is a resident of Bel Air, Maryland and was a Maryland resident during the period of the Home Depot breach. Plaintiff Burden shopped at a Home Depot retail store in Maryland between April 1 and September 18, 2014 by swiping his Home Depot credit card through Home Depot point-of-sale devices to make payment. Plaintiff Burden's Home Depot credit card was linked to his credit union checking account. Subsequent to his referenced Home Depot transactions, in early September 2014, Plaintiff Burden wrote a check to a friend that bounced. Plaintiff Burden contacted his credit union and also checked his Home Depot credit card statement, discovering two fraudulent charges. Although Home Depot eventually reversed the fraudulent charges, Plaintiff Burden's checking account information was compromised. Plaintiff Burden had to wait approximately five days for his new checking account to be created, and an additional five days waiting for a replacement debit card for the new checking account. Plaintiff Burden also cancelled his Home Depot card to mitigate further fraud. Plaintiff Burden spent six hours addressing issues arising from the Home

Depot breach. Plaintiff Burden never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

58. Plaintiff Daniel Durgin is a resident of Boston, Massachusetts and was a Massachusetts resident during the period of the Home Depot breach. Plaintiff Durgin shopped at a Home Depot retail store in Massachusetts between April 1 and September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. Subsequent to his referenced Home Depot transactions, in or around the fall of 2014, Plaintiff Durgin received a phone call from his credit union indicating that his credit account was being closed and a new card with new numbers would be issued as a result of the Home Depot breach. Plaintiff Durgin lost access to his line of credit for 10 days while waiting for a new card. Plaintiff Durgin spent over two hours addressing issues arising from the Home Depot breach and monitoring for fraud. Plaintiff Durgin never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

59. Plaintiff Larry Flores is a resident of Westland, Michigan and was a Michigan resident during the period of the Home Depot breach. Plaintiff Flores shopped at a Home Depot retail store in Michigan between April 1 and September 18, 2014 by swiping his debit and credit cards through Home Depot point-of-sale devices to make payment. On or about October 17, 2014, Plaintiff Flores received



a letter from Barclay's notifying him that his MasterCard credit card was affected by the Home Depot breach. Plaintiff Flores also received a letter from his bank notifying him that his debit card had been affected by the Home Depot breach. He also received an e-mail from Home Depot regarding the breach in late October 2014, as well as a second e-mail notification from Home Depot regarding the breach on or about November 11, 2014. Plaintiff Flores spent over five hours addressing issues arising from the Home Depot breach and monitoring for fraudulent activity.

60. Plaintiff Nicholas Hott is a resident of Lansing, Michigan and was a Michigan resident during the period of the Home Depot breach. Plaintiff Hott shopped at a Home Depot retail store in Michigan between April 1 and September 18, 2014 by swiping his debit card through Home Depot point-of-sale devices to make payment. On or about September 24, 2014, fraudulent charges totaling approximately \$500 were identified on Plaintiff Hott's debit card account. After reporting the fraudulent charges to his bank, Plaintiff Hott lost access to the funds in his debit account for approximately two weeks while waiting to receive a replacement card. During that waiting period, Plaintiff Hott maxed out a separate line of credit to cover his living expenses. Plaintiff Hott also incurred unreimbursed late and/or declined payment fees as a result of failed automatic bill payments scheduled to be paid with his debit card. On or about November 11,

2014, Plaintiff Hott received an e-mail notification from Home Depot regarding the breach. Plaintiff Hott spent approximately 15 hours addressing issues arising from the Home Depot breach.

61. Plaintiff Scott Ferguson is a resident of St. Paul, Minnesota and was a Minnesota resident during the period of the Home Depot breach. Plaintiff Ferguson shopped at a Home Depot retail store in Minnesota between April 1 and September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. Plaintiff Ferguson spent over 15 hours addressing issues arising from the Home Depot breach and monitoring his accounts for fraud. Plaintiff Ferguson never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

62. Plaintiff Mario Tolliver is a resident of Jackson, Mississippi and was a Mississippi resident during the period of the Home Depot breach. Plaintiff Tolliver shopped at a Home Depot retail store in Mississippi between April 1 and September 18, 2014 by swiping his debit cards through Home Depot point-of-sale devices to make payment. Subsequent to his referenced Home Depot transactions, in or around September 2014, Plaintiff Tolliver's bank notified him by mail of the Home Depot breach. On or about November 10, 2014, Plaintiff Tolliver received an e-mail notification from Home Depot regarding the breach. On or about February 26, 2015, Plaintiff Tolliver experienced fraudulent charges on his debit

card for \$113 in Europe. Plaintiff Tolliver was not reimbursed for the stolen funds and he was forced to borrow money, as he was on a business trip when the fraudulent charges occurred. Plaintiff Tolliver spent over 35 hours attempting to resolve his finances and monitoring his accounts for fraud arising from the Home Depot breach.

63. Plaintiff Jeffrey Hartman is a resident of Chesterfield, Missouri and was a Missouri resident during the period of the Home Depot breach. Plaintiff Hartman shopped at a Home Depot retail store in Missouri between April 1 and September 18, 2014 by swiping his credit cards through Home Depot point-of-sale devices to make payment. On or about April 1, 2015, Plaintiff Hartman's wife, a joint account holder on one of his credit cards, attempted to make a retail purchase with that line of credit and was declined. After using cash to make the purchase, she contacted their financial institution, which indicated that the account was frozen because of suspicious activity. The financial institution further informed Plaintiff Hartman's wife that three fraudulent charges were already attempted, and approximately eight more were attempted while she was on the line. The financial institution then closed Plaintiff Hartman's line of credit and opened a new credit account. Although the financial institution expedited shipment of his wife's new credit card, Plaintiff Hartman's card was sent via regular mail and he did not receive it before leaving on a weekend vacation. As a result of this line of credit

being temporarily unavailable, Plaintiff Hartman expended additional cash and made charges on another credit card, losing the cash back benefits he would have received by using the unavailable line of credit. Plaintiff Hartman spent over six hours addressing issues arising from the Home Depot breach and monitoring his accounts for fraud. Plaintiff Hartman never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

64. Plaintiff Katherine Holmes is a resident of Kansas City, Missouri and was a Missouri resident during the period of the Home Depot breach. Plaintiff Holmes shopped at a Home Depot retail store in Missouri between April 1 and September 18, 2014 by swiping her debit card through Home Depot point-of-sale devices to make payment. Subsequent to her referenced Home Depot transactions, unbeknownst to Plaintiff Holmes, her bank deactivated her debit card and when she attempted to use the debit card to make a purchase it was declined by the retail vendor. Plaintiff Holmes' husband suffered a similar embarrassment as his card was also temporarily shut down. As a result of the Home Depot breach, Plaintiff Holmes spent over twelve hours attempting to resolve her and her husband's finances and checking for fraudulent activity. Plaintiff Holmes never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

65. Plaintiff Rebecca McGehee is a resident of Grandview, Missouri and was a Missouri resident during the period of the Home Depot breach. Plaintiff McGehee shopped at a Home Depot retail store in Missouri between April 1 and September 18, 2014 by swiping her debit card through Home Depot point-of-sale devices to make payment. Plaintiff McGehee learned of the Home Depot breach in or around November or December 2014 when her credit union informed her of the breach and that it was issuing her a replacement debit card. Following the Home Depot breach, an identity thief filed a fraudulent income tax return using Plaintiff McGehee's name and Social Security number. Her accountant informed her that the IRS had rejected her income tax filing because of the fraudulent return. Plaintiff McGehee spent over 10 hours addressing issues arising from the Home Depot breach, and her efforts are ongoing. She was required to file paper tax returns as opposed to filing online and will likely be required to file paper returns going forward. Plaintiff McGehee never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

66. Plaintiff Gilda Wynne is a resident of Reno, Nevada and was a Nevada resident during the period of the Home Depot breach. Plaintiff Wynne shopped at a Home Depot retail store in Nevada between April 1 and September 18, 2014 by swiping her credit card through Home Depot point-of-sale devices to make payment. Plaintiff Wynne learned of the Home Depot breach on or about

December 29, 2014 when she received her credit card statement and discovered a fraudulent charge from the same Home Depot location where she had shopped. Although her financial institution ultimately reversed the fraudulent charge, the investigation took several weeks and Plaintiff Wynne had to wait for a replacement card to be delivered. Plaintiff Wynne also incurred unreimbursed late and/or declined payment fees as a result of failed automatic bill payments scheduled to be paid with her credit card. As a result of the Home Depot breach, Plaintiff Wynne spent approximately 14 hours attempting to resolve her finances. Plaintiff Wynne never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

67. Plaintiff Laureen Anyon is a resident of Toms River, New Jersey and was a New Jersey resident during the period of the Home Depot breach. Plaintiff Anyon shopped at a Home Depot retail store in New Jersey between April 1 and September 18, 2014 by swiping her debit and credit cards through Home Depot point-of-sale devices to make payment. Plaintiff Anyon learned of the Home Depot breach on or about October 1, 2014, when her bank called her to report approximately \$100 of fraudulent charges to her debit account at an online pet store. The bank informed Plaintiff Anyon that it blocked additional attempted charges of approximately \$600 to her debit card. Although Plaintiff Anyon's debit account was reimbursed within three days, she had to wait approximately ten days

for a replacement debit card, during which time she had to go to the bank to get cash. Plaintiff Anyon also had to borrow money from her mother to cover bill payments. In addition, Plaintiff Anyon incurred unreimbursed late and/or declined payment fees totaling approximately \$10 as a result of failed automatic bill payments scheduled to be paid with her debit card, and her newspaper subscription was cancelled. Plaintiff Anyon spent approximately 25 to 30 hours addressing issues arising from the Home Depot breach. Plaintiff Anyon never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

68. Plaintiff Mary Gorman is a resident of Maplewood, New Jersey and was a New Jersey resident during the period of the Home Depot breach. Plaintiff Gorman shopped at a Home Depot retail store in New Jersey between April 1 and September 18, 2014 by swiping her debit card through Home Depot point-of-sale devices to make payment. Plaintiff Gorman spent approximately five hours addressing issues arising from the Home Depot breach and monitoring for fraud. Plaintiff Gorman never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

69. Plaintiff Gary Lowenthal is a resident of Ridgewood, New Jersey and was a New Jersey resident during the period of the Home Depot breach. Plaintiff Lowenthal shopped at a Home Depot retail store in New Jersey between April 1

and September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. As a result of the Home Depot breach, Plaintiff Lowenthal spent approximately four hours monitoring his account for fraud. Plaintiff Lowenthal never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

70. Plaintiff Barbara Saffran ("B. Saffran") is a resident of Lakewood, New Jersey and was a New Jersey resident during the period of the Home Depot breach. Plaintiff B. Saffran shopped at a Home Depot retail store in New Jersey between April 1 and September 18, 2014 by swiping her credit card through Home Depot point-of-sale devices to make payment. Plaintiff B. Saffran spent over three hours addressing issues arising from the Home Depot breach and searching for fraudulent charges. Plaintiff B. Saffran never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

71. Plaintiff Robert Vandertoorn is a resident of North Bergen, New Jersey and was a New Jersey resident during the period of the Home Depot breach. Plaintiff Vandertoorn shopped at a Home Depot retail store in New Jersey between April 1 and September 18, 2014 by swiping his debit card through Home Depot point-of-sale devices to make payment. Subsequent to his referenced Home Depot transactions, on or about July 8, 2014, fraudulent charges appeared on two of his



credit cards issued through the same financial institution as his debit card. After experiencing these fraudulent charges, Plaintiff Vandertoorn lost access to these lines of credit for several days until he was reimbursed for the fraudulent charges and replacement cards were issued. Plaintiff Vandertoorn spent approximately 10 hours addressing issues arising from the Home Depot breach. Plaintiff Vandertoorn never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

72. Plaintiff Ronald Levene is a resident of Sandia Park, New Mexico and was a New Mexico resident during the period of the Home Depot breach. Plaintiff Levene shopped at a Home Depot retail store in New Mexico between April 1 and September 18, 2015 by swiping his credit card through Home Depot point-of-sale devices to make payment. As a result of the Home Depot breach, Plaintiff Levene has spent approximately one hour per month monitoring his account for fraudulent activity. Plaintiff Levene never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

73. Plaintiff Alexandra O'Brien ("A. O'Brien") is a resident of Wading River, New York and was a New York resident during the period of the Home Depot breach. Plaintiff A. O'Brien shopped at a Home Depot retail store in New York between April 1 and September 18, 2014 by swiping her debit card through Home Depot point-of-sale devices to make payment. Plaintiff A. O'Brien was

assessed late and/or declined payment fees as a result of failed automatic bill payments tied to her debit card. Plaintiff A. O'Brien spent over 30 hours addressing issues arising from the Home Depot breach and monitoring her accounts daily for fraudulent activity. Plaintiff A. O'Brien never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

74. Plaintiff Jason O'Brien ("J. O'Brien") is a resident of Wading River, New York and was a New York resident during the period of the Home Depot breach. Plaintiff J. O'Brien shopped at a Home Depot retail store in New York between April 1 and September 18, 2014 by swiping his debit and credit cards through Home Depot point-of-sale devices to make payment. On or about November 14, 2014, Plaintiff J. O'Brien received an e-mail notification from Home Depot regarding the breach. Plaintiff J. O'Brien spent over 10 hours addressing issues arising from the Home Depot breach and monitoring his accounts for fraudulent activity.

75. Plaintiff Sara Saffran ("S. Saffran") is a resident of Staten Island, New York and was a New York resident during the period of the Home Depot breach. Plaintiff S. Saffran shopped at a Home Depot retail store in New York between April 1 and September 18, 2014 by swiping her credit card through Home Depot point-of-sale devices to make payment. Plaintiff S. Saffran spent over three hours

addressing issues arising from the Home Depot breach and monitoring her credit account for fraud. Plaintiff S. Saffran never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

76. Plaintiff Travis Russell is a resident of West Fargo, North Dakota and was a North Dakota resident during the period of the Home Depot breach. Plaintiff Russell shopped at a Home Depot retail store in North Dakota between April 1 and September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. Subsequent to his referenced Home Depot transactions, on or about August 27, 2014, Plaintiff Russell received an e-mail from his financial institution indicating his credit card was compromised. Plaintiff Russell spent over thirty hours addressing issues arising from the Home Depot breach and checking his credit account for fraudulent transactions. Plaintiff Russell never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

77. Plaintiff David Erisman is a resident of Greenville, Ohio and was an Ohio resident during the period of the Home Depot breach. Plaintiff Erisman shopped at a Home Depot retail store in Ohio between April 1 and September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. In or around March 2015, Plaintiff Erisman's credit card was declined

when he attempted to make a purchase at a hardware store. Plaintiff Erisman then contacted his financial institution, which had flagged his account due to fraudulent charge attempts. His financial institution issued a replacement card, which took about two weeks to arrive. Plaintiff Erisman spent over 25 hours addressing issues arising from the Home Depot breach. Plaintiff Erisman never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

78. Plaintiff Mary Stenart is a resident of Bethany, Oklahoma and was an Oklahoma resident during the period of the Home Depot breach. Plaintiff Stenart shopped at a Home Depot retail store in Missouri between April 1 and September 18, 2014 by swiping her credit card through Home Depot point-of-sale devices to make payment. On or about September 11, 2014, Plaintiff Stenart received a letter from her credit union indicating that her credit card was compromised in the Home Depot breach. As a result of the Home Depot breach, Plaintiff Stenart spends time every month reviewing the transactions on her account. Plaintiff Stenart never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

79. Plaintiff Dennis Borrell is a resident of Ephrata, Pennsylvania and was a Pennsylvania resident during the period of the Home Depot breach. Plaintiff Borrell shopped at a Home Depot retail store in Pennsylvania between April 1 and

September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. Plaintiff Borrell learned of the Home Depot breach on or about September 17, 2014, when he reviewed his online bank statement and discovered approximately \$4,500 in fraudulent charges for the purchase of airline tickets. Plaintiff Borrell's financial institution froze his credit card account and he could not access this line of credit for over one week. The frozen credit card account was Plaintiff Borrell's only credit card and it was linked to his PayPal account, which limited his access to that account. He then had to reset many auto-bill payment accounts. Although his financial institution removed the fraudulent charges, it did not complete its investigation until on or about November 1, 2014. On or about September 21, 2014, Plaintiff Borrell received an email notification from Home Depot regarding the breach. Plaintiff Borrell spent over 10 hours addressing issues arising from the Home Depot breach.

80. Plaintiff Michelle Jhingoor is a resident of Great Bend, Pennsylvania and was a Pennsylvania resident during the period of the Home Depot breach. Plaintiff Jhingoor shopped at Home Depot retail stores in Pennsylvania and New York between April 1 and September 18, 2014 by swiping her debit card through Home Depot point-of-sale devices to make payment. Subsequent to her referenced Home Depot transactions, in late August 2014, Plaintiff Jhingoor learned that her debit card was frozen because an automatic payment linked to that debit card for

the monthly premium on a \$100,000 life insurance policy on her ex-husband, of which she was a beneficiary, was declined. At the time of the attempted payment on or about July 8, 2014, Plaintiff Jhingoor received a confirmation number for the transaction and believed the payment was accepted. However, the debit card was cancelled due to the Home Depot breach and the charge never went through. Consequently, the life insurance policy was cancelled and the insurance provider refused to reinstate it at the same rate because of her ex-husband's health issues. As a result of the Home Depot breach, Plaintiff Jhingoor spent over 50 hours attempting to resolve her finances and reinstate the life insurance policy at its former rate. Plaintiff Jhingoor never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

81. Plaintiff Doug Travers is a resident of Woonsocket, Rhode Island and was a Rhode Island resident during the period of the Home Depot breach. Plaintiff Travers shopped at Home Depot retail stores in Rhode Island and Massachusetts between April 1 and September 18, 2014 by swiping his debit card through Home Depot point-of-sale devices to make payment. As a result of the Home Depot breach, Plaintiff Travers' debit card was automatically replaced and he had to wait for the replacement card to arrive. Plaintiff Travers never received any individual notification from Home Depot regarding the breach.

82. Plaintiff Lawrence Elledge is a resident of Hanahan, South Carolina and was a South Carolina resident during the period of the Home Depot breach. Plaintiff Elledge shopped at a Home Depot retail store in South Carolina between April 1 and September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. On or about October 9, 2014, when reviewing his credit card statement, Plaintiff Elledge discovered fraudulent charges totaling approximately \$230 at a North Carolina grocery store. After identifying these fraudulent charges and notifying his financial institution, Plaintiff Elledge's credit card account was frozen and he lost access to his line of credit for two weeks. The fraudulent charges were not reversed until October 31, 2014. Plaintiff Elledge spent over four hours addressing issues arising from the Home Depot breach, not including his daily monitoring of his account for fraud. Plaintiff Elledge never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

83. Plaintiff Pauline Cuff is a citizen of Crowborough, United Kingdom who has a vacation home in Little River, South Carolina. Plaintiff Cuff shopped at a Home Depot retail store in South Carolina between April 1 and September 18, 2014 by swiping her credit card through Home Depot point-of-sale devices to make payment. Subsequent to her referenced Home Depot transactions, on or about September 3, 2014, Plaintiff Cuff's financial institution called her to confirm

whether suspicious charges on her credit account totaling approximately \$1,900 to a Charlotte, North Carolina store were fraudulent, and she confirmed that they were. Thereafter, Plaintiff Cuff lost access to her line of credit and could not obtain a replacement card until she returned to the United Kingdom, as she was in the United States on vacation at the time of the unauthorized charges. Plaintiff Cuff missed bill payments and was assessed late and/or declined payment fees' totaling approximately \$60 as a result of failed automatic bill payments scheduled to be paid with her credit card, and was not reimbursed for approximately \$30 of these fees. Plaintiff Cuff incurred unreimbursed expenses, including loss of cash back on credit cards used to pay monthly expenses, and spent approximately 10 hours to date addressing issues arising from the Home Depot breach. Plaintiff Cuff never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

84. Plaintiff Lindsay Wirth is a resident of Nashville, Tennessee and was a Tennessee resident during the period of the Home Depot breach. Plaintiff Wirth shopped at a Home Depot retail store in Tennessee between April 1 and September 18, 2014 by swiping her debit cards through Home Depot point-of-sale devices to make payment. Subsequent to her referenced Home Depot transactions, in June 2014, Plaintiff Wirth identified fraudulent charges on one of her debit card accounts of approximately \$2,260 made on or about May 31, 2014. After notifying



her bank of these fraudulent charges, Plaintiff Wirth's debit card account was frozen and she had to make trips to the bank to get cash. She was also forced to use funds from a secondary checking account for approximately two months while her bank conducted a fraud investigation. Since the Home Depot breach, Plaintiff Wirth now pays approximately \$6 per month for credit monitoring protection. On or about November 9, 2014, Plaintiff Wirth received an e-mail notification from Home Depot regarding the breach. Plaintiff Wirth incurred unreimbursed expenses and spent over 25 hours addressing issues arising from the Home Depot breach.

85. Plaintiff Marilyn Geller is a resident of Houston, Texas and was a Texas resident during the period of the Home Depot breach. Plaintiff Geller shopped at a Home Depot retail store in Texas between April 1 and September 18, 2014 by swiping her credit card through Home Depot point-of-sale devices to make payment. Subsequent to her referenced Home Depot transactions, on or about September 10, 2014, Plaintiff Geller's financial institution e-mailed and texted her to notify her of a possible fraudulent charge. Plaintiff Geller thereafter confirmed that a charge of approximately \$280 reflected on her credit card account was fraudulent. The financial institution further informed her that two additional attempts to make fraudulent charges on that account for similar amounts had been blocked. After experiencing these fraudulent charges, Plaintiff Geller's credit card was deactivated and she lost access to her line of credit until she received her

replacement card. Plaintiff Geller spent over 10 hours addressing issues arising from the Home Depot breach. Plaintiff Geller never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

86. Plaintiff Scott McGiffid is a resident of Houston, Texas and was a Texas resident during the period of the Home Depot breach. Plaintiff McGiffid shopped at a Home Depot retail store in Texas between April 1 and September 18, 2014 by swiping his credit cards through Home Depot point-of-sale devices to make payment. On or about November 7, 2014, Plaintiff McGiffid identified fraudulent charges of approximately \$1 and \$2 on his credit card statement (indicating that the criminal was testing the validity of the card) and charges for \$49.95 pending and ready to post from Europe on one of his credit card statements. After notifying the financial institution of the unauthorized activity, Plaintiff McGiffid's credit card account was frozen and he lost access to that line of credit for 10 days. As a result, Plaintiff McGiffid missed approximately 20 automatic bill payments scheduled to be paid with the frozen credit card account. Further, Plaintiff McGiffid's second line of credit with the same financial institution that did not have any fraudulent charges was lowered \$11,500. Plaintiff McGiffid spent over 70 hours addressing issues arising from the Home Depot breach. Plaintiff

McGiffid never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

87. Plaintiff Alma Pineda is a resident of Houston, Texas and was a Texas resident during the period of the Home Depot breach. Plaintiff Pineda shopped at a Home Depot retail store in Texas between April 1 and September 18, 2014 by swiping her debit card through Home Depot point-of-sale devices to make payment. Subsequent to her referenced Home Depot transactions, on or about August 4, 2014, a criminal used her debit card information to fraudulently purchase approximately \$2,750 of merchandise at a Home Depot store in Galveston, Texas. After identifying the fraudulent charge, Plaintiff Pineda's debit card was deactivated, she lost access to funds in her debit account until she received a replacement debit card, and she had to travel to her bank branch multiple times to fill out paperwork in connection with the fraud investigation. Eventually, the stolen funds were reimbursed to her debit card account. Plaintiff Pineda incurred unreimbursed expenses and spent approximately six hours addressing issues arising from the Home Depot breach. Plaintiff Pineda never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

88. Plaintiff DeAnn Fieselman is a resident of New Harmony, Utah and was a Utah resident during the period of the Home Depot breach. Plaintiff

Fieselman shopped at a Home Depot retail store in Utah between April 1 and September 18, 2014 by swiping her credit cards through Home Depot point-of-sale devices to make payments. Subsequent to her referenced Home Depot transactions, on or about September 12, 2014, Plaintiff Fieselman received a text alert and phone call from one of her financial institutions informing her that her credit card had an attempted fraudulent charge for approximately \$80. During this phone call, the financial institution asked her if she had shopped at Home Depot and notified her of the breach. After confirming that the charge was fraudulent, Plaintiff Fieselman lost access to her credit card for approximately three days. As a result of the Home Depot breach, Plaintiff Fieselman spent approximately two hours attempting to rectify the issues related to the fraudulent charges on her credit card. Following the Home Depot breach, Plaintiff Fieselman also began to receive spam IRS phone calls. She received two such calls; one in September 2014 and one in April 2015. Plaintiff Fieselman never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

89. Plaintiff Kent Coulson is a resident of Ivins, Utah and was a Utah resident during the period of the Home Depot breach. Plaintiff Coulson shopped at a Home Depot retail store in Utah between April 1 and September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. After the breach period, in the fall of 2014, Plaintiff Coulson received an

e-mail notification from Home Depot regarding the breach. Plaintiff Coulson's credit card was cancelled and a replacement card was issued, which he received after approximately one week. As a result of the Home Depot breach, Plaintiff Coulson spent approximately 15 hours attempting to resolve his finances and monitoring his accounts for fraudulent activity.

90. Plaintiff Samuel Welch is a resident of Chesapeake, Virginia and was a Virginia resident during the period of the Home Depot breach. Plaintiff Welch shopped at a Home Depot retail store in Virginia between April 1 and September 18, 2014 by swiping his debit card through Home Depot point-of-sale devices to make payment. On or about September 15, 2014, Plaintiff Welch received an e-mail from his bank indicating that his debit card was compromised in the Home Depot breach. As a result of the Home Depot breach, Plaintiff Welch purchased credit monitoring and identity theft prevention and paid an annual fee of approximately \$20, which has not been reimbursed. Plaintiff Welch was required by his bank to change his debit card number and as a result had to reset his automatic payment system for over 40 automated payment accounts. Plaintiff Welch expended additional time addressing issues arising from the Home Depot breach and monitoring his debit account for fraud. Plaintiff Welch never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

91. Plaintiff Sandra Sowell is a resident of Culloden, West Virginia and was a West Virginia resident during the period of the Home Depot breach. Plaintiff Sowell shopped at a Home Depot retail store in West Virginia between April 1 and September 18, 2014 by swiping her credit card through Home Depot point-of-sale devices to make payment. On or about December 13, 2014, while she was traveling on business, a criminal attempted to make fraudulent charges on Plaintiff Sowell's credit card, but her bank blocked the charges and they never posted to her account. As a result of this fraudulent activity and unbeknownst to Plaintiff Sowell, her credit card was frozen; her credit card was then declined when she attempted to pay for a meal. Plaintiff Sowell had no access to any cash or other credit cards and had to borrow money while traveling until she could secure alternative funds from her husband. Plaintiff Sowell spent over six hours addressing issues arising from the Home Depot breach and monitoring her account for fraudulent activity. Plaintiff Sowell never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

92. Plaintiff Douglas Hinton is a resident of Waukesha, Wisconsin and was a Wisconsin resident during the period of the Home Depot breach. Plaintiff Hinton shopped at a Home Depot retail store in Wisconsin between April 1 and September 18, 2014 by swiping his credit card through Home Depot point-of-sale devices to make payment. Subsequent to his referenced Home Depot transactions,

on or about August 28, 2014, a criminal attempted to make a fraudulent international charge on his credit card account for approximately \$160, but his credit card company contacted him and was able to block the charge. Plaintiff Hinton's card was cancelled and a replacement card was issued per his request. Plaintiff Hinton spent approximately five hours addressing issues arising from the Home Depot breach and checking his credit account for fraud. Plaintiff Hinton never received any individual notification from Home Depot regarding the breach or Home Depot's free credit monitoring offer.

93. Plaintiff Scott Pelky is a resident of Racine, Wisconsin and was a Wisconsin resident during the period of the Home Depot breach. Plaintiff Pelky shopped at a Home Depot retail store in Wisconsin between April 1 and September 18, 2014 by swiping his debit and credit cards through Home Depot point-of-sale devices to make payment. In or around October or November 2014, Plaintiff Pelky received a notification from Home Depot regarding the breach. Plaintiff Pelky spent over eight hours addressing issues arising from the Home Depot breach and monitoring his accounts for fraud.

94. Plaintiff James Hansen is a resident of St. Croix, United States Virgin Islands and was a United States Virgin Islands resident during the period of the Home Depot breach. Plaintiff Hansen shopped at a Home Depot retail store in the United States Virgin Islands between April 1 and September 18, 2014 by swiping

his debit card through Home Depot point-of-sale devices to make payment. On or about November 20, 2014, Plaintiff Hansen's debit card was declined when he attempted to make an online purchase and he was unable to access his funds. Plaintiff Hansen's bank told him that his inability to use his debit card was due to the Home Depot breach, but he was unable to resolve the issue over the phone. There was a long line at Plaintiff Hansen's bank, where he waited approximately five hours throughout three separate visits to the bank's branch office to speak with a banker about his debit account. After finally meeting with a bank representative, Plaintiff Hansen learned that, on or about November 12, 2014, fraudulent charges totaling approximately \$1,300 appeared on Plaintiff Hansen's debit card account. Thereafter, Plaintiff Hansen lost access to his debit account funds for about one month until the bank reimbursed the stolen funds to his account, and his account was later closed. Plaintiff Hansen had to borrow money from his mother during this time to pay his bills. Plaintiff Hansen spent over 20 hours addressing issues arising from the Home Depot breach, including time spent looking through statements, standing in line at the bank, resolving his finances, and monitoring his account for additional fraud.

95. Consumer Plaintiffs would not have used their credit or debit cards to make purchases at Home Depot—indeed, they would not have shopped at Home Depot at all during the period of the Home Depot data breach—had Home Depot



told them that it lacked adequate computer systems and data security practices to safeguard customers' personal and financial information from theft, and had Home Depot provided them with timely and accurate notice of the Home Depot data breach.

96. Each of the Consumer Plaintiffs suffered actual injury from having his or her credit or debit card account and personal information compromised and stolen in and as a result of the Home Depot data breach.

97. Each of the Consumer Plaintiffs suffered actual injury and damages in paying money to and purchasing products from Home Depot during the Home Depot data breach that they would not have paid had Home Depot disclosed that it lacked computer systems and data security practices adequate to safeguard customers' personal and financial information and had Home Depot provided timely and accurate notice of the data breach.

98. Each of the Consumer Plaintiffs suffered actual injury in the form of damages to and diminution in the value of his or her personal and financial identity information—a form of intangible property that each of the Consumer Plaintiffs entrusted to Home Depot for the purpose of purchasing its products and that was compromised in and as a result of the Home Depot data breach.

99. Each of the Consumer Plaintiffs has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft

and misuse posed by his or her personal and financial information being placed in the hands of criminals who have already misused such information stolen in the Home Depot data breach via sale of Consumer Plaintiffs' and Class members' personal and financial information on the Internet black market. Consumer Plaintiffs have a continuing interest in ensuring that their private information, which remains in the possession of Home Depot, is protected and safeguarded from future breaches.

100. None of the Consumer Plaintiffs who suffered a loss of use of their account funds, or who had restrictions placed on their accounts, as a result of the Home Depot data breach was reimbursed for the loss of access to or restrictions placed upon their accounts and the resulting loss of use of their own funds.

101. Defendant Home Depot U.S.A., Inc. is a Delaware corporation based in Atlanta, Georgia and operates as a subsidiary of The Home Depot, Inc.

102. Defendant The Home Depot, Inc. is a Delaware corporation based in Atlanta, Georgia. The Home Depot, Inc. is the parent company of Home Depot, U.S.A., Inc. and describes itself in annual reports filed with the Securities Exchange Commission ("SEC") as the world's largest home improvement retailer.

## **STATEMENT OF FACTS**

### **Home Depot's Investment in Technology But Not Data Security**

103. The Home Depot, Inc. is the world's largest home improvement retailer, selling a wide assortment of building materials, home improvement products and lawn and garden products along with a number of other building services. As of the end of fiscal 2014, The Home Depot Inc. and its consolidated subsidiaries operate 2,269 stores throughout the United States, including the Commonwealth of Puerto Rico and the territories of the U.S. Virgin Islands, and Guam, Canada and Mexico. For the fiscal year 2014, Home Depot generated \$83.2 billion in net sales and \$6.3 billion in net earnings, the highest net earnings in company history.

104. The Home Depot, Inc. and Home Depot U.S.A., Inc. operate approximately 1,977 retail stores in the United States. When The Home Depot, Inc., refers to "Home Depot," the "Company," "we," or "our" in its annual reports, it is referring to The Home Depot, Inc. and its consolidated subsidiaries. Further, its publicly filed 2014 annual report admits that "Home Depot, Inc. and its subsidiaries (the 'Company') operate The Home Depot stores, which are full-service, warehouse-style stores." The Home Depot, Inc. and Home Depot U.S.A., Inc. share the same key executives in directing operations and abide by the same established uniform corporate policies and procedures. Therefore, as it relates to the matters pertinent to the claims at issue in this litigation, there is no semblance of independence between the parent, The Home Depot, Inc., and its wholly owned

consolidated subsidiary, Home Depot U.S.A., Inc. as the parent's control over the subsidiary is so complete that it is in fact merely a division or department of the parent. To the extent that Home Depot U.S.A., Inc. is truly a distinct entity, by The Home Depot Inc.'s own admissions, its subsidiaries act as agents for and/or joint venturers with The Home Depot, Inc. in operating stores.

105. As set forth herein, all decisions relating to data security were made from Home Depot's corporate headquarters in Atlanta, Georgia.

106. Over more than a decade, a clear pattern in Home Depot's corporate strategy has emerged: the company is willing to invest in technology that will fuel its revenue growth and increase its profits, but Home Depot is not willing to invest in implementing corresponding security measures that do not provide an immediate boost to the bottom line.

107. Between 2002 and 2004, Home Depot committed to spending more than \$1 billion on new technology, including installation of new self-checkout registers, touchscreen point-of-sale systems and cordless scan guns in its stores. According to its annual reports to shareholders, Home Depot implemented this software in order to eliminate "redundant tasks" and staff fewer employees at the front of their stores.

108. In 2005, Home Depot opened its second technology and customer service center in Austin, Texas to support what it referred to as "growing

technology investment through a staff of engineers, system and application programmers, help desk personnel, system and network operators as well as security administrators.” In spite of this, Home Depot maintained a sparse IT security staff, offering under-market salaries and suffering from poor leadership and high turnover.

109. In 2006 and 2007, Home Depot touted its technological investments in online order processing and customer support, payroll functions, automating supply chain functions, implementation of new systems for warehouse distribution and increased network connectivity to Home Depot’s data centers. Despite a period of record profits, Home Depot’s technological enhancements did not include corresponding investments in IT security.

110. In 2008, Home Depot identified, for the first time, the potential repercussions of a data security breach as a “Risk Factor” in its annual SEC filings and report to shareholders:

***The regulatory environment related to information security and privacy is increasingly rigorous, and a significant privacy breach could adversely affect our business.***

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

111. While paying lip-service to the importance of data security, Home Depot management was focused not on protecting the personal and financial information of its customers, but rather turning around plummeting profits in the wake of the 2008 crash of the national housing market and combatting the increasing market share of rival Lowe's Home Improvement. In 2008, Home Depot's retail sales declined by 7.8 percent, with comparable same-store sales down 8.7 percent, and profits down an astounding \$2.1 billion from the prior fiscal year.

112. In addressing the company's poor performance to shareholders, Home Depot stated that it was "making the adjustments necessary to respond to the economic environment" including "carefully controlling our discretionary spending" and "scrutinizing every dollar of capital." Despite recognizing the risks of a data breach and the expectations of its customers in securing their sensitive data, Home Depot management had no intention to invest in IT security, which fell under the category of "discretionary spending" and was neglected even more in the wake of poor financial performance.

113. That same year, in 2008, Home Depot hired Matthew Carey as its new Chief Information Officer recognizing that the company's "IT capabilities were years behind other retailers of [Home Depot's] size." At all times relevant herein,

Mr. Carey maintained offices in Atlanta, Georgia and made all decisions relating to Home Depot's IT and data security from Atlanta, Georgia.

114. But Mr. Carey's expertise was in software development, not data security. A 2012 article from the *Wall Street Journal* entitled "Home Depot's IT Jumps 'From the Caveman Age to the Modern Age'" notes that Mr. Carey's primary focus as CIO was on technological improvements in the company's supply chain—"an area highly dependent on IT infrastructure," not data security.

115. Mr. Carey oversaw the rollout of Motorola MC75 Enterprise Digital Assistant (EDA) handheld devices referred to by Home Depot as "First Phones." Employees used these devices to locate specific products within the store, search for products at other stores, monitor sales trends, order products, communicate with other employees via walkie-talkie or cell phone, and serve as a mobile point-of-sale register that allows customers to check out using debit or credit cards. The First Phones also provided store managers with real-time sales and gross margin productivity data by department, isle, bay, and stock-keeping unit (SKU). The phones came packaged with mobile device management software known as "Athena," which was manufactured and sold by Odyssey Software, Inc.

116. Following a six-month pilot program in 2009 and 2010, First Phones were deployed to all U.S. Home Depot stores in late 2010 at a cost of \$64 million. After their implementation, Mr. Carey stated in an interview that, "If you compare

us to a world-class retailer, from a technology perspective, 1991 is kind of where we are pegged. This is the first big customer-service tool we've given our associates in a very long time.”

117. While Home Depot's rollout of First Phones initially looked like a success as they accounted for almost a million point-of-sale transactions in the last quarter of 2010, employees' concerns with First Phones were mounting. According to a 2011 industry-trade article, Home Depot employees complained of “First Phone shortages, bulky hardware, buggy software and lack of training—and the fact that IT either can't or won't fix problems with the devices, even when associates take the trouble to send descriptions of device problems up the chain of command.” One employee noted that, “We have all found the obvious and not-so-obvious glitches and flaws in the First Phone and brought them to the attention of folks who should care but either don't or are powerless to affect changes to correct them, the thing was not quite ready for prime time and suggestions and critiques go ignored, because we are not qualified to question the work of the ‘experts.’”

118. Home Depot's response to employee complaints regarding the First Phone portended the company's management culture with respect to other complaints. Thus, although Home Depot professed to encourage its employees to make recommendations and voice concerns about their experiences with Home



Depot technology and data security, when employees actually did so, their concerns fell on deaf ears.

### **Home Depot's History of Ignoring Major Security Risks**

119. In November of 2010, an assistant Home Depot store manager with a computer science background (“HD Employee”) discovered a major security vulnerability inherent in the Athena management software found on Home Depot’s First Phone devices. The HD Employee learned that the Athena software permitted any person with physical access to a Home Depot computer to obtain login credentials of any First Phone user without detection and gain access to Home Depot’s internal systems. Having infiltrated the system, the attacker could then “elevate” its credentials to the highest level of “administrator” so that it would appear as if an authorized person was navigating Home Depot’s systems without triggering alarms. At that point, the attacker could access personal information of Home Depot employees, customers, and vendors, and install malware on point-of-sale terminals that would allow the attacker to collect customers’ credit and debit card information.

120. On November 31, 2010, the HD Employee disclosed the security vulnerability to the employee’s immediate manager (“Store Manager”), who proceeded to contact the district operations manager (“District Operations Manager”) to immediately address the issue. On December 1, 2010, the three

individuals met to discuss the nature of the security vulnerability and ways to resolve the problem. At the conclusion of their meeting, the District Operations Manager placed a telephone call to Home Depot's IT department to alert them of the security vulnerability.

121. On January 3, 2011, the HD Employee confirmed that Home Depot had not addressed the security vulnerability in the Athena software. As a result, the HD Employee met again with the District Operations Manager, who requested that the HD Employee provide an e-mail explanation of the vulnerability for Home Depot's IT department. After preparing a detailed e-mail on the subject, two days later the District Operations Manager confirmed that the information had been forwarded to the appropriate IT personnel.

122. On January 21, 2011, upon receiving no response from Home Depot's IT department and seeing no changes made to the software, the HD Employee sent a letter via certified mail to Home Depot's corporate office in Atlanta, Georgia addressed to Home Depot's General Counsel, Jack A. VanWoerkom, entitled "Breach of Security Notification." (the "January 21 Letter"). The January 21 Letter provided in pertinent part:

This letter serves as formal notification to Home Depot of a serious breach of security on Home Depot's information technology (IT) systems. This breach of security is caused by a failure to safeguard sensitive applications and information as they are found on Home Depot's FIRST Phone Devices (Motorola/Symbol MC75A). Specifically, the Athena management software provided by Odyssey

Software, Inc. has not been properly configured for use in a business environment, or does not contain the functionality required to. The aforementioned software allows any user of Home Depot's internal systems to obtain login credentials of any other user without detection. The only prerequisite to exploitation of this vulnerability is physical access to a Home Depot computer — the attacker need not possess any credentials of their own.

123. After detailing the HD Employee's prior conversations and correspondence with the employee's Store Manager and District Operations Manager, the January 21 Letter alerted Home Depot's legal department to the immediacy of the threat:

To the date of this writing, Home Depot IT has not taken any substantive action to correct this serious breach of security. In the world of IT, it is commonplace for a vulnerability to be exploited within 24 hours of its discovery i.e. the 0-day exploit. If one were to assess the current situation, it has been 52 days to date, since my initial disclosure of the vulnerability — ample time for a malicious individual to exploit any and all avenues of attack and collect all personally identifiable information of Home Depot's associates, customers and vendors stored on Home Depot's IT systems (and additional information for more sophisticated attacks).

Such a serious oversight of information security is clearly contrary to Home Depot's own privacy and security standards [quoting Home Depot's privacy policy available on its website].

The nature of this attack makes it extremely difficult to determine whether a theft of information has occurred as it would appear nearly indistinguishable from normal business operations without a full audit of information logs (which I assume have been maintained at least since the introduction of the FIRST Phone Device). In addition to being in clear non-compliance with Home Depot's own security standards, Home Depot's systems are also deficient with accepted security standards as a matter of law [quoting state-specific law].

To remove any further exposure to the vulnerability, I respectfully request that Home Depot immediately deactivate and remove the Athena management software from all business devices Home Depot manages through this software (Odyssey Software provides clients for other platforms as well e.g. Blackberry - it would be prudent to assume that all clients share this vulnerability) until a suitable fix or replacement software can be found. All users of all affected devices should change their passwords as soon as technically feasible. Additionally, it would be prudent for Home Depot to notify the Massachusetts Attorney General and the Director of Consumer Affairs that such a breach of security has and continues to exist.

124. The letter was signed for and received by a representative of Home Depot in Atlanta, Georgia, but neither Mr. VanWoerkom nor anyone from Home Depot's legal department followed up with the HD Employee.

125. Having received no response to the January 21 Letter, the HD Employee sent a follow-up letter and package via certified mail to Mr. VanWoerkom on March 7, 2011 (the "March 7 Letter"). The March 7 Letter was entitled "Notice of Intent to Disclose" and provided that:

This letter serves as follow-up to the January 21st communication, Breach of Security Notification. An additional 30 days have passed since your receipt of that letter. I am writing again due to the regrettable circumstance that no action has been taken to date by The Home Depot regarding the concerns raised in my initial letter. Additionally, The Home Depot has not indicated any desire to maintain the confidentiality of material facts which pertain to both the vulnerability itself, and its known and potential abuses. The Home Depot's own Data Loss Prevention Policy, Standards and Information Classification and Control Standard (hereinafter *Information Assurance*, attached) serve as controlling documents with respect to the issue at hand.

As stated in my previous letter, vulnerabilities in computer software are an extremely time sensitive issue. At the time of this writing, this vulnerability has been known to exist for 90 days (most likely since the introduction of the FIRST Device). The vulnerability inherent to the Athena software poses an extreme threat to the security of information categorized as “Restricted” by The Home Depot as the level of technical knowledge required to exploit is near zero — basic internet usage skills are sufficient — and that its immediate consequences are theft of “Identity verification information, etc,” privilege escalation and remote execution of code.

The Athena software is not a required, or even marginally useful piece of software for the daily operations of which the FIRST Device was intended — the end user, typically a store associate. Despite my full technical disclosure with practical demonstrations, The Home Depot continues to operate this software known to contain such serious flaws in the configuration, design or both, on it’s [sic] Information Technology (“IT”) systems. By allowing the described situation to continue, The Home Depot’s complacency jeopardizes the confidentiality of “Restricted” Personally Identifiable Information (“PII”) of The Home Depot’s customers, associates and vendors which is stored on The Home Depot’s IT systems, assuming that such a theft of PII has not already occurred or in process. The vulnerability disclosed inherently circumvents the Data Loss Prevention system The Home Depot has established to specifically prevent such loss.

The Home Depot’s own Information Assurance documents describe a set of procedures, systems and people upon which the responsibility to maintain the security of information is held. Specifically, **“It is the responsibility of all associates to enforce this standard as it applies to the information and data within The Home Depot** (emphasis ab origine).” As an associate of The Home Depot, I seek to enforce with respect to the Athena software and its associated tools the standards described in The Home Depot’s own Information Assurance documents. Emphasis is given regarding the responsibility of associates to enforce this standard, while the responsibility to protect “Restricted” information lacks such emphasis; therefore, the Information Assurance documents provide sufficient guidance that proper disclosure seeking enforcement of this standard supersedes an obligation to maintain the confidentiality of “Restricted” information.

Attached you will find a draft of the proposed Initial Public Disclosure document, subject to change to include additional information as it becomes known. In the event that The Home Depot does not, within 14 days of receipt of this letter, remove the Athena software from Home Depot's IT systems in entirety, or make the necessary modifications to the software to make it acceptable for business use, I will provide full disclosure to any third party which I believe will make a good faith effort to compel The Home Depot to do so. Additionally, if I do not receive any communication from The Home Depot within 14 days of receipt of this letter, I will understand The Home Depot's silent acquiescence as indication The Home Depot bears no objections to third-party disclosure.

126. The March 7 Letter also included a number of important enclosures, including:

- a. A document entitled "Initial Public Disclosure" which was the HD Employee's eight-page, technical, step-by-step explanation of the security vulnerability;
- b. Copies of Home Depot's Data Loss Prevention Policy, Data Loss Prevention Standards, Employee "Data Loss Prevention" FAQ, and the company's "Information Classification and Control Standard," all of which the HD Employee was attempting to comply with by notifying superiors of the security vulnerability;
- c. A screen shot showing the HD Employee's ability to capture the log information of the device belonging to Home Depot CEO Francis Blake;

- d. The computer source code needed to aid an attacker to breach Home Depot's systems; and
- e. A compact disk including two videos showing the HD Employee providing a step-by-step walk through of the security vulnerabilities.

127. The letter and package was again signed for and received by a representative of Home Depot in Atlanta, Georgia. But this time, several days later, the HD Employee received a telephone call from a member of Home Depot's legal department ("HD Legal Representative") acknowledging receipt of the employee's letter and package.

128. The HD Legal Representative asked for clarification as to whether a potential attacker needed a user name of his or her own in order to access Home Depot's system, to which the HD Employee replied "no," that no credentials were required on the attacker's behalf, only physical access to any Home Depot computer. The HD Legal Representative expressed shock to this response. The HD Legal Representative stated that the Senior Director of IT was reviewing the information provided by the HD Employee and that IT personnel would reach out to the employee shortly thereafter.

129. The HD Employee explained that this was the employee's third attempt to communicate the seriousness of the issue to Home Depot, and that the

employee had previously sent multiple letters via certified mail and provided complete details as to how to accomplish the attack, including providing the source code that would aid an attacker. The HD Employee stressed the sensitivity of the information and that, upon review by IT personnel, it should be readily apparent that something is “very, very wrong.” The HD Legal Representative thanked the HD Employee for the employee’s cooperation.

130. Other than a minor change to the Microsoft Windows mobile registry software affecting password transparency (the change obscured the last character typed when entering a password, making it more difficult to gain a user’s password by looking over their shoulder, but not preventing any of the other numerous ways to gain login information), Home Depot did not correct the fundamental security vulnerability allowing access to its systems identified by the HD Employee.

131. Rather than heed the HD Employee’s explicit warnings, which were accompanied by supporting data, step-by-step examples and precise explanations as to the nature and source of the threats, Home Depot instead terminated the HD Employee’s employment under the pretense of an unrelated policy violation.

132. The decision of Home Depot to ignore a blatant security threat which permitted attackers to not only enter its systems, but then navigate the systems undetected to gain access to customer payment information *after being explicitly warned of the threat*, epitomized Home Depot’s cavalier attitude toward data



security, and served as an ominous precursor to the massive data breach Home Depot experienced through similar means just over three years later.

**Home Depot's Employees Confirm Data Security Failures**

133. Interviews conducted with former Home Depot IT personnel and security employees, including investigations conducted by *The New York Times*, *Bloomberg Business*, and *The Huffington Post*, confirm that Home Depot's lack of concern with data security was a serious problem and major source of tension within the company in the years leading up to the data breach. According to these reports:

- a. Home Depot managers failed to take seriously security threats and "red flags" raised by its employees;
- b. Home Depot managers relied on outdated antivirus software and did not continuously monitor the network for unusual behavior, including unusual activity at its checkout registers;
- c. Home Depot irregularly performed vulnerability scans on its computer systems inside its stores and often scanned only a small number of stores;
- d. More than a dozen Home Depot systems handling customer information were not regularly assessed or scanned for

vulnerabilities and were off limits to much of the security staff;  
and

- e. Despite alarms as far back as 2008, Home Depot was slow to respond to early cybersecurity threats and started taking action only after it was already too late.

134. The blame for many of data security issues described above can be placed squarely on the shoulders of Home Depot's management. First, despite maintaining two large data and technology centers in Atlanta, Georgia and Austin, Texas, Home Depot's IT security department was woefully understaffed. Home Depot rarely employed more than 50 or 60 IT security personnel at any given time (and oftentimes less than half that number), instead outsourcing work to "security consultants" and requesting undertrained staffers to accept projects outside their scope of expertise. Companies comparable in size to Home Depot typically employ hundreds or thousands of IT employees.

135. From the top of the company down, Home Depot made a series of baffling hires to serve in leadership positions within the company's IT security department. As mentioned above, Home Depot hired Matthew Carey as Chief Information Officer in 2008. Although he received an annual compensation package routinely exceeding \$3 million, Mr. Carey's primary background and focus was on IT infrastructure and software development, not data security. In the

years after his hiring, it became clear that Mr. Carey's only interest in data security was using it as a cost-cutting measure.

136. In 2009, Matthew Carey hired Jeff Mitchell as an IT enterprise architect at Home Depot, one year after he was fired as the director of IT security and architecture by Lowe's Home Improvement. In August of 2011, Jeff Mitchell was promoted to Senior Director of IT Security and served in the role of Chief Information Security Officer (CISO) after the departure of former CISO, Tammy Moskites. At all times relevant herein, Jeff Mitchell maintained offices in Atlanta, Georgia and made all decisions relating to Home Depot's IT and data security from Atlanta, Georgia.

137. Former employees described Jeff Mitchell as "bullying" and "abrasive." After his promotion, Jeff Mitchell shelved numerous IT data security projects that had been under development for extensive periods in order to cut expenses and minimize disruptions across the network. Jeff Mitchell's management style was so polarizing that within three months of his promotion, approximately half of Home Depot's 60 IT security employees had left the company.

138. The departures included a number of employees tasked with finding security flaws in Home Depot's network and ensuring that Home Depot was compliant with industry security standards. For the remaining staffers, their

workload increased and constant employee turnover made their jobs extremely difficult to perform. As noted by one former IT security engineer, “You’re having a hard enough time finding security holes, then half the people in your department leave and your workload doubles. It makes it even harder to catch stuff.”

139. In early 2012, the entire (remaining) IT security staff of approximately 30 individuals held a meeting with Home Depot’s HR leaders and Matthew Carey in a company boardroom to raise their concerns about Jeff Mitchell’s management style and carelessness regarding IT security and the lack of qualified staffing to handle the company’s extensive IT security needs. Matthew Carey dismissed the claims against Mitchell, informing the employees that cost-cutting was a necessity within the department, and made no changes to the department he was paid millions to oversee.

140. In fact, former employees referred to Jeff Mitchell as Matthew Carey’s “enforcer” and believed Mitchell was actually acting at the direction of Carey in cutting a number of necessary security programs and protocols implemented by the former regime. Many employees felt that Matthew Carey was the root of the problem by continuously ignoring issues raised by staffers.

141. Former IT security managers stated that when they attempted to make improvements or suggest upgrades to Home Depot’s security systems, they were routinely rejected by Jeff Mitchell and Home Depot’s IT executives. For example,

prior to Mitchell's promotion, Home Depot maintained an IT security team dedicated to installing security "patches" within the company's computer systems. Patches are pieces of critical software used to update a computer program in order to fix bugs or address security vulnerabilities. After his promotion, Mitchell no longer prioritized the installation of security upgrades and "things just fell between the cracks." Employees attributed this to a lack of qualified staffers and Jeff Mitchell's directives to put cost savings in front of data security for even the most basic of security measures.

142. Home Depot security executives, including Jeff Mitchell, exacerbated the employees' concerns by refusing to approve upgrades to software and shelving major security projects implemented by former CISO Tammy Moskites. As a cost-cutting measure, Mitchell badgered IT security staffers to eliminate certain security features previously deployed under Moskites, replacing them with weaker or no alternatives.

143. The first security project shelved by Jeff Mitchell was implementation of the "Symantec Control Compliance Suite," which was software designed to automate the assessment of technical controls and security configuration standards to ensure a consistent, centralized approach to evaluating security compliance status across all company systems. This would have allowed Home Depot to replace tedious, manual security checks with frequent, automated assessments of

key IT risk and compliance management tasks. In response to staffers' many requests to implement the important system, Jeff Mitchell stated, "We will get to it when we get to it" or "Matt [Carey] said to leave it alone."

144. Jeff Mitchell also shelved a project designed to provide better protection for "privileged accounts" within the company. Home Depot had a four-year relationship with Israel-based IT security company Cyber-Ark Software Ltd., which is a provider of IT security software designed to better protect from infiltration high-level accounts with access to company servers, routers, databases and infrastructure. Despite the fact that Home Depot IT security employees had devoted months of time to working on the project and Home Depot had already paid for the Cyber-Ark Software licensing fees, Home Depot abandoned the project at the direction of Jeff Mitchell.

145. One specific area of concern for Home Depot's IT employees was the lack of point-of-sale encryption in Home Depot's systems. In early 2011, with Tammy Moskites still serving as CISO, the IT security department was working on a project to fully encrypt data processed at Home Depot stores throughout the payment card cycle. Specifically, when a card was swiped at a Home Depot point-of-sale terminal, the payment card data was visible in clear text (and thus vulnerable) while being sent to Home Depot's main servers. The project implemented by Moskites would have encrypted information at the point-of-sale so

that even if the information was siphoned off moments after it is swiped, it would be virtually useless to hackers. Shortly after taking over, Jeff Mitchell terminated this essential project.

146. Prior to Jeff Mitchell's promotion, Home Depot also required a Memorandum of Records and Requirements ("MORR") assessment for every IT product that Home Depot considered implementing. The MORR assessment was an approximately 30-page memorandum that documented potential security risks the product was designed to prevent. If the potential security risks were high, then Home Depot required upper-level management to approve purchase of (or passing on) the product. Once Jeff Mitchell took over as CISO, the company stopped performing MORR assessments.

147. Home Depot also maintained what was known as a "Security Review Board" comprised of several IT employees within the company who met regularly in Atlanta, Georgia. The purpose of the Security Review Board was to allow IT employees to periodically make security recommendations and discuss ongoing projects that would then be approved or rejected by the board. While Matthew Carey and Jeff Mitchell were not on the Security Review Board, the board could only act at their direction. In addition, any time the board rejected a proposed security measure, Matthew Carey was required to personally "sign off" on the

board's decision indicating that he was aware an "exception" was being made to customary security protocols.

148. Home Depot IT security personnel recommended to the Security Review Board implementation of point-of-sale encryption across all Home Depot stores. But the board rejected the proposal at the direction of Carey and Mitchell, noting that it would "address the concerns again in the future." Although Home Depot had the capability to implement point-of-sale encryption, and had taken preliminary steps to do so under Tammy Moskites, Home Depot's executives continuously delayed the project citing costs and operational disruptions.

149. After Security Review Board meetings, Jeff Mitchell would routinely question employees who raised concerns with current security protocols or made proposals as to new security measures for "trying to change the environment." With respect to the point-of-sale encryption project, Mitchell routinely told staffers, "it's going to interrupt the business" or "it's more of an expense" than it's worth.

150. According to *The Huffington Post* investigation, "Over three months in the spring of 2013, four of the eight people responsible for ensuring that credit card data was encrypted as it traveled through Home Depot's computer network left the company, continuing a pattern of high turnover and turmoil that former employees said had persisted since late 2011. The four left in part because they



were frustrated that management did not address their security concerns.” A former employee stated that he had raised “red flags” with Home Depot management about the lack of encryption, but management did not address his concerns. According to the former employee, “It was painfully easy to capture that data.”

151. Multiple former managers said Jeff Mitchell told them to settle for “C-level security” (as opposed to “A-level” or “B-level” security) because ambitious upgrades would be costly and might disrupt the operation of critical business systems. Indeed, it was Home Depot’s *unwritten internal company policy* to maintain substandard data security so as to not cut into profits or disrupt daily operations.

152. Former employees believed that IT security at Home Depot was an “afterthought” and “just a check-mark” on management’s list. Given Home Depot’s lack of concern for data security, it is no surprise that one former Home Depot IT security employee “went so far as to warn friends to use cash, rather than credit cards, at the company’s stores” in the months before the data breach.

153. Matthew Carey and Jeff Mitchell were not Home Depot management’s only questionable hires in the years leading up to the data breach. In July of 2012, Home Depot hired Ricky Joe Mitchell (no relation to Jeff Mitchell) as an IT security engineer responsible for security engineering and IT architecture within the company. Upon acceptance of the job, Ricky Joe Mitchell moved from

Charleston, West Virginia to Atlanta, Georgia. The following year, Ricky Joe Mitchell was promoted by Jeff Mitchell to Senior Architect for IT Security at Home Depot and was in charge of IT security, access management projects, and IT security engineering and architecture across all of Home Depot.

154. In June of 2012, just one month before he was hired by the Home Depot, Ricky Joe Mitchell had been fired as a network engineer by his former employer, an oil and gas company called EnerVest Operating. In July of 2013, two months after he was promoted by Home Depot, Ricky Joe Mitchell was indicted on federal charges for intentionally sabotaging his former company's computer servers.

155. Ricky Joe Mitchell's indictment asserted that he knowingly accessed a protected computer without authorization, erased backup information, and disabled a data replication process designed to transmit backup data. Ricky Joe Mitchell was also alleged to have deleted all of the EnerVest Operating's phone system accounts, extensions, and accounting data. The company was unable to conduct business for a month and lost significantly in excess of \$1 million because of Ricky Joe Mitchell's actions. After pleading guilty in January of 2014, Ricky Joe Mitchell was sentenced to four years in federal prison.

156. Home Depot did not bother to conduct even rudimentary due diligence prior to hiring and promoting an employee responsible for protecting the

data security of millions of Home Depot's customers. If it had, the company would have learned that Ricky Joe Mitchell left his prior employer on negative terms and had a history of destructive behavior, including having been suspended from his high school for attempting to plant viruses in his school's computer system, and threatening the students he believed reported his actions. The incident was even the subject of public court filings that ultimately reached the West Virginia Supreme Court.

157. By 2013, ineffective management and leadership had effectively driven off the majority of Home Depot's IT security employees due to their ongoing frustration with Home Depot's lack of concern for data security. In fact, Symantec, one of Home Depot's top security vendors, told Jeff Mitchell that even it would stop working for Home Depot unless Home Depot took security more seriously. The frustrations of employees and third-party security vendors were perhaps best epitomized by a phrase they often heard from CIO Matthew Carey in response to requests for new software and training: "We sell hammers."

**Pre-Breach: July 2013-March 2014**

158. There were several internal incidents that should have put Home Depot on high alert about the potential for an impending company-wide data breach. According to the *Bloomberg Business* investigation, on July 25, 2013, a data-stealing virus at a Home Depot in Denton, Texas spread to at least eight of the

store's registers. This incident may have signaled that hackers were testing the security of Home Depot's point-of-sale systems.

159. On October 1, 2013, IT security consultant FishNet Security prepared a report for Home Depot regarding its data security providing that the company's computer systems were vulnerable because Symantec's Network Threat Protection ("NTP") firewall had been shut off in favor of one packaged with Microsoft Windows. According to *Bloomberg*, the report stated that, "It is highly advised and recommended the NTP Firewall component be deployed and that Windows Firewall be discontinued" and in order for intrusion prevention to work properly, "NTP was needed on all Home Depot computers, including register payment terminals." Home Depot ignored this warning and chose not to deploy the essential theft prevention components on its point-of-sale terminals.

160. Further, Home Depot insisted on maintaining out-of-date antivirus software from 2007 known as Symantec Endpoint Protection 11 on its point-of-sale systems. In 2011, Symantec released an updated version of the software, Endpoint Protection 12, stating in a news release that the "threat landscape has changed significantly" and that the newer product would protect against the "explosion in malware scope and complexity." But despite warnings and pleas from Home Depot security employees to upgrade to the newer antivirus software, which had the capacity to "detect sophisticated new threats earlier and more

accurately than any other security product,” Home Depot refused to purchase and install the upgrade.

161. Home Depot also declined to use essential features in its *existing* software. As reported by *Bloomberg Business*, Home Depot failed to even *turn on* a key intrusion-prevention feature included in its existing antivirus software:

Internal Home Depot documents show the Atlanta-based retailer had chosen to keep the extra security measure deactivated even though it was designed specifically to spot the kind of malicious software that attacks systems’ endpoints, like the registers that were hit at Target, Michaels (MIK), Neiman Marcus, and others.

\*\*\*

It’s unclear why Home Depot resisted activating the intrusion prevention feature in its software suite, a Symantec (SYMC) product called Endpoint Protection. The internal documents suggest the program sometimes generated false positives. Two information security managers who previously worked for Home Depot say their supervisor told them to minimize costs and system downtime at the expense of improving security. They and three other former employees, who requested anonymity because they fear retribution, say the information security department has struggled with employee turnover and old software for about three years.

162. In December of 2013, Home Depot discovered that point-of-sale terminals at a store in Columbia, Maryland store were infected with malware known as “Infostealer.” Infostealer is malware installed on point-of-sale devices to siphon payment card data and then forward that information to a remote location. It is exactly the type of malware that the Symantec NTP firewall component, which Home Depot chose not to deploy, is designed to block.

163. In February of 2014, FishNet again issued a report to Home Depot urging it to deploy Symantec NTP on its point-of-sale devices in order to strengthen its defenses against a data breach. Again, Home Depot ignored these warnings. Former employees report that as of April 2014, when attackers first infiltrated Home Depot's point-of-sale systems, Home Depot still had not discontinued the vulnerable Microsoft Windows firewall in favor of Symantec's secure NTP firewall.

164. One major area of concern at Home Depot's U.S. stores was a lack of sufficient bandwidth to extract point-of-sale log files from the stores' servers to Home Depot's main offices in Atlanta, Georgia to be reviewed by IT security staffers in order to look for any potential abnormalities or malware deployed by hackers (commonly known as "security event logs"). Matthew Carey and Jeff Mitchell were repeatedly told by IT staffers about the bandwidth issue for U.S. stores and warned that critical files, including "security event logs," were not being reviewed. Matthew Carey repeatedly ignored staffers' pleas to upgrade stores' bandwidth or implement "accelerators," which would collapse the size of the respective files to allow for information sharing with corporate IT security, because such corrective measures would be costly to the company.

165. Despite the numerous internal warnings outlined above, Home Depot's first urgent wake-up call relating to data security came from a well-

publicized data breach suffered by the nation's second largest retailer, Target Corporation, in December of 2013. There, hackers used the credentials of a third-party vendor to install data-stealing malware into Target's in-store cash registers via remote upload over the Target network.

166. At the time, the Target data breach was the largest retailer data breach in U.S. history, with hackers stealing the debit and credit card information of 40 million individuals, and the names, e-mail and mailing addresses and phone numbers of an additional 70 million individuals. The Target data breach received worldwide attention and put the entire retail industry on notice that lax IT security would be exploited on a massive scale.

167. In the weeks following the Target data breach, Home Depot executives, led by CEO Francis Blake, assembled a task force in Atlanta, Georgia to make recommendations on how to avoid a similar fate. Knowing of Home Depot's unwritten internal policy to implement "C-level security," Mr. Blake requested CIO Matthew Carey and IT personnel working under his direction to prepare a report explaining how to block hackers from infiltrating the company's servers and making recommendations as to necessary security upgrades. The task force was also charged with forming a "playbook" on how to respond to a data breach if one did in fact occur.

168. In or about February of 2014, the task force made a series of recommendations, most of which had been *previously proposed to and rejected by* Matthew Carey and the Home Depot IT security executives for years. Among others, the recommendations included:

- a. Implementing stronger security-threat detection software;
- b. Upgrading the company's security operations center;
- c. Purchasing intelligence feeds on hacker behavior;
- d. Installing regularly-updated security "patches";
- e. Upgrading software on the company's point-of-sale terminals; and
- f. Implementing encryption for debit and credit card data in the stores' point-of-sale terminals.

169. Indeed, the recommendations made by the task force almost directly mirrored recommendations made by Home Depot's IT security staffers and outside security consultants for years.

170. Point-of-sale encryption is generally viewed as the strongest line of defense to thwart a retailer-based data breach. Encryption works in the following manner: In a debit or credit card purchase transaction, card data must flow through multiple systems and parties to be processed. Generally, the cardholder presents a payment card to a retailer to pay for merchandise. The card is then "swiped" and information about the card and the purchase is stored in the retailer's computers



and then transmitted to the acquirer (*i.e.*, the retailer's bank). The acquirer relays the transaction information to the payment card company, who then sends the information to the issuer (*i.e.*, cardholder's bank). The issuer then notifies the payment card company of its decision to authorize or reject the transaction.

171. There are two points in the payment process where sensitive cardholder data is at risk of being exposed or stolen: *pre-authorization* when the merchant has captured a consumer's data and it is waiting to be sent to the acquirer; and *post-authorization* when cardholder data has been sent back to the merchant with the authorization response from the acquirer, and it is placed into some form of storage in the merchant's servers.

172. In the Target data breach, for example, the hackers collected customers' card information pre-authorization by installing malware on Target's point-of-sale registers and collecting the information the moment each card was swiped. The stolen data was then automatically sent from each register to one of three "staging points," or secret locations installed on Target's network where the hackers temporarily stored the data before retrieving it off of Target's systems.

173. Encryption mitigates security weaknesses that exist when cardholder data has been stored, but not yet authorized, by using algorithmic schemes to transform plain text information into a non-readable format called "ciphertext." By scrambling the payment card data the moment it is swiped, hackers who steal the

data are left with useless, unreadable text in the place of debit and credit card numbers accompanying the cardholder's personal information.

174. Prior to the Target breach, encryption of payment card data at point-of-sale terminals had been recommended to and rejected by Home Depot executives by IT security employees and third-party consultants for close to six years. Jeff Mitchell shelved the enhanced encryption project implemented by his predecessor and Matthew Carey explicitly rejected implementing point-of-sale encryption after it was recommended to the Security Review Board. As a result, in the spring of 2013, half of the Home Depot employees responsible for ensuring credit card data was encrypted at later points in the payment card transaction process quit the company out of frustration that management would not address their security concerns.

175. Home Depot CEO Francis Blake finally gave the green light to implement encryption technology at point-of-sale terminals in all U.S. Home Depot stores. But by the time Home retained and finalized negotiations with a vendor to start the project several months later, hackers were already deep in Home Depot's systems.

#### **The Home Depot Data Breach: April to September 2014**

176. In or around April of 2014, hackers gained access to Home Depot's systems by using the credentials of a third-party vendor. Once inside Home

Depot's systems, the hackers were able to "jump the barriers" between a peripheral third-party vendor system and the company's main computer network.

177. According to a report by the *Wall Street Journal*, the hackers were able to enter the company's main computer network by exploiting a vulnerability in Microsoft Window's operating system. Although Home Depot installed a patch to fix the vulnerability after the breach began, it was too late. Once inside Home Depot's main computer network, the hackers were able to "elevate" their credentials to act like Home Depot employees with high-level permissions in order to navigate Home Depot's systems undetected.

178. The hackers were then able to navigate to Home Depot's point-of-sale systems and target 7,500 of the company's self-checkout lanes because they were identified as payment terminals within Home Depot's systems. The standard cash registers (mainline payment terminals staffed by Home Depot employees), by contrast, were identified only by number, likely making them more difficult for the hackers to locate.

179. After locating the self-checkout registers, the hackers installed malware that operated similarly to the malware used in the Target data breach. Specifically, the malware was designed to siphon off credit and debit card information the moment it was swiped on Home Depot's self-checkout terminals, and then transmit that information to a remote location outside of Home Depot's

systems. The hackers managed to evade detection by navigating the computer systems during regular business hours and designing the malware to erase its tracks after completing designated tasks.

180. That same month in April 2014, unaware that hackers had already exploited gaping holes in its security systems, Home Depot's data breach task force was putting the finishing touches on a 45-page "playbook" about how to respond to a data breach if one did occur. The playbook included media talking points, sample letters to customers and law enforcement, and task lists outlining responsibilities of Home Depot executives. "The irony was not lost on us," admitted Home Depot CEO Francis Blake in the months following the breach.


181. In July of 2014, Home Depot contracted Symantec to perform a "health check" on Home Depot's computer systems. The health check identified as critical issues the same issues to which Home Depot IT employees had alerted superiors months prior: that Home Depot was using out-of-date antivirus software and malware detection systems on its point-of-sale terminals.

182. Had Home Depot upgraded its software when first recommended by Home Depot's own IT security employees, the data breach could have been detected immediately, if not altogether prevented. Instead, the hackers were able to navigate Home Depot's systems undetected for approximately six months while

stealing the debit and credit card information of tens of millions of Home Depot customers.

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

184. On September 2, 2014, stolen card numbers were offered for sale in two batches under the name “American Sanctions” on the Rescator website. Security blogger Brian Krebs of Krebs on Security broke the news that multiple banks were seeing evidence of fraud on customer accounts with the common link being purchases at Home Depot.

[USA & WORLD UPDATE!](#) /  02 SEPTEMBER 2014 / COMMENTS:

## **USA & World Dumps update!**

Base name: **European Sanctions**

Valid rate of: 100%

No replacements!

Base name: **American Sanctions 1, 2**

Valid rate of: 100%

Track 1, Track 2, State/zip. No replacements!

**MoneyGram** is faster and works on Saturday!

*Source: Krebs on Security*

185. That same day, Home Depot's banking contacts and law enforcement officials alerted Home Depot executives that the company's computer systems had likely been breached. Matthew Carey, Home Depot's CIO, was vacationing in Mexico when he got word that the U.S. Secret Service had linked the stolen cards to Home Depot. Home Depot's treasurer, Dwaine Kimmet, received a similar call from an analyst at Capital One Financial Corp. If not for the massive online sale of customer card data, Home Depot's data breach may not have been discovered until much later.

186. Rather than confirm the data breach, however, Home Depot issued a self-serving statement buried on its corporate website noting that the company was "looking into some unusual activity" and touting how seriously it takes the protection of customers' information.

187. The Rescator website indexed and let customers sort stolen card numbers by card type (debit, credit, platinum credit, etc.), issuing bank, expiration date, last four digits of the card number, and city, state and ZIP code of the Home Depot store from which each card was stolen.

Source: Bloomberg Business

	VISA	DEBIT	PLATINUM	10/17	Yes	101	United States, NY, Rochester, 14623	BANK OF AMERICA N.A.	American Sanctions 1	52.5\$
	VISA	DEBIT	PLATINUM	05/15	Yes	101	United States, IA, Bettendorf, 52722	WELLS FARGO BANK N.A.	American Sanctions 1	52.5\$
	VISA	DEBIT	BUSINESS	05/16	Yes	101	United States, PA, Hanover, 17331	MEMBERS 1ST F.C.U.	American Sanctions 1	52.5\$
	VISA	DEBIT	PLATINUM	04/17	Yes	101	United States, CO, Littleton, 80129	WELLS FARGO BANK N.A.	American Sanctions 1	52.5\$
	VISA	DEBIT	CLASSIC	01/16	Yes	101	United States, WI, Green Bay, 54303	ITS BANK	American Sanctions 1	22.5\$
	VISA	CREDIT	SIGNATURE	10/16	Yes	101	United States, CA, Mission Viejo, 92692	CAPITAL ONE BANK (USA) N.A.	American Sanctions 1	42.01\$

Dump or cc of this particular bank (BIN)

Source: Krebs on Security

188. Including the location of the Home Depot store from which each card was stolen was valuable information for card purchasers. As explained by Krebs:

The ZIP code data allows crooks who buy these cards to create counterfeit copies of the credit and debit cards, and use them to buy gift cards and high-priced merchandise from big box retail stores. This information is extremely valuable to the crooks who are purchasing the stolen cards, for one simple reason: Banks will often block in-store card transactions on purchases that occur outside of the legitimate cardholder's geographic region (particularly in the wake of a major breach).

Thus, 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.

189. According to *Bloomberg Business*, these two batches of “American Sanctions” cards sold for between \$50 to \$100 per card and claimed a 100% validity rate, meaning that the cards numbers were valid and working. Specialty cards including “platinum” and “business” credit cards commanded higher prices, while debit cards generally sold for less. The Rescator website, praised by cybercriminals for its customer service and ease of use, even temporarily crashed because it received so many hits.


190. On September 3, 2014, Brian Krebs, not Home Depot, reported that new evidence suggested nearly all U.S. Home Depot stores were affected by the massive data breach. By comparing the ZIP code data available on the Rescator website to the ZIP code locations of Home Depot stores, Krebs was able to establish “a staggering 99.4 percent overlap”—all but confirming that Home Depot



was the source of the data breach and that Home Depot stores across the country were involved. Despite this overwhelming evidence, Home Depot still did not publicly disclose its systems had been breached.

191. On September 4, 2014, Home Depot's CEO Francis Blake spoke publicly for the first time about the breach in addressing investors. Mr. Blake would not confirm that the breach actually took place, but claimed the company was communicating facts as they became known. By this time, Home Depot's security consultants had acquired batches of card numbers from the Rescator website and began visiting stores in Atlanta, Georgia and Austin, Texas to try to determine usage patterns. Home Depot still did not publicly disclose its systems had been breached.

192. On September 4, 2014, three additional batches of stolen card numbers were made available on the Rescator website. Because Home Depot had not yet confirmed the breach, however, financial institutions were reluctant to issue replacement cards, which resulted in the new batches still claiming a 100% validity rate.

[USA DUMPS UPDATE!](#) /  04 SEPTEMBER 2014 / COMMENTS:

## **USA Dumps update you asked for!**

**Base name: American Sanctions 5**

**Valid rate of: 100%**

**Track 1, Track 2, State/Zip. No replacements!**

**Base name: American Sanctions 4**

**Valid rate of: 100%**

**Track 1, Track 2, State/Zip. No replacements!**

**Base name: American Sanctions 3**

**Valid rate of: 100%**

**Track 1, Track 2, State/Zip. No replacements!**

*Source: Krebs on Security*

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

194. On September 7, 2014, seven additional batches of stolen card numbers were made available on the Rescator website, resulting in a massive uptick in debit and credit fraud for Home Depot customers. But again, because Home Depot had not yet confirmed the breach, financial institutions were reluctant to preemptively issue replacement cards. As such, the new batches continued to claim a 100% validity rate.

[EVEN MORE USA DUMPS UPDATED](#) /  07 SEPTEMBER 2014 / COMMENTS:

## **Even more USA Dumps updated!**

Base name: **American Sanctions 6, 7, 8, 9**

Valid rate of: 100%

*Track 1, Track 2, State/Zip. No replacements!*

Base name: **American Sanctions 10, 11, 12**

Valid rate of: 100%

*Track 1, Track 2, State/Zip. No replacements!*

*Source: Krebs on Security*

195. Also on September 7, 2014, Krebs reported that the malware used in the Home Depot data breach was a variant of the “BlackPOS” malware strain used in the Target breach, both designed to siphon card data the moment it is swiped at a point-of-sale terminal. Krebs noted that, “Clues buried within this newer version of BlackPOS support the theory put forth by multiple banks that the Home Depot breach may involve compromised store transactions going back at least several months.” Compared to Target, the malware had an enhanced capability to capture card data from the physical memory of infected point-of-sale devices and disguise itself as a component of the antivirus product running on the system.

196. On September 8, 2014, six full days after the data breach was first made public, Home Depot finally broke its silence and issued a news release buried on its website that its computer systems had been breached. The news release feebly confirmed that the breach was widespread, potentially impacting any person who used a payment card at a U.S. or Canadian Home Depot store since

April of 2014, but utterly failed to capture the severity of the breach or provide customers with any other relevant information.

197. In fact, Home Depot's September 8, 2014 news release was simply an attempt to downplay the severity of the incident rather than serve as an explicit warning to customers that their personal and financial information was currently *for sale and being purchased by criminals* around the world. Indeed, the release offers several "reassuring" anecdotes that:

- a. "There is no evidence that the breach has impacted stores in Mexico or customers who shopped online at HomeDepot.com";
- b. "While the company continues to determine the full scope, scale and impact of the breach, there is no evidence that debit PIN numbers were compromised";
- c. "[T]he company has taken aggressive steps to address the malware and protect customer data. The Home Depot is offering free identity protection services, including credit monitoring, to any customer who used a payment card at a Home Depot store in 2014, from April on";
- d. "It's important to emphasize that no customers will be responsible for fraudulent charges to their accounts";

- e. “[T]he company’s internal IT security team has been working around the clock with leading IT security firms, its banking partners and the Secret Service to rapidly gather facts and provide information to customers”; and
- f. “Responding to the increasing threat of cyber-attacks on the retail industry, The Home Depot previously confirmed it will roll out EMV ‘Chip and PIN’ to all U.S. stores by the end of this year, well in advance of the October 2015 deadline established by the payments industry.”

198. Customers who actually stumbled across Home Depot’s uninformative and self-serving news release would read a statement from Home Depot that contained numerous material omissions:

- a. Home Depot failed to include the source of the breach or provide a general description of the nature of the security breach;
- b. Home Depot failed to include the number of payment cards compromised;
- c. Home Depot failed to include how many individuals were affected;
- d. Home Depot failed to include *what customer information* was actually compromised (even though it was for sale on the Internet

and Home Depot even purchased such information from Rescator);

and

- e. Home Depot failed to include whether the threat was ongoing or whether it was safe to continue using payment cards at Home Depot stores.

199. Home Depot should have confirmed that the data breach exposed not only the customer's payment card data, including credit and debit card numbers, expiration dates, and three-digit security codes, but also the customer's personally-identifiable information, including the customer's name, mailing address, and in many cases, phone number and e-mail address. By withholding this information, Home Depot failed to put its customers on notice that they could be subject to a wide-range of potential fraud *in addition to* experiencing unauthorized charges.

200. In addition, Home Depot's completely irrelevant anecdote that "it will roll out EMV 'Chip and PIN' to all U.S. stores by the end of this year" was of no benefit to its customers. It is well-documented that this technology has existed since the early 1990s and has been in widespread use throughout the world for close to 10 years. The purpose of the technology is to replace the magnetic strip on credit and debit cards with an embedded microchip that stores and transmits encrypted data and is authenticated using a PIN number, making the cards more difficult to counterfeit. In 2011, major credit card companies including MasterCard

and Visa *required* merchants to convert to this technology by October 15, 2015, or otherwise accept liability for fraud going forward. The fact that Home Depot was rolling out this project several months ahead of schedule (but had not done so yet) was of no benefit to the millions of customers who were at imminent risk of harm by way of Home Depot's inadequate security.

201. While Home Depot purported to offer its customers a year of free credit monitoring, the vast majority of Home Depot customers were not made aware of this offer, or if they were, experienced difficulties attempting to sign up. Moreover, credit monitoring is of no actual value to customers as a preventative measure because it is reactionary—it does nothing to prevent fraud in the first instance. As noted by Krebs:

Please note that credit monitoring services will not help with [the task of preventing or discovering unauthorized charges], as they are not designed to look for fraud on existing accounts tied to your name and personal information. As I've noted in several stories, credit monitoring services are of dubious value because although they may alert you when thieves open new lines of credit in your name, those services do not prevent that activity. The one thing these services *are good for* is in helping identity theft victims clean up the mess and repair their good name.

202. Prior to the Home Depot breach, the *Chicago Tribune* published an article entitled, "Why credit monitoring will not help you after a data breach." The article noted that retailers offering credit monitoring services and instructing their customers to check their credit reports in the wake of a data breach is "bad advice"

because “[p]ayment card breaches have nothing to do with credit reports.” As one security expert noted, offering credit monitoring “seems to be the knee-jerk reaction” after a breach but “makes no sense at all.” The biggest concern is that credit monitoring offers customers a false sense of security but in reality offers little protection once the customer’s personal information is exposed.

203. Despite having prepared a data breach response “playbook” for this exact purpose months earlier, Home Depot’s delayed and incomplete notification of the breach was widely criticized by security experts. As noted by one expert, “Home Depot is in trouble here . . . . This is not how you handle a significant security breach, nor will it provide any sort of confidence that Home Depot can solve the problem going forward.”

204. On the same day as Home Depot’s confirmation, Krebs reported that “multiple financial institutions” were “reporting a steep increase over the past few days in fraudulent ATM withdrawals on customer accounts.” On its face, this would seem at odds with Home Depot’s statement that debit PIN numbers were not compromised. But, as Krebs explained, purchasers of the stolen card information had enough of the cardholder’s personal information available to fabricate *new PIN numbers* for stolen debit cards:

The card data for sale in the underground that was stolen from Home Depot shoppers allows thieves to create counterfeit copies of debit and credit cards that can be used to purchase merchandise in big box stores. But if the crooks who buy stolen debit cards also are able to



change the PIN on those accounts, the fabricated debit cards can then be used to withdraw cash from ATMs.

Experts say the thieves who are perpetrating the debit card fraud are capitalizing on a glut of card information stolen from Home Depot customers and being sold in cybercrime shops online. Those same crooks also are taking advantage of weak authentication methods in the automated phone systems that many banks use to allow customers to reset the PINs on their cards.

Here's the critical part: The card data stolen from Home Depot customers and now for sale on the crime shop Rescator[dot]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 (presumably by malware installed on some part of the retailer's network, and probably on each point-of-sale device).

*This is especially helpful for fraudsters since most Home Depot transactions are likely to occur in the same or nearby ZIP code as the cardholder.* The ZIP code data of the store is important because it allows the bad guys to quickly and more accurately locate the Social Security number and date of birth of cardholders using criminal services in the underground that sell this information.

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.

205. With this valuable information, purchasers of the stolen card information had countless methods of fraud at their disposal. Indeed, information pertaining to the cardholder's location allows fraudsters to obtain a cardholder's social security number and date of birth, further increasing the risk of identity theft for affected Home Depot customers. Krebs gave several real-life examples in the wake of the data breach:

On Thursday, I spoke with a fraud fighter at a bank in New England that experienced more than \$25,000 in PIN debit fraud at ATMs in Canada. The bank employee said thieves were able to change the PINs on the cards using the bank's automated VRU system. In this attack, the fraudsters were calling from disposable, prepaid Magic Jack telephone numbers, and they did not have the Cv2 for each card. But they were able to supply the other three data points.

KrebsOnSecurity also heard from an employee at a much larger bank on the West Coast that 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. The manager said the bad guys called the customer service folks at the bank and provided the last four [digits] of each cardholder's Social Security number, date of birth, and the expiration date on the card. And, as with the bank in New England, that was enough information for the bank to reset the customer's PIN.

The fraud manager said the scammers in this case also told the customer service people they were traveling in Italy, which made two things possible: It raised the withdrawal limits on the debit cards and allowed thieves to withdraw \$300,000 in cash from Italian ATMs in the span of less than 120 minutes.

206. On September 9, 2014, the day after Home Depot confirmed the data breach, Attorneys General in Connecticut, Illinois and California announced their

decision to lead a multi-state investigation into Home Depot's data security practices leading up to the breach. Moreover, senators from Connecticut and Massachusetts wrote a letter to the Federal Trade Commission urging the commission to launch its own investigation into Home Depot's negligent data security practices. Their letter stated, "Online discussions of vulnerabilities on Home Depot's website date back to 2008. These revelations raise serious concerns about Home Depot's responsiveness to potential attacks, particularly in light of other retailers that have recently been targeted by hackers. . . . Given the unprecedented scope and extended duration of Home Depot's data breach, it appears that Home Depot may have failed to employ reasonable and appropriate security measures to protect sensitive personal information."

207. On September 11, 2014, senators from West Virginia and Missouri wrote a letter to Home Depot's CEO Francis Blake requesting that the company "provide a briefing to Committee staff regarding [Home Depot's] investigation and latest findings on the circumstances that may have permitted unauthorized access to sensitive consumer information."

208. On September 18, 2014, Home Depot issued a second news release, this time promoting "a major payment security project" rather than providing its customers with necessary information about the breach. This news release included the following anecdotes:

- a. Home Depot “today confirmed that the malware used in its recent breach has been eliminated from its U.S. and Canadian networks”;
- b. “The company also has completed a major payment security project that provides enhanced encryption of payment data at point of sale in the company’s U.S. stores, offering significant new protection for customers”;
- c. “The company’s ongoing investigation has determined the following: (i) Criminals used unique, custom-built malware to evade detection. The malware had not been seen previously in other attacks, according to Home Depot’s security partners; (ii) The cyber-attack is estimated to have put payment card information at risk for approximately 56 million unique payment cards; (iii) The malware is believed to have been present between April and September 2014.”
- d. “The company’s new payment security protection locks down payment data through enhanced encryption, which takes raw payment card information and scrambles it to make it unreadable and virtually useless to hackers. Home Depot’s new encryption technology, provided by Voltage Security, Inc., has been tested and validated by two independent IT security firms.”

209. The news release also included information clearly geared towards investors, not data breach victims, including “sales growth guidance” and revised “2014 diluted earnings-per-share growth guidance.” Home Depot’s inclusion of complex investor information made it difficult for customers looking for information about the data breach to “separate the wheat from the chaff” regarding the status of their personal and financial data.

210. Home Depot’s second news release again raised more questions than it answered. Specifically, if malware had only been eliminated from Home Depot’s systems as of September 18, then Home Depot had permitted its customers to keep using payments cards at its stores, and continue exposing their personal and financial data, for over two weeks after Home Depot had actual knowledge of the breach.

211. While Home Depot’s second news release also confirmed for the first time that a staggering 56 million Home Depot customers were affected by the data breach, Home Depot again failed to confirm exactly what customer information was compromised, despite having exclusive knowledge of that fact.

212. Moreover, while Home Depot touted its “major payment security project,” enhanced encryption should have been implemented years earlier. The founder of credit card processor Heartland Payment Systems, which suffered its own data breach six years ago, urged retailers in 2009 to adopt “end-to-end

encryption” (meaning that information should be encrypted at all points of the card payment cycle, including at the point-of-sale). This sentiment, echoed by Home Depot IT security employees and outside consultants for many years, was explicitly rejected by Home Depot management on multiple occasions. As noted by one cyber-security expert, “What’s unreasonable is this was a 2014 decision.”

213. Home Depot’s outgoing CEO Francis Blake even admitted that prior to the company’s enhanced encryption upgrade, Home Depot’s computer systems were “desperately out of date.”

214. Additionally, according to the *Wall Street Journal*, on or about September 2, 2014, when Home Depot first became aware its systems may have been breached, Home Depot’s enhanced encryption project (which was recommended by the task force in early 2014 and launched beginning in April), had been rolled out to only 25% of its U.S. stores. Therefore, in approximately 11 days, Home Depot was able to install enhanced encryption in the remaining 75% of its stores, and have it tested and validated by two independent IT security firms. As noted by *Forbes*, “One wonders why, if such steps are so easy to implement, they weren’t put in place earlier.”

215. Given the massive scope of the breach, which was much larger than originally anticipated, Visa Inc. and MasterCard Inc. began alerting thousands of

card-issuing banks to be on the lookout for fraudulent transactions associated with Home Depot.

216. Other details regarding the breach also continued to come to light. For example, Krebs reported that MasterCard informed its card-issuing financial institutions that Home Depot's forensic investigation into the data breach was focusing on the company's self-checkout registers as housing the malware. There was also evidence indicating that the self-checkout registers were running the Windows XPe (Windows XP Embedded) operating system, which was released in 2001 and approaching its end-of-life cycle. Hackers often targeted Windows XPe systems because they are viewed as the most vulnerable systems still in use.

217. *Bloomberg Business* reported that the Home Depot malware was specifically designed to impersonate a McAfee antivirus program in order to avoid suspicion by IT security personnel. Of course, Home Depot did not use McAfee products across its systems, so the presence of a "McAfee"-like program anywhere on its systems should have sounded alarm bells within the company.

218. On November 6, 2014, after a claimed two-month internal investigation, Home Depot released its third and final news release regarding the data breach. For the third time, Home Depot failed to confirm exactly what customer information was compromised. The news release stated in pertinent part:

- Criminals used a third-party vendor's user name and password to enter the perimeter of Home Depot's network. These stolen

credentials alone did not provide direct access to the company's point-of-sale devices.

- The hackers then acquired elevated rights that allowed them to navigate portions of Home Depot's network and to deploy unique, custom-built malware on its self-checkout systems in the U.S. and Canada.
- In addition to the previously disclosed payment card data, separate files containing approximately 53 million e-mail addresses were also taken during the breach. These files did not contain passwords, payment card information or other sensitive personal information. The company is notifying affected customers in the U.S. and Canada. Customers should be on guard against phishing scams, which are designed to trick customers into providing personal information in response to phony e-mails.

219. Home Depot's revelation that the e-mail addresses of 53 million customers were also compromised was a new development relating to the breach. Home Depot attempted to downplay this incident by sending e-mails to some or all of the compromised accounts stating, "In all likelihood this event will not impact you, but we recommend that you be on alert for phony e-mails requesting personal or sensitive information." Home Depot provided no support for its conclusion that the event was not likely to impact customers.

220. Home Depot's admission that hackers "acquired elevated rights" in order to navigate Home Depot's systems and install malware in the point-of-sale terminals was shocking because the HD Employee had explicitly warned Home Depot about this possibility with respect to the First Phones in late 2010. In fact,



had Home Depot taken any number of the security upgrades recommended by the HD Employee, its IT security employees and outside security consultants since 2008, the data breach either would not have been possible, or would have been detected much sooner. These upgrades, each proposed to Home Depot IT executives and explicitly rejected, included:

- a. Fixing security vulnerabilities in Home Depot's computer systems which permitted anyone who gained physical access to a Home Depot computer or the login credentials of third-party vendor or low-level employee to access Home Depot's network and then obtain "elevated" credentials to navigate Home Depot's systems undetected;
- b. Implementing bandwidth accelerators that would have permitted transfer of point-of-sale log files from the stores' servers to Home Depot's data centers so that IT security staffers could review security event logs and discover potential abnormalities or data-stealing malware;
- c. Identifying all payment terminals within Home Depot's systems with coded numbers, making it substantially more difficult for hackers to locate point-of-sale devices to install malware;

- d. Deploying essential theft-prevention components on its point-of-sale terminals by enabling Symantec's NTP firewall component in favor of the more-vulnerable Windows firewall;
- e. Simply *activating* an important, unused intrusion-detection feature of Home Depot's existing antivirus software that would have added a layer of protection to its point-of-sale terminals;
- f. Completing the Cyber-Ark Software Ltd. security project, shelved by Home Depot management, which was designed to better protect high-level accounts with access to company servers, routers, databases and infrastructure;
- g. Completing the "Symantec Control Compliance Suite" project, shelved by Home Depot management, which would have provided automated assessments of key IT security risks and compliance management tasks;
- h. Upgrading Home Depot's out-of-date virus detection software from 2007 when first recommended by Home Depot employees and outside consultants; and
- i. Implementing enhanced point-of-sale encryption technology when first proposed in 2009, rather than after the fact in 2014.

221. These specific failures, among many others, are consistent with Home Depot management's overarching complacency when it came to data security. This included woefully understaffing Home Depot's IT security department, failing to heed the advice of IT security employees and outside consultants, and hiring unqualified individuals to serve in key IT security management positions.

222. Home Depot's data breach notifications were equally deficient. Despite having actual knowledge of the breach on September 2, 2014, Home Depot failed to timely and accurately notify customers of the data breach in the most expedient time possible and without unreasonable delay, sitting idly by for six days as hackers openly sold at least 12 massive batches of Home Depot payment card data and customer information over the Internet. Because of Home Depot's delay in confirming it was the source of the breach, and delay in confirming the period of the data breach, financial institutions were reluctant to preemptively issue replacement cards to customers with Home Depot purchases, resulting in massive numbers of customers suffering fraud between September 2 and September 8, 2014. Additionally, Home Depot allowed its customers to continue using payment cards at its stores between September 2 and September 17, 2014, before the data-stealing malware had been removed from its systems.

223. To date, millions of potentially impacted Home Depot customers have not been adequately notified of the data breach by Home Depot. Home Depot's

“news releases” were buried on its website and may have only reached a small fraction of Home Depot customers. While Home Depot sent e-mail notifications to certain Home Depot customers whose e-mail addresses it had on file, the vast majority of customers were not individually notified of the breach. Importantly, none of Home Depot’s formal news releases have confirmed exactly what customer information was compromised in the breach.

224. In light of these facts, outgoing Home Depot CEO Francis Blake was willing to concede his company’s data security failures: **“If we rewind the tape, our security systems could have been better. Data security just wasn’t high enough in our mission statement.”**

**Home Depot Knew of the Risks Long Before the Target Breach**

225. Even before the Target data breach, Home Depot was well-aware that hackers had been targeting the payment card data of major U.S. companies for many years. Indeed, in the years leading up to the Home Depot breach, companies including Heartland Payment Systems, T.J. Maxx, Sony, eBay, Adobe and JPMorgan Chase were subject to well-publicized data breaches.

226. Each year since 2008, Home Depot has disclosed in its SEC 10-K Form filings and annual reports to shareholders that a “Risk Factor” for Home Depot’s business was suffering a breach of data security. In 2013, the year before the breach, Home Depot disclosed:

***If we do not maintain the privacy and security of customer, associate, supplier or Company information, we could damage our reputation, incur substantial additional costs and become subject to litigation.***

Our business involves the storage and transmission of customers' personal information, consumer preferences and credit card information, as well as confidential information about our associates, our suppliers and our Company. Our information systems are vulnerable to an increasing threat of continually evolving cybersecurity risks. Any significant compromise or breach of our data security, whether external or internal, or misuse of associate or customer data, could significantly damage our reputation, cause the disclosure of confidential customer, associate, supplier or Company information, and result in significant costs, lost sales, fines and lawsuits. While we have implemented systems and processes to protect against unauthorized access to or use of secured data and to prevent data loss, there is no guarantee that these procedures are adequate to safeguard against all data security breaches or misuse of the data. The regulatory environment related to information security, data collection and use, and privacy is increasingly rigorous, with new and constantly changing requirements applicable to our business, and compliance with those requirements could result in additional costs.

227. In August of 2013, more than seven months before Home Depot's systems were breached, Visa sent a letter to Home Depot entitled "Retail Merchants Targeted by Memory-Parsing Malware." The letter warned retailers like Home Depot that, "Since January 2013, Visa has seen an increase in network intrusions involving retail merchants. Once inside the merchant's network, the hacker will install memory parser malware on the Windows based cash register system in each lane." Despite receiving a warning to be on the lookout for the exact type of intrusion that ultimately took place (including exploitation of

vulnerabilities in the Windows operating system), Home Depot did not even begin to take action until after it witnessed what happened to Target.

228. On January 17, 2014, the U.S. Federal Bureau of Investigation (FBI) distributed a confidential, three-page report to Home Depot entitled “Recent Cyber Intrusion Events Directed Toward Retail Firms” describing the risks posed by memory-parsing malware that infects point-of-sale systems. The report stated, “We believe POS malware crime will continue to grow over the near term, despite law enforcement and security firms’ actions to mitigate it . . . . The accessibility of the malware on underground forums, the affordability of the software and the huge potential profits to be made from retail POS systems in the United States make this type of financially motivated cybercrime attractive to a wide range of actors.” Had Home Depot heeded this warning and streamlined its encryption enhancement project immediately (in the manner it did *after* it learned of the breach), the personal and financial information of 56 million individuals would have been unreadable and worthless to hackers.

**Home Depot Was Aware of its Obligation to Protect Customers’ Personal Identity Information and Violated its Own Internal Policies and Standards**

229. In permitting the data breach to occur, Home Depot breached its agreement with customers to protect their personal and financial information and violated its own internal policies and information handling standards.

230. When consumers make purchases at Home Depot retail stores using payment cards, Home Depot collects payment card data related to those cards, including the cardholder's name and the card account number, expiration date, card verification value, and PIN data for debit cards ("PCD"). Home Depot stores PCD in its computer systems and transmits the information to third-parties to complete the payment card transaction process for each purchase. Home Depot also collects and stores customers' personally-identifiable information, including, but not limited to, certain financial information, customer names, mailing addresses, phone numbers, driver's license numbers, and e-mail addresses ("PII") (PCD and PII collectively defined as "Personal Information").

231. Home Depot saves consumers' Personal Information indefinitely and uses it in ways to increase Home Depot's profits. Through its Privacy Policy, which is available on its website, Home Depot identifies the categories of 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, e-mail 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.

232. Home Depot collects customers' Personal Information not only via point-of-sale purchases, but also "passively" from "tracking tools like browser cookies, flash cookies, and web beacons," and from "other sources" like "third party business partners." The information is used for any number of purposes including entering customers into sweepstakes, marketing, and to share with third



parties in order to offer customers “financial products” like the Home Depot credit card and home improvement loans. Home Depot states that it uses “industry standard means to protect our websites and your information.”

233. Any Home Depot employee can access a customer’s Personal Information, including complete sales data on any credit, debit, or check transaction, via a browser-based terminal or point-of-sale device. Home Depot also compiles and maintains files concerning consumers’ financial and credit histories. Thus, Home Depot stores massive amounts of customer information in its systems and utilizes this information to maximize profits by sharing customer information with third-party affiliates, recommending add-on financial services, and employing predictive marketing and other marketing techniques. Home Depot neglects to inform its customers, however, that the company maintains possession of customers’ personal information, payment card data and magnetic card stripe data *indefinitely* on Home Depot’s servers.

234. In its regular course of business, Home Depot maintains internal data loss prevention policies, data loss prevention standards, and classification and control standards for stored information. In permitting the data breach to occur, Home Depot violated a number of its own internal policies and information-storing procedures.

235. Home Depot's 2010 data loss prevention policy provides in pertinent part:

The information and data developed and collected by The Home Depot, Inc. ("Home Depot or Company") constitute a significant and vital part of the Company's operations and are directly related to its success and profitability. The Home Depot relies on the availability and accuracy of its data assets, including, but not limited to confidential and proprietary Company information, associate and customer information, and vendor and supplier information. Pursuant to The Home Depot's policies regarding the protection, use and disposal of Company information and federal, state and international laws governing the protection and disposal of personally identifiable information, all associates, third-party contractors and service providers with access to such information are responsible for protecting this information and keeping it confidential.

The Home Depot classifies all Company information. The value placed by The Home Depot on a Company asset determines its classification and the level of security required for its protection. Information classifications are specified in The Home Depot's Information Classification and Control Standard and in The Home Depot's Privacy Policy. All associates must comply with the requirements of both the Information Classification and Control Standard and The Home Depot's Privacy Policy when transmitting and storing Company information. Associates must exercise due diligence to protect The Home Depot assets from unauthorized access and distribution.

236. In other words, Home Depot treats the personal and financial information of its *customers* as an "asset" of the *company* that must be protected to preserve its value to Home Depot, not the customer. This conclusion is supported by Home Depot's Information Classification and Control Standard document from 2010 ("HD Information Standards"), which provides that:

Data and information are among [Home Depot's] most important assets. Without appropriate classification and control, the value and usefulness of our data and information will quickly become non-existent. To ensure that all data and information in use within [Home Depot] is appropriately handled, this standard establishes classification requirements, handling requirements and security controls imperative to maintaining confidentiality, integrity and availability.

237. The HD Information Standards set forth the “roles and responsibilities” for different departments within Home Depot. The standards provide that Home Depot’s “Information Technology” department is responsible for:

- a. Ensuring appropriate technological solutions are designed and implemented which support the requirements of this standard.
- b. Ensuring that software/operating system vulnerabilities are mitigated in a timely manner and the necessary software upgrades and configurations are maintained and protected.
- c. Notifying Information Assurance of any identified exceptions to this standard.

238. As alleged above, when Home Depot IT security employees attempted to comply with these standards by notifying superiors of “system vulnerabilities” and recommending “necessary software upgrades and configurations,” they were routinely ignored by Home Depot’s management.

239. The HD Information Standards also include “Information Sensitivity Classification” in order to classify categories of information commensurate with their internal value to Home Depot. According to Home Depot, information classification is necessary because:

All data and information must be assessed for its value not only to The Home Depot and our customers but also to our competitors. To ensure data and information is handled commensurate with its value, [Home Depot] requires all data and information be classified as defined in the following sections. [Home Depot] Associates who violate these requirements are subject to disciplinary action up to and including termination.

240. Home Depot categorized “Restricted” information as “regulated or controlled information that has legal ramifications if disclosed either internally or externally or information that, if improperly disclosed, will cause grave damage to the company’s competitive advantage, its business partners, and/or the privacy or financial viability of its customers or associates. This category of information is extremely sensitive in nature and may not be shared except when deemed absolutely necessary for continuation of business.” Examples of “restricted information” defined by Home Depot included:

- a. Identity verification information such as passwords, customer PINs, dynamic password PINs, or customer identification and authentication information;
- b. Credit card or procurement card numbers;

- c. Bank account numbers;
- d. Any form of cryptographic key;
- e. Highly sensitive customer data (including customer transactions, driver's license numbers and social security numbers);
- f. Highly sensitive information about associates (including social security numbers, background and drug screen results, medical information); and
- g. Company business strategies and forecasts (acquisitions, mergers, trade secrets, financial reporting information, Board of Directors meeting notes, or other company information that would gravely damage Home Depot should it be exposed to individuals who do not have the "need to know").

241. Home Depot categorized "Confidential" information as "information, which if disclosed, could violate the privacy of individuals or customers, reduce the company's competitive advantage, or cause significant financial damage to its external business partners and/or customers. This category of information is very sensitive in nature and may only be released with the permission of the data custodian on a "need-to-know" basis." Examples of "confidential information" defined by Home Depot included:

- a. Customer names and contact information (such as home addresses, telephone numbers, e-mail address, etc.);
- b. Personally identifiable information regarding [Home Depot] Associates (such as home address, personal telephone numbers, personal e-mail addresses, salary information, performance data);
- c. Customer Buying History and Buying Patterns;
- d. Security configurations and controls for systems, applications and networks;
- e. Security logs, audit data and assessment reports; and
- f. Proprietary data (such as vendor pricing, pricing models, markup/markdown models, forecasting models, etc.).

242. Home Depot also classified information as “internal” and “public” Home Depot information. Home Depot maintained “information handling” procedures for each category of information. As of 2010, Home Depot required storage of restricted and confidential information stored by LAN (which stands for Local Area Network and refers to computer devices connected to a server using a shared communications line or wireless link) to be encrypted. Home Depot also required all restricted information stored on fixed media to be encrypted.

243. Home Depot violated its own internal policies by failing to implement point-of-sale encryption across all of its U.S. stores until September 2014. As a

result, customers' personal and financial information, which Home Depot internally classified as "restricted" or "confidential" because of its value to the company, was exposed and made available to criminals across the globe.

### **Home Depot Violated Industry Standards**

244. The Payment Card Industry Data Security Standards ("PCI DSS") list 12 information security requirements promulgated by the Payment Card Industry Security Standards Council ("Council"). These industry requirements apply to all organizations and environments where cardholder data is stored, processed, or transmitted and require merchants, including Home Depot, to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies. The PCI DSS prohibited Home Depot from retaining certain customer data. Below is a "high-level overview" of the 12 requirements:

**PCI Data Security Standard – High Level Overview**

<b>Build and Maintain a Secure Network and Systems</b>	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
<b>Protect Cardholder Data</b>	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
<b>Maintain a Vulnerability Management Program</b>	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
<b>Implement Strong Access Control Measures</b>	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
<b>Regularly Monitor and Test Networks</b>	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
<b>Maintain an Information Security Policy</b>	12. Maintain a policy that addresses information security for all personnel

245. Home Depot is required to adhere to the PCI DSS in order to accept all major credit cards. The PCI DSS require that all merchants, including Home Depot, establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.

246. The PCI DSS further require that all merchants, including Home Depot, perform internal and external network “vulnerability scans” at least quarterly and after any significant change in the network such as new system component installations, changes in network topology, firewall rule modifications, and product upgrades. If “high-risk” vulnerabilities are detected, re-scans must be regularly performed until the vulnerabilities are resolved. To stay PCI DSS compliant, companies often employ Qualified Security Assessors (“QSAs”), or



organizations that have been qualified by the PCI Council to have their employees assess compliance to the PCI DSS.

247. In approximately February 2011, Home Depot's QSA identified a "major gap" in the company's data security system which fell below basic PCI DSS and implicated major concerns about how Home Depot stored customers' financial data on its network. Home Depot put together a team of employees to address the problem. Home Depot's QSAs ultimately provided a written report to Matthew Carey and Home Depot's IT executives in Atlanta, Georgia identifying security deficiencies that needed to be immediately addressed in order to remain PCI DSS compliant. While Home Depot made representations that it would comply with the recommendations in order to ease the concerns of the Council, the recommendations were never actually fully implemented. After this incident, Matthew Carey sought to replace Tammy Moskites as CISO with Jeff Mitchell.

248. In 2012, Home Depot was using a company called Solutionary as its QSA to audit PCI DSS compliance. In approximately September 2012, Home Depot's security personnel charged with overseeing PCI DSS compliance submitted a detailed PowerPoint report to Jeff Mitchell that identified multiple deficiencies in Solutionary's auditing procedures and identified several areas where the company was not in compliance with the PCI DSS. For example, Home Depot was running "vulnerability scans" at less than 10% of the company's U.S.

stores, when the PCI DSS required all stores to be scanned. Additionally, Home Depot misrepresented to Solutionary and the Council that each Home Depot store utilized “20 systems” which housed security data, when in fact, each store maintained approximately 200 systems. As a cost-savings measure, Home Depot intentionally misrepresented to Solutionary the extent to which its systems were “segmented” in order to convince the QSAs that each system did not need to be independently monitored or evaluated. Upon reviewing the report, Jeff Mitchell denied any wrongdoing and dismissed his security team’s findings.

249. An investigation by *The New York Times* confirms that while Home Depot permitted vulnerability scans at its data centers, “more than a dozen systems handling customer information were not assessed and were off limits to much of the security staff.” It is unclear why Home Depot refused to scan all of its data systems. As one expert noted: “Scanning is the easiest part of compliance . . . . There are a lot of services that do this. They hardly cost any money. And they can be run cheaply from the cloud.”

250. Among other failures, Home Depot failed to protect against malware and failed to regularly update its antivirus software, even when specifically advised to do so, and was in clear violation of the PCI DSS requiring such compliance. The PCI DSS are considered the “floor” level of security for a company to maintain, not the ceiling. Nevertheless, Home Depot could not even maintain the necessary

base level of security, despite regularly holding itself out as PCI DSS compliant over the last six years.

251. In its 2015 Form 10-K filed with the SEC, Home Depot acknowledged that it may *not* be PCI DSS compliant and believes it will be sued by the payment card networks as a result:

***Litigation, Claims and Government Investigations***

In addition to the above expenses, we believe it is probable that the payment card networks will make claims against us. The ultimate amount of these claims will likely include amounts for incremental counterfeit fraud losses and non-ordinary course operating expenses (such as card reissuance costs) that the payment card networks assert they or their issuing banks have incurred. **In order for us to have liability for such claims, we believe it would have to be determined, among other things, that (1) at the time of the Data Breach the portion of our network that handles payment card data was noncompliant with applicable data security standards, and (2) the alleged noncompliance caused at least some portion of the compromise of payment card data that occurred during the Data Breach.**

**Although an independent third-party assessor found the portion of our network that handles payment card data to be compliant with applicable data security standards in the fall of 2013, and the process of obtaining such certification for 2014 was ongoing at the time of the Data Breach, in March 2015 the forensic investigator working on behalf of the payment card networks alleged that we were not in compliance with certain of those standards at the time of the Data Breach. As a result, we believe it is probable that the payment card networks will make claims against us and that we will dispute those claims.** When those claims are asserted, we will have to determine, based on the facts and information then available to us, whether to litigate or seek to settle those claims. At this time, we believe that settlement negotiations will ensue and that it is probable that we will incur a loss in connection with those claims.

252. Additionally, financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants such as Home Depot must take to ensure that valuable transactional data is secure and protected. The debit and credit card companies issue regulations (“Card Operating Regulations”) that bind Home Depot as a condition of its contract with its acquiring bank. The Card Operating Regulations prohibit Home Depot and other merchants from disclosing any cardholder account numbers, personal information, magnetic stripe information or transaction information to third parties (other than the merchant’s agent, the acquiring bank, or the acquiring bank’s agents). The Card Operating Regulations further require Home Depot to maintain the security and confidentiality of debit and credit cardholder information and magnetic stripe information and protect it from unauthorized disclosure.

253. Despite Home Depot’s awareness of its data protection obligations, Home Depot’s treatment of the PII and PCD entrusted to it by its customers fell far short of satisfying Home Depot’s legal duties and obligations, and included violations of the PCI DSS and Card Operating Regulations. Home Depot failed to ensure that access to its data systems was reasonably safeguarded, and failed to acknowledge and act upon numerous warning signs and properly utilize its own security systems that were put in place to detect and deter this exact type of attack.

**Personal Identity and Financial Information Is Valuable Property**

254. Consumer Plaintiffs' PII is personal property and when stolen, particularly in conjunction with PCD, is an extremely valuable commodity. A "cyber black-market" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. PII and PCD is "as good as gold" to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

255. As described above, millions of Home Depot customers had their PII and PCD made available for resale in at least 12 separate batches on the underground website Rescator (along with other underground websites), with card numbers selling between \$50 and \$100 per card. Individuals from all over the world purchased the information in order to perpetrate frauds on the cardholders.

256. The online black markets also provide purchasing thieves with the ZIP code and location of the Home Depot store where the information was stolen. This allows thieves to make same-state purchases, thus avoiding blocks from financial institutions that suspect fraud. With location information in hand, fraudsters also have the ability to determine and change PIN numbers and withdraw cash from ATMs, and get access to the cardholder's social security number and date of birth

in order to perpetrate more severe forms of fraud and identity theft. According to one study, “1 in 4 data breach notification recipients becomes a victim of identity fraud.”

257. The ramifications of Home Depot’s failure to protect its customers’ Personal Information are severe. Fraudsters can use such information to perpetrate a variety of crimes that harm victims. For instance, fraudsters 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, or using the victim’s information to obtain government benefits. Some of this activity may not come to light for years.

258. In addition, 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. Most victims who have had their information used for fraudulent purchases spend more than a month attempting to resolve problems. In some cases, it can take years.

259. Moreover, 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, 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.

260. There is a strong probability that entire batches of stolen information have yet to be dumped on the black market, meaning Home Depot customers could be at risk of fraud and identity theft for years into the future.

261. Consumer Plaintiffs and members of the classes defined below have or will suffer actual injury as a direct result of Home Depot's data breach. In addition to fraudulent charges and damage to their credit, many victims spent substantial time and expense relating to:

- a. Finding fraudulent charges;
- b. Canceling and reissuing cards;
- c. Purchasing credit monitoring and identity theft prevention;
- d. Addressing their inability to withdraw funds linked to compromised accounts;
- e. Removing withdrawal and purchase limits on compromised accounts;
- f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
- g. Resetting automatic billing instructions; and

- h. Paying late fees and declined payment fees imposed as a result of failed automatic payments.

262. Home Depot victims who had their social security number and date of birth compromised may suffer additional hardships. Under U.S. Social Security Administration (SSA) policy, individuals cannot obtain a new social security number until there is evidence of ongoing problems due to misuse of the Social Security number. Even then, the SSA recognizes that “a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start.”

263. In fact, a new social security number is substantially less effective where “other personal information, such as [the victim’s] name and address, remains the same” and for some victims, “a new number actually creates new problems. If the old credit information is not associated with [the victim’s] new number, the absence of any credit history under your new number may make it more difficult for [the victim] to get credit.”



264. As a direct and proximate result of Home Depot's conduct, Consumer Plaintiffs and members of the classes defined below have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud. Consumer Plaintiffs now have to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Moreover, Consumer Plaintiffs and members of the classes have an interest in ensuring that their Personal Information, which remains in the possession of Home Depot, is protected from further breaches by the implementation of security measures and safeguards.

265. Home Depot customers have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

- a. Trespass, damage to and theft of their personal property including PII and PCD;
- b. Improper disclosure of their PII and PCD property;
- c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by customers' Personal

Information being placed in the hands of criminals and having been already misused via the sale of such information on the Internet black market;

- d. Damages flowing from Home Depot's untimely and inadequate notification of the data breach;
- e. Loss of privacy suffered as a result of the data breach;
- 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 customers' Personal Information for which there is a well-established and quantifiable national and international market;
- h. 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 customers were permitted to obtain from their accounts.

### **CLASS ALLEGATIONS**

#### **A. The State Statutory Classes**

266. Pursuant to Fed. R. Civ. P. 23, Consumer Plaintiffs assert their claims that Home Depot violated state consumer statutes (Count I) and state data breach

notification laws (Count II) on behalf of separate statewide classes, defined as follows:

**Statewide [Consumer Protection or Data Breach Notification] Classes:**

All residents of [name of State] whose Personal Information was compromised as a result of the data breach first disclosed by Home Depot in September 2014.

267. Consumer Plaintiffs assert the state consumer law claims (Count I) under the listed consumer protection laws of Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, U.S. Virgin Islands, Washington, West Virginia, Wyoming, and the District of Columbia.

268. Consumer Plaintiffs assert the state data breach notification law claims (Count II) on behalf of separate statewide classes in and under the respective data breach statutes of the States of Alaska, California, Colorado, Delaware, Georgia, Hawaii, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maryland, Michigan, Montana, New Hampshire, New Jersey, North Carolina, North Dakota, Oregon, Puerto Rico, South Carolina, Tennessee, Virginia, U.S.

Virgin Islands, Washington, Wisconsin and Wyoming, and the District of Columbia.

**B. The Nationwide Class**

269. Pursuant to Fed. R. Civ. P. 23, Consumer Plaintiffs assert their common law claims for negligence (Count III), breach of implied contract (Count IV), unjust enrichment (Count V), and declaratory judgment (Count VI) on behalf of a nationwide class, defined as follows:

**Nationwide Class:**

All residents of the United States whose Personal Information was compromised as a result of the data breach first disclosed by Home Depot in September 2014.

270. As alleged herein, Home Depot is headquartered in Atlanta, Georgia, maintains its primary data center in Atlanta, Georgia, and the employees charged with making decisions concerning data security are based in Atlanta, Georgia. Home Depot's conduct resulting in the Home Depot data breach took place exclusively, or primarily, in Georgia. Accordingly, this Court has general jurisdiction over Home Depot and original jurisdiction over Consumer Plaintiffs' claims. Applying Georgia law, therefore, comports with due process.

**C. The State Common Law Classes**

271. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Consumer Plaintiffs assert claims for negligence (Count III), breach of implied contract (Count IV), unjust enrichment

(Count V), and declaratory judgment (Count VI) under the laws of the individual States and Territories of the United States, and on behalf of separate statewide classes, defined as follows:

**Statewide [Negligence, Breach of Implied Contract, Unjust Enrichment, or Declaratory Judgment] Classes:**

All residents of [name of State] whose Personal Information was compromised as a result of the data breach first disclosed by Home Depot in September 2014.

**D. The California Class**

272. Pursuant to Fed. R. Civ. P. 23, Consumer Plaintiffs Earls, Fuller, Gonzalez, Hernandez, Holt, Khalaf, Metter, Moran, Newton, and O'Brien (collectively, the "California Plaintiffs") assert a claim under the California Customer Records Act, California Civil Code section 1798.81.5, and the "unlawful prong" of California's Unfair Competition Law, California Business and Professions Code section 17200 (Count VIII) on behalf of a California class defined as follows:

**California Class:**

All residents of California whose Personal Information was compromised as a result of the data breach first disclosed by Home Depot in September 2014.

**E. The Maryland Class**

273. Pursuant to Fed. R. Civ. P. 23, Consumer Plaintiff James Burden asserts a claim under the Maryland Personal Information Protection Act, Maryland Code, Commercial Law section 14-3503, and the Maryland Consumer Protection

Act, Maryland Code, Commercial Law section 13-101, et seq. (Count IX), on behalf of a Maryland class defined as follows:

**Maryland Class:**

All residents of Maryland whose Personal Information was compromised as a result of the data breach first disclosed by Home Depot in September 2014.

274. Excluded from each of the above Classes are Defendants and their parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

275. Each of the proposed classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3):

276. **Numerosity.** The proposed classes include many thousands to tens of millions of customers whose data was compromised in the data breach. While the precise number of Class members in each proposed class has not yet been determined, the massive size of the Home Depot data breach indicates that joinder of each member would be impracticable.

277. **Commonality.** Common questions of law and fact exist and predominate over any questions affecting only individual Class members. The common questions include:

- a. whether Home Depot engaged in the conduct alleged herein;

- b. whether Home Depot's conduct constituted Deceptive Trade Practices (as defined below) actionable under the applicable consumer protection laws;
- c. whether Home Depot had a legal duty to adequately protect Consumer Plaintiffs' and Class members' Personal Information;
- d. whether Home Depot breached its legal duty by failing to adequately protect Consumer Plaintiffs' and Class members' Personal Information;
- e. whether Home Depot had a legal duty to provide timely and accurate notice of the Home Depot data breach to Consumer Plaintiffs and Class members;
- f. whether Home Depot breached its duty to provide timely and accurate notice of the Home Depot data breach to Consumer Plaintiffs and Class members;
- g. whether and when Home Depot knew or should have known that Consumer Plaintiffs' and Class members' Personal Information stored on its computer systems was vulnerable to attack;
- h. whether Consumer Plaintiffs and Class members are entitled to recover actual damages and/or statutory damages; and

- i. whether Consumer Plaintiffs and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

278. **Typicality.** Consumer Plaintiffs' claims are typical of the claims of the Class. Consumer Plaintiffs and Class members were injured through Home Depot's uniform misconduct and their legal claims arise from the same core Home Depot practices.

279. **Adequacy.** Consumer Plaintiffs are adequate representatives of the proposed classes because their interests do not conflict with the interests of the Class members they seek to represent. Consumer Plaintiffs' counsel are very experienced in litigating consumer class actions and complex commercial disputes, and include lawyers who have successfully prosecuted similarly massive retail data breach cases.

280. **Superiority.** A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Home Depot. Even if it were economically feasible, requiring millions of injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class



treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

281. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). 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.

282. Finally, 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 to identify Class members.

**COUNT I**  
**VIOLATIONS OF STATE CONSUMER LAWS**  
**(ON BEHALF OF CONSUMER PLAINTIFFS AND THE SEPARATE**  
**STATEWIDE CONSUMER LAW CLASSES)**

283. Consumer Plaintiffs reallege, as if fully set forth, the allegations of paragraphs 1-264 above.

284. Consumer Plaintiffs and members of the statewide Consumer Law Classes (the “Class” for purposes of this claim) are consumers who used their credit or debit cards to purchase products or services from Home Depot primarily for personal, family, or household purposes.

285. Home Depot engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of goods or services to consumers, including Consumer Plaintiffs and members of the Class.

286. Home Depot is engaged in, and its acts and omissions affect, trade and commerce. Home Depot's acts, practices, and omissions were done in the course of Home Depot's business of marketing, offering for sale, and selling goods and services throughout the United States.

287. Home Depot's conduct constitutes unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices (collectively, "Deceptive Trade Practices"), including, among other things, Home Depot's:

- a. failure to maintain adequate computer systems and data security practices to safeguard customers' Personal Information;
- b. failure to disclose that its computer systems and data security practices were inadequate to safeguard customers' Personal Information from theft;
- c. failure to timely and accurately disclose the data breach to Consumer Plaintiffs and Class members;
- d. continued acceptance of Consumer Plaintiffs' and Class members' credit and debit card payments and storage of other personal

- information after Home Depot knew or should have known of the security vulnerabilities that were exploited in the data breach; and
- e. continued acceptance of Consumer Plaintiffs' and Class members' credit and debit card payments and storage of other personal information after Home Depot knew or should have known of the data breach and before it allegedly fixed the breach.

288. By engaging in such Deceptive Trade Practices, Home Depot has violated state consumer laws, including those that prohibit:

- a. representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;
- b. representing that goods and services are of a particular standard, quality or grade, if they are of another;
- c. omitting material facts regarding the goods and services sold;
- d. engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding;
- e. unfair methods of competition;
- f. unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices; and/or

- g. similar prohibitions under the state consumer laws identified below.

289. As a direct result of Home Depot's violating state consumer laws, Consumer Plaintiffs and Class members suffered damages that include:

- a. fraudulent charges on their debit and credit card accounts, some of which were never reimbursed;
- b. theft of their Personal Information by criminals;
- c. costs associated with the detection and prevention of identity theft;
- d. costs associated with the fraudulent use of their financial accounts;
- e. loss of use of and access to some or all of their account funds and costs incurred as a result of being unable to access those funds;
- f. costs and lost time associated with handling the administrative consequences of the Home Depot data breach, including identifying, disputing, and seeking reimbursement for fraudulent charges, canceling and activating payment cards, and shopping for credit monitoring and identity theft protection;
- g. purchasing products and services at Home Depot stores that they would not have purchased, or would have not had paid the same price for, had they known of Home Depot's Deceptive Trade Practices;

- h. impairment to their credit scores and ability to borrow and/or obtain credit; and
- i. the continued risk to their personal information, which remains on Home Depot's insufficiently secured computer systems.

290. Home Depot's Deceptive Trade Practices violate the following state consumer statutes:

- a. The Alabama Deceptive Trade Practices Act, Ala. Code §§ 8-19-5(2), (3), (5), (7), and (27), et seq.;
- b. The Alaska Unfair Trade Practices and Consumer Protection Act, Alaska Stat. §§ 45.50.471-45.50.561;
- c. The Arizona Consumer Fraud Act, A.R.S. § 44-1522;
- d. The Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-107(a)(1)(10) and 4-88-108(1)(2), et seq.;
- e. The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, et seq., and the California Unfair Competition Law, Cal. Bus. and Prof. Code, § 17200, et seq.;
- f. The Colorado Consumer Protection Act, Col. Rev. Stat. Ann. §§ 6-1-105(1)(b), (c), (e) and (g), et seq.;
- g. The Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110(b), et seq.;

- h. The Delaware Consumer Fraud Act, Del. Code Ann. Title 6 § 2513, et seq.;
- i. The District of Columbia Consumer Protection Act, D.C. Code §§ 28-3904(a), (d), (e), (f) and (r), et seq.;
- j. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1), et seq.;
- k. The Georgia Fair Business Practices Act, Ga. Code Ann. §§ 10-1-393(a) and (b)(2), (3), (5), and (7), et seq.;
- l. The Hawaii Deceptive Trade Practices Act, Haw. Rev. Stat. Ann. §§ 481A-3(a)(5), (7) and (12), et seq., and the Hawaii Consumer Protection Act, Haw. Rev. Stat. Ann. § 480-2(a), et seq.;
- m. The Idaho Consumer Protection Act, Idaho Code §§ 48-603(5), (7), (17) and (18), et seq., and Idaho Code § 48-603C, et seq.;
- n. The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Stat. § 505/2, et seq., and the Illinois Uniform Deceptive Trades Practices Act, 815 Ill. Stat. §§ 510/2(a)(5), (7) and (12), et seq.;
- o. The Indiana Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5-3(a) and (b)(1) and (2), et seq.;

- p. The Iowa Consumer Fraud Act, I.C.A. §§ 714H.3 and 714H.5, et seq. (Consumer Plaintiffs have obtained the approval of the Iowa Attorney General for filing this class action lawsuit as provided under I.C.A. § 714H.7);
- q. The Kansas Consumer Protection Act, Kan. Stat. §§ 50-626(a) and (b)(1)(A)(D) and (b)(3), et seq.;
- r. The Kentucky Consumer Protection Act, Ky. Rev. Stat. §§ 367.170(1) and (2), et seq.;
- s. The Louisiana Unfair Trade Practices and Consumer Protection Law, La. Rev. Stat. Ann. § 51:1405(A), et seq.;
- t. The Massachusetts Consumer Protection Act, Ma. Gen. Laws Ann. Ch. 93A § 2(a), et seq.;
- u. The Maine Uniform Deceptive Trade Practices Act, 10 M.R.S.A. §§ 1212(1)(E) and (G), et seq., and the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 207, et seq.;
- v. The Maryland Consumer Protection Act, Md. Code Commercial Law, §§ 13-301(1) and (2)(i)-(ii), and (iv), (5)(i), and (9)(i), et seq.;
- w. The Michigan Consumer Protection Act, M.C.P.L.A. §§ 445.903(1)(c)(e), (s) and (cc), et seq.;

- x. The Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.44, subd. 1(5), (7) and (13), et seq., and the Minnesota Consumer Fraud Act, Minn. Stat. § 325F.69, subd. 1, and Minn. Stat. § 8.31, subd. 3(a);
- y. The Mississippi Consumer Protect Act, Miss. Code Ann. §§ 75-24-5(1), (2)(b), (c), (e), and (g), et seq.;
- z. The Missouri Merchandising Practices Act, Mo. Ann. Stat. § 407.020(1), et seq.;
- aa. The Montana Unfair Trade Practices and Consumer Protection Act, Mont. Code Ann. § 30-14-103, et seq.;
- bb. The Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1602, and the Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-302(a)(5) and (7), et seq.;
- cc. The Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann. §§ 598.0915(5) and (7), et seq.;
- dd. The New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 358-A:2(v) and (vii), et seq.;
- ee. The New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2, et seq.;



- ff. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2(D)(5)(7) and (14) and 57-12-3, et seq.;
- gg. The New York Business Law, N.Y. Gen. Bus. Law § 349(a);
- hh. The North Carolina Unfair Trade Practices Act, N.C.G.S.A. § 75-1.1(a), et seq.;
- ii. The North Dakota Unlawful Sales or Advertising Practices Act, N.D. Cent. Code § 51-15-02, et seq.;
- jj. The Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. §§ 1345.02(A) and (B)(1) and (2), et seq.;
- kk. The Oklahoma Consumer Protection Act, 15 Okl. Stat. Ann. §§ 753(5), (7) and (20), et seq.;
- ll. The Oregon Unfair Trade Practices Act, Or. Rev. Stat. §§ 646.608(1)(e)(g) and (u), et seq.;
- mm. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-2(4)(v)(vii) and (xxi), and 201-3, et seq.;
- nn. The Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws §§ 6-13.1-1(6)(v), (vii), (xii), (xiii) and (xiv), et seq.;
- oo. The South Carolina Unfair Trade Practices Act, S.C. Code Ann. § 39-5-20(a), et seq.;

- pp. The South Dakota Deceptive Trade Practices Act and Consumer Protection Act, S.D. Codified Laws § 37-24-6(1), et seq.;
- qq. The Tennessee Consumer Protection Act, Tenn. Code Ann. §§ 47-18-104(a), (b)(2), (3), (5), and (7), et seq.;
- rr. The Texas Deceptive Trade Practices Consumer Protection Act, V.T.C.A., Bus. & C. §§ 17.46(a), (b)(5) and (7), et seq.;
- ss. The Utah Consumer Sales Practices Act, Utah Code Ann. §§ 13-11-4(1), (2)(a), (b), and (i) et seq.;
- tt. The Vermont Consumer Fraud Act, 9 V.S.A. § 2453(a), et seq.;
- uu. The Virgin Islands Consumer Protection Law, V.I. Code Ann. tit. 12A, § 101, et seq.;
- vv. The Virginia Consumer Protection Act, Va. Code Ann. §§ 59.1-200(A)(5)(6) and (14), et seq.;
- ww. The Washington Consumer Protection Act, Wash. Rev. Code § 19.86.020, et seq.;
- xx. The West Virginia Consumer Credit and Protection Act, W.V.A. Code § 46A-6-104, et seq.; and
- yy. The Wyoming Consumer Protection Act, Wyo. Stat. Ann. §§ 40-12-105(a), (i), (iii) and (xv), et seq.

291. As a result of Home Depot's violations, Consumer Plaintiffs and members of the Class are entitled to injunctive relief, including, but not limited to: (1) ordering that Home Depot 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, and ordering Home Depot to promptly correct any problems or issues detected by such third-party security auditors; (2) ordering that Home Depot engage third-party security auditors and internal personnel to run automated security monitoring; (3) ordering that Home Depot audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Home Depot segment customer 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; (5) ordering that Home Depot purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services; (6) ordering that Home Depot conduct regular database scanning and securing checks; (7) ordering that Home Depot routinely and continually 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 (8) ordering Home Depot to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal

information to third parties, as well as the steps Home Depot customers must take to protect themselves.

292. Because of Home Depot's Deceptive Trade Practices, Consumer Plaintiffs and the Class members are entitled to relief, including restitution of the costs associated with the data breach, disgorgement of all profits accruing to Home Depot because of its Deceptive Trade Practices, attorneys' fees and costs, declaratory relief, and a permanent injunction enjoining Home Depot from its Deceptive Trade Practices.

293. Consumer Plaintiffs bring this claim on behalf of themselves and the Class members for the relief requested and to benefit the public interest. This claim supports the public interests in assuring that consumers are provided truthful, non-deceptive information about potential purchases and protecting members of the public from Home Depot's Deceptive Trade Practices. Home Depot's wrongful conduct, including its Deceptive Trade Practices has affected the public at large because a substantial percentage of the U.S. population has been affected by Home Depot's conduct.

294. Before filing this Complaint, counsel for Consumer Plaintiffs and the Class members provided Home Depot with pre-suit demand letters in compliance with state consumer laws, including Alaska Stat. Ann. § 45.50.535(b); Cal. Civ. Code § 1782(a); Me. Rev. Stat. Ann. Tit. 5, § 213(1-A); Mass. Gen. Laws Ann.

Ch. 93A § 9(3); Tex. Bus. & Com. Code Ann. § 17.505(a); W.Va. Code § 46A-6-106(b); and Wyo. Stat. § 40-12-109. Additionally, Home Depot has long had notice of Consumer Plaintiffs' allegations, claims, and demands based on the numerous consumer class actions related to this Complaint.

295. Consumer Plaintiffs have provided notice of this action and a copy of this Complaint to the appropriate Attorneys General pursuant to Conn. Gen. Stat. § 42-110g(c); 815 Ill. Stat. § 505/6; I.C.A. § 714H.7; Kan. Stat. § 50-634(g); N.J. Stat. Ann. § 56:8-20; Ore. Rev. Stat. Ann. § 646.638(s); and Wash. Rev. Code § 19.86.095.

**COUNT II**  
**VIOLATIONS OF STATE DATA BREACH NOTIFICATION STATUTES**  
**(ON BEHALF OF CONSUMER PLAINTIFFS AND THE SEPARATE**  
**STATEWIDE DATA BREACH STATUTE CLASSES)**

296. Consumer Plaintiffs reallege, as if fully set forth, the allegations of paragraphs 1-264 above.

297. Legislatures in the states and jurisdictions listed below have enacted data breach statutes. These statutes generally apply to any person or business conducting business within the state that owns or licenses computerized data containing personal information. If the personal information is acquired or accessed in a way that compromises its security or confidentiality, the covered entity must notify the affected individuals in the most expedient time and manner possible and without unreasonable delay.

298. The Home Depot data breach constituted a security breach that triggered the notice provisions of the data breach statutes and the Personal Information taken includes categories of personal information protected by the data breach statutes.

299. Home Depot unreasonably delayed in informing Consumer Plaintiffs and members of the statewide Data Breach Statute Classes (“Class,” as used in this Claim II), about the data breach after Home Depot knew or should have known that the data breach had occurred.

300. Consumer Plaintiffs and Class members were damaged by Home Depot’s failure to comply with the data breach statutes.

301. Had Home Depot provided timely and accurate notice, Consumer Plaintiffs and Class members could have avoided or mitigated the harm caused by the data breach. For example, they could have contacted their banks to cancel any affected cards, taken security precautions in time to prevent or minimize identity theft, or could have avoided using uncompromised payment cards during subsequent Home Depot purchases.

302. Home Depot’s failure to provide timely and accurate notice of the Home Depot data breach violated the following state data breach statutes:

- a. Alaska Stat. Ann. § 45.48.010(a), et seq.;
- b. Cal. Civ. Code § 1798.80, et seq.;

- c. Colo. Rev. Stat. Ann § 6-1-716(2), et seq.;
- d. Del. Code Ann. Tit. 6 § 12B-102(a), et seq.;
- e. D.C. Code § 28-3852(a), et seq.;
- f. Ga. Code Ann. § 10-1-912(a), et seq.;
- g. Haw. Rev. Stat. § 487N-2(a), et seq.;
- h. Ill. Comp. Stat. Ann. 530/10(a), et seq.;
- i. Iowa Code Ann. § 715C.2(1), et seq.;
- j. Kan. Stat. Ann. § 50-7a02(a), et seq.;
- k. Ky. Rev. Stat. Ann. § 365.732(2), et seq.;
- l. La. Rev. Stat. Ann. § 51:3074(A), et seq.;
- m. Md. Code Ann., Commercial Law § 14-3504(b), et seq.;
- n. Mich. Comp. Laws Ann. § 445.72(1), et seq.;
- o. Mont. Code Ann. § 30-14-1704(1), et seq.;
- p. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), et seq.;
- q. N.J. Stat. Ann. § 56:8-163(a), et seq.;
- r. N.C. Gen. Stat. Ann. § 75-65(a), et seq.;
- s. N.D. Cent. Code Ann. § 51-30-02, et seq.;
- t. Or. Rev. Stat. Ann. § 646A.604(1), et seq.;
- u. P.R. Laws Ann. tit. 10, § 4052, et seq.;
- v. S.C. Code Ann. § 39-1-90(A), et seq.;

- w. Tenn. Code Ann. § 47-18-2107(b), et seq.;
- x. V.I. Code Ann. tit. 14 § 2209(a), et seq.;
- y. Va. Code Ann. § 18.2-186.6(B), et seq.;
- z. Wash. Rev. Code Ann. § 19.255.010(1), et seq.;
- aa. Wis. Stat. Ann. § 134.98(2), et seq.; and
- bb. Wyo. Stat. Ann. § 40-12-502(a), et seq.

303. Consumer Plaintiffs and members of each of the statewide Data Breach Statute Classes seek all remedies available under their respective state data breach statutes, including but not limited to damages, equitable relief, including injunctive relief, treble damages, reasonable attorneys' fees and costs, as provided by the applicable laws.

**COUNT III**  
**NEGLIGENCE**  
**(ON BEHALF OF CONSUMER PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, CONSUMER PLAINTIFFS AND THE SEPARATE STATEWIDE NEGLIGENCE CLASSES)**

304. Consumer Plaintiffs reallege, as if fully set forth, the allegations of paragraphs 1-264 above.

305. Home Depot owed numerous duties to Consumer Plaintiffs and to members of the Nationwide Class, or, alternatively, members of the Separate Statewide Negligence Classes (collectively, the "Class" as used in this Count). Home Depot's duties included the following:



- a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII and PCD in its possession;
- b. to protect their PII and PCD using reasonable and adequate security procedures and systems that are compliant with the PCI-DSS standards and consistent with industry-standard practices; and
- c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Consumer Plaintiffs and Class members of the Home Depot data breach.

306. Home Depot owed a duty of care not to subject Consumer Plaintiffs, along with their PII and PCD, and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices. Home Depot solicited, gathered, and stored Consumer Plaintiffs' and Class members' Personal Information to facilitate sales transactions.

307. Home Depot knew, or should have known, of the risks inherent in collecting and storing Personal Information and the importance of adequate security. Home Depot received warnings from within and outside the company that hackers routinely attempted to access Personal Information without authorization. Home Depot also knew about numerous, well-publicized data breaches by other national retailers.

308. Home Depot knew, or should have known, that its computer systems did not adequately safeguard Consumer Plaintiffs' and Class members Personal Information.

309. Because Home Depot knew that a breach of its systems would damage millions of its customers, including Consumer Plaintiffs and Class members, it had a duty to adequately protect their Personal Information.

310. Home Depot had a special relationship with Consumer Plaintiffs and Class members. Consumer Plaintiffs' and Class members' willingness to entrust Home Depot with their Personal Information was predicated on the understanding that Home Depot would take adequate security precautions. Moreover, only Home Depot had the ability to protect its systems and the Personal Information it stored on them from attack.

311. Home Depot's own conduct also created a foreseeable risk of harm to Consumer Plaintiffs and Class members and their Personal Information. Home Depot's misconduct included failing to: (1) secure its point-of-sale systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) follow the PCI-DSS standards, (4) encrypt PCD at the point-of-sale and during transit, (5) employ adequate network segmentation, (6) implement adequate system and event monitoring, and (7) implement the systems, policies, and procedures necessary to prevent this type of data breach.

312. Home Depot also had independent duties under state laws that required Home Depot to reasonably safeguard Consumer Plaintiffs' and Class members' Personal Information and promptly notify them about the data breach.

313. Home Depot breached the duties it owed to Consumer Plaintiffs and Class members in numerous ways, including:

- a. by creating a foreseeable risk of harm through the misconduct previously described;
- b. by failing to implement adequate security systems, protocols and practices sufficient to protect their Personal Information both before and after learning of the data breach;
- c. by failing to comply with the minimum industry data security standards, including the PCI-DSS, during the period of the data breach; and
- d. by failing to timely and accurately disclose that their Personal Information had been improperly acquired or accessed.

314. But for Home Depot's wrongful and negligent breach of the duties it owed Consumer Plaintiffs and Class members, their personal and financial information either would not have been compromised or they would have been able to prevent some or all of their damages.

315. The injury and harm that Consumer Plaintiffs and Class members suffered (as alleged above) was the direct and proximate result of Home Depot's negligent conduct. Accordingly, Consumer Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

**COUNT IV**  
**BREACH OF IMPLIED CONTRACT**  
**(ON BEHALF OF CONSUMER PLAINTIFFS AND THE NATIONWIDE**  
**CLASS, OR, ALTERNATIVELY, CONSUMER PLAINTIFFS AND THE**  
**SEPARATE STATEWIDE BREACH OF IMPLIED CONTRACT**  
**CLASSES)**

316. Consumer Plaintiffs reallege, as if fully set forth, the allegations of paragraphs 1-264 above.

317. When Consumer Plaintiffs and the members of the Nationwide class or, alternatively, the members of the Separate Statewide Breach of Implied Contract Classes (collectively, the "Class" as used in this Count), provided their Personal Information to Home Depot in making purchases at Home Depot stores, they entered into implied contracts by which Home Depot agreed to protect their Personal Information and timely notify them in the event of a data breach.

318. Home Depot invited its customers, including Consumer Plaintiffs and Class members, to purchase products and services at Home Depot stores using credit or debit cards in order to increase sales by making purchases more convenient. The Personal Information also was valuable to Home Depot, because Home Depot uses it for ancillary marketing and business purposes.

319. An implicit part of the offer was that Home Depot would safeguard the Personal Information using reasonable or industry-standard means and would timely notify Consumer Plaintiffs' and the Class in the event of a data breach.

320. Home Depot also affirmatively represented that it collected its customers' Personal Information when they made purchases at Home Depot stores, used that information for a variety of business purposes, and protected the Personal Information using "industry standard means."

321. Based on the implicit understanding and also on Home Depot's representations, Consumer Plaintiffs and the Class accepted the offers and provided Home Depot with their Personal Information by using their credit or debit cards in connection with purchases at Home Depot stores during the period of the Home Depot data breach.

322. Consumer Plaintiffs and Class members would not have provided their Personal Information to Home Depot had they known that Home Depot would not safeguard their Personal Information as promised or provide timely notice of a data breach.

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

324. Home Depot breached the implied contracts by failing to safeguard Consumer Plaintiffs' and Class members' Personal Information and failing to

provide them with timely and accurate notice when their Personal Information was compromised in the data breach.

325. The losses and damages Consumer Plaintiffs and Class members sustained (as described above) were the direct and proximate result of Home Depot's breaches of its implied contracts with them.

**COUNT V**  
**UNJUST ENRICHMENT**  
**(ON BEHALF OF CONSUMER PLAINTIFFS AND THE NATIONWIDE**  
**CLASS, OR, ALTERNATIVELY, CONSUMER PLAINTIFFS AND THE**  
**SEPARATE STATEWIDE UNJUST ENRICHMENT CLASSES)**

326. Consumer Plaintiffs reallege, as if fully set forth, the allegations of paragraphs 1-264 above.

327. Consumer Plaintiffs and members of the Nationwide class or, alternatively, the members of the Separate Statewide Unjust Enrichment Classes (collectively, the "Class" as used in this Count), conferred a monetary benefit on Home Depot. Specifically, they purchased goods and services from Home Depot at retail prices and provided Home Depot with their Personal Information by using their credit or debit cards for the purchases. In exchange, Consumer Plaintiffs and Class members should have been compensated by Home Depot with the goods or services that were the subject of the transaction and by having Home Depot process and store their Personal Information using adequate data security.

328. Home Depot knew that Consumer Plaintiffs and the Class conferred a benefit on Home Depot. Home Depot profited from their purchases and used their Personal Information for its own business purposes.

329. Home Depot failed to secure the Consumer Plaintiffs' and Class members' Personal Information, and, therefore, did not provide full compensation for the benefit the Consumer Plaintiffs and Class members provided.

330. Home Depot acquired the Personal Information through inequitable means because it failed to disclose the inadequate security practices previously alleged.

331. Had Consumer Plaintiffs and Class members known that Home Depot would not secure their Personal Information using adequate security, they would not have completed their purchases with Home Depot.

332. Consumer Plaintiffs and the Class have no adequate remedy at law.

333. Under the circumstances, it would be unjust for Home Depot to be permitted to retain any of the benefits that Consumer Plaintiffs and Class members of the Class conferred on it.

334. Home Depot should be compelled to disgorge into a common fund or constructive trust for the benefit of Consumer Plaintiffs and Class members proceeds that it unjustly received from them. In the alternative, Home Depot

should be compelled to refund the amounts that Consumer Plaintiffs and the Class overpaid.

**COUNT VI**  
**DECLARATORY JUDGMENT**  
**(ON BEHALF OF CONSUMER PLAINTIFFS AND THE NATIONWIDE**  
**CLASS OR, ALTERNATIVELY, THE SEPARATE STATEWIDE**  
**NEGLIGENCE AND BREACH OF IMPLIED CONTRACT CLASSES)**

335. Consumer Plaintiffs reallege, as if fully set forth, the allegations of paragraphs 1-264 above.

336. As previously alleged, Consumer Plaintiffs and members of the Breach of Implied Contract classes entered into an implied contract that required Home Depot to provide adequate security for the Personal Information it collected from their credit and debit card transactions. As previously alleged, Home Depot owes duties of care to Consumer Plaintiffs and the members of the Nationwide class or, alternatively, the separate statewide Negligence classes, that require it to adequately secure Personal Information.

337. Home Depot still possesses Personal Information regarding the Consumer Plaintiffs' and the Class members.

338. After the Home Depot data breach, Home Depot announced changes that it claimed would improve data security. These changes, however, did not fix many systemic vulnerabilities in Home Depot's computer systems.



339. Accordingly, Home Depot still has not satisfied its contractual obligations and legal duties to Consumer Plaintiffs and the Class members. In fact, now that Home Depot's lax approach towards information security has become public, the Personal Information in Home Depot's possession is more vulnerable than previously.

340. Actual harm has arisen in the wake of Home Depot's data breach regarding its contractual obligations and duties of care to provide security measures to Consumer Plaintiffs and the members of the Breach of Implied Contract and Negligence Classes. Home Depot maintains that its security measures now are adequate even though the changes it announced were insufficient to meet Home Depot's contractual obligations and legal duties.

341. Consumer Plaintiffs, therefore, seek a declaration (a) that Home Depot's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (b) that to comply with its contractual obligations and duties of care, Home Depot must implement and maintain reasonable security measures, including, but not limited to: (1) ordering that Home Depot 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, and ordering Home Depot to promptly correct any problems or issues detected by such

third-party security auditors; (2) ordering that Home Depot engage third-party security auditors and internal personnel to run automated security monitoring; (3) ordering that Home Depot audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Home Depot segment customer 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; (5) ordering that Home Depot purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services; (6) ordering that Home Depot conduct regular database scanning and securing checks; (7) ordering that Home Depot routinely and continually 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 (8) ordering Home Depot to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Home Depot customers must take to protect themselves.

**COUNT VII**  
**VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT,  
CALIFORNIA CIVIL CODE § 1798.81.5 AND THE CALIFORNIA UNFAIR  
COMPETITION LAW'S UNLAWFUL PRONG  
(ON BEHALF OF THE CALIFORNIA PLAINTIFFS AND  
THE CALIFORNIA CLASS)**

342. California Plaintiffs reallege, as if fully set forth, the allegations of paragraphs 1-264 above.

343. “[T]o ensure that personal information about California residents is protected,” the California Legislature enacted the Customer Records Act, California Civil Code §1798.81.5, which requires that any business that “owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”

344. As described above, Home Depot failed to implement and maintain reasonable security procedures and practices to protect the California Plaintiffs’ and California Class members’ personal information, and thereby violated California Civil Code section 1798.81.5.

345. By violating section 1798.81.5 of the California Customer Records Act, Home Depot is liable to the California Plaintiffs and California Class members for damages under California Civil Code section 1798.84(b).

346. Because Home Depot “violates, proposes to violate, or has violated,” the California Customer Records Act, California Plaintiffs are entitled to injunctive relief under California Civil Code section 1798.84(e).

347. In addition, Home Depot’s violations of the Customer Records Act constitute unlawful acts or practices under California’s Unfair Competition Law, California Business and Professions Code sections 17200, et seq., which provides for restitution damages, and grants the Court discretion to enter whatever orders may be necessary to prevent future unlawful acts or practices.

348. Accordingly, the California Plaintiffs request that the court enter an injunction that requires Home Depot to implement reasonable security procedures and practices, including, but not limited to: (1) ordering that Home Depot 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, and ordering Home Depot to promptly correct any problems or issues detected by such third-party security auditors; (2) ordering that Home Depot engage third-party security auditors and internal personnel to run automated security monitoring; (3) ordering that Home Depot audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Home Depot segment customer 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; (5) ordering that Home Depot purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services; (6) ordering that Home Depot conduct regular database scanning and securing checks; (7) ordering that Home Depot routinely and continually 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 (8) ordering Home Depot to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Home Depot customers must take to protect themselves.

349. California Plaintiffs and members of the California Class seek all remedies available under the California Customer Records Act and the California Unfair Competition Law, including but not limited to, restitution, damages, equitable relief, including injunctive relief, reasonable attorneys' fees and costs, and all other relief allowed under the applicable laws.

**COUNT VIII**  
**VIOLATION OF THE MARYLAND PERSONAL INFORMATION  
PROTECTION ACT AND CONSUMER PROTECTION ACT, MARYLAND  
CODE COMMERCIAL LAW §§ 13-101 ET SEQ., 14-3501 ET SEQ.  
(ON BEHALF OF PLAINTIFF JAMES BURDEN AND THE MARYLAND  
CLASS)**

350. Plaintiff James Burden realleges, as if fully set forth, the allegations of paragraphs 1-264 above.

351. “[T]o protect personal information from unauthorized access, use, modification, or disclosure,” the Maryland Legislature enacted the Personal Information Protection Act, Maryland Code, Commercial Law § 14-3503(a), which requires that any business that “owns or licenses personal information about a [Maryland resident] shall implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations.”

352. As described above, Home Depot failed to implement and maintain reasonable security procedures and practices to protect Mr. Burden’s and the Maryland Class members’ personal information, and thereby violated Maryland Code, Commercial Law section 14-3503(a).

353. Under Maryland Code, Commercial Law section 14-3508, Home Depot’s violations of the Maryland Personal Information Protection Act also constitute unfair or deceptive trade practices prohibited by the Maryland Consumer

Protection Act, and subject to the Consumer Protection Act's enforcement provisions.

354. Accordingly, Home Depot is liable to the Mr. Burden and the Maryland Class members for damages and attorneys' fees under Maryland Code, Commercial Law section 13-408.

355. Mr. Burden and the Maryland Class members seek all remedies available under Maryland law, including but not limited to, damages and attorneys' fees.

### **PRAYER FOR RELIEF**

WHEREFORE, Consumer Plaintiffs, on behalf of themselves and the Classes, respectfully request that the Court enter judgment in their favor that:

- A. certifies the Classes requested, appoints the Consumer Plaintiffs as class representatives of the applicable classes and the Court-appointed Liaison Counsel and Co-Lead Counsel Representing Consumer Plaintiffs as Class counsel;
- B. awards the Consumer Plaintiffs and Class members appropriate monetary relief, including actual and statutory damages, restitution, and disgorgement,
- C. on behalf of Consumer Plaintiffs and the Statewide Consumer Classes, enters an injunction against Home Depot's Deceptive Trade Practices and

- requires Home Depot to implement and maintain adequate security measures, including the measures specified above to ensure the protection of Consumer Plaintiffs' Personal Information, which remains in the possession of Home Depot;
- D. on behalf of Consumer Plaintiffs and the Statewide Data Breach Statute Classes, awards appropriate equitable relief, including an injunction requiring Home Depot to promptly notify all affected customers of future data breaches;
- E. orders Home Depot to pay the costs involved in notifying the Class members about the judgment and administering the claims process;
- F. awards Consumer Plaintiffs and the Classes pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and
- G. awards such other and further relief as this Court may deem just and proper.



**JURY TRIAL DEMANDED**

Consumer Plaintiffs demand a trial by jury on all issues so triable.

Dated: May 1, 2015

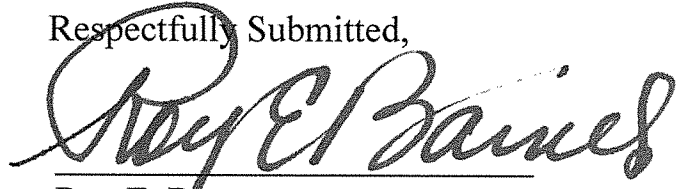
David J. Worley  
James M. Evangelista  
**HARRIS PENN LOWRY, LLP**  
400 Colony Square  
1201 Peachtree Street, NE, Suite 900  
Atlanta, GA 30361  
Telephone: 404-961-7650  
Fax: 404-961-7651  
david@hpllegal.com  
jim@hpllegal.com

*Consumer Co-Lead Counsel  
and Steering Committee Members*

John A. Yanchunis, Sr.  
**MORGAN & MORGAN**  
**COMPLEX LITIGATION GROUP**  
201 N Franklin Street  
Tampa, FL 33602  
Telephone: 813-223-5505  
Fax: 813-223-5402  
jyanchunis@forthepeople.com

*Consumer Co-Lead Counsel  
and Steering Committee Member*

Respectfully Submitted,



Roy E. Barnes  
GA Bar No. 039000  
John R. Bevis  
GA Bar No. 056110  
**THE BARNES LAW GROUP, LLC**  
31 Atlanta Street  
Marietta, GA 30060  
Telephone: 770-227-6375  
Fax: 770.227.6373  
roy@barneslawgroup.com  
bevis@barneslawgroup.com

*Consumer Liaison Counsel  
and Steering Committee Members*

Norman E. Siegel  
Barrett J. Vahle  
**STUEVE SIEGEL HANSON LLP**  
460 Nichols Road, Suite 200  
Kansas City, MO 64112  
Telephone: 816-714-7100  
Fax: 816-714-7101  
siegel@stuevesiegel.com  
vahle@stuevesiegel.com

*Consumer Co-Lead Counsel  
and Steering Committee Members*

Tina Wolfson  
**AHDOOT AND WOLFSON, P.C.**  
1016 Palm Avenue  
West Hollywood, CA 90069  
Telephone: 310-474-9111  
Fax: 310-474-8585  
twolfson@ahdootwolfson.com

*Consumer Plaintiffs’  
Steering Committee Member*

William B. Federman  
**FEDERMAN & SHERWOOD**  
10205 N. Pennsylvania Avenue  
Oklahoma, OK 73120  
Telephone: 405-235-1560  
Fax: 405-239-2112  
wbf@federmanlaw.com

*Consumer Plaintiffs’  
Steering Committee Member*

Howard T. Longman  
**STULL STULL & BRODY**  
6 East 45th Street  
New York, NY 10017  
Telephone: 212-687-7230  
Fax: 212-490-2022  
hlongman@ssbny.com

*Consumer Plaintiffs’  
Steering Committee Member*

Daniel C. Girard  
**GIRARD GIBBS LLP**  
601 California Street, 14th Floor  
San Francisco, CA 94108  
Telephone: 415-981-4800  
Fax: 415-981-4846  
dgc@girardgibbs.com

*Consumer Plaintiffs’  
Steering Committee Member*

Gary S. Graifman  
**KANTROWITZ, GOLDHAMER  
& GRAIFMAN, P.C.**  
210 Summit Avenue  
Montvale, NJ 07645  
Telephone: 201-391-7600  
Fax: 201-307-1086  
ggraifman@kgglaw.com

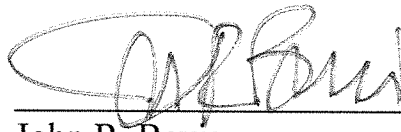
*Consumer Plaintiffs’  
Steering Committee Member*

**CERTIFICATE OF SERVICE**

I hereby certify that on this day I served the above and foregoing on all parties by causing a true and correct copy to be filed with the court's electronic filing system, which automatically sends a copy to all counsel of record.

This 1<sup>st</sup> day of May, 2015.

BARNES LAW GROUP, LLC

A handwritten signature in black ink, appearing to read "John R. Bevis", is written over a horizontal line.

John R. Bevis

GA Bar No. 056110

31 Atlanta Street  
Marietta, GA 30060  
Telephone: 770-227-6375  
Facsimile: 770-227-6373