Jason S. Hartley (CA Bar No. 192514)
Jason M. Lindner (CA Bar No. 211451)
STUEVE SIEGEL HANSON LLP
550 West C Street, Suite 1750
San Diego, CA 92101
Phone: (619) 400-5822
Fax: (619) 400-5832
hartley@stuevesiegel.com
lindner@stuevesiegel.com

Norman E. Siegel
(*pro hac vice forthcoming*)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Phone: (816) 714-7100
Fax: (816) 714-7101
siegel@stuevesiegel.com

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE SOUTHERN DISTRICT OF CALIFORNIA

JOSEPH MORAN,
on behalf of himself and all others similarly situated,

Plaintiff,

v.

HOME DEPOT U.S.A., INC.,

Defendant.

CASE NO. **'14CV2375 MMAKSC**

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Joseph Moran, individually and on behalf of the Class defined below of similarly situated persons, alleges the following against Home Depot U.S.A., Inc. ("Home Depot" or "Defendant") based upon personal knowledge with respect to himself 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 ACTION

1. Plaintiff brings this consumer class action against Home Depot for its failure to secure and safeguard its customers' credit and debit card numbers, three-digit security codes and other payment card data ("PCD"), personally identifiable information such as the cardholder's names, mailing addresses, e-mail addresses and other personal information ("PII") (collectively "Personal Information"), and for failing to provide timely and adequate notice to Plaintiff and other Class members that their Personal Information had been stolen and precisely what types of information were stolen.

2. Home Depot permitted unauthorized access of its customers' Personal Information from April of 2014 to at least September 2, 2014 in its U.S. and Canadian stores. As a result of Home Depot's own acts and omissions, Home Depot's point-of-sale system exposed Defendant Home Depot's customers' Personal Information to criminals. The Personal Information of millions of Home Depot customers was accessed without their knowledge or authorization, including debit and credit card account information (the "Data Breach").

3. On September 2, 2014, security blogger Brian Krebs first reported that "[m]ultiple banks say they are seeing evidence that Home Depot stores may be the source of a massive new batch of stolen credit and debit cards that went on sale this morning in the cybercrime underground."[1]

[1] <http://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/> (last visited Oct. 3, 2014).

4. That same day, after the facts of the data breach were made public, Home Depot issued a statement disclosing only that there "might" be a "possible payment data breach." This statement was not one designed to notify affected customers directly. Instead, Home Depot posted the statement on its corporate website and not on the front page of the Home Depot shopping site regularly accessed by customers.

5. On September 7, 2014, Brian Krebs reported that Home Depot's store registers had been infected with a new variant of "BlackPOS," the malicious software (or malware) used to perpetrate the widely-reported Target Corporation data breach.[2] Krebs further reported that "[c]lues 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."[3]

6. On September 8, 2014, six days after the breach was first reported, Home Depot finally issued a press release confirming the massive breach of its customers' Personal Information.[4]

7. Experts believe that Home Depot's data breach could be significantly larger than the massive data breach experienced by Target Corporation. Indeed, more than 60 million credit card numbers may have already been stolen from Home Depot's payment system. "Comparatively, hackers stole data for over 40 million cards from Target's system following a three-week attack during the busy Black Friday shopping season. However, the breach at Home Depot went undetected for a much longer period of time . . . all customers that have shopped in a retail store in

---

[2] <http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/> (last visited Oct. 3, 2014).

[3] *Id*.

[4] <https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf> (last visited Oct. 3, 2014).

the U.S. or Canada (more than 2,250 locations, 400 more than affected Target stores) and paid with a debit or credit card."[5]

8. Home Depot's security protocols were so deficient that the Data Breach continued for nearly five months while Home Depot failed to even detect it. Home Depot disregarded Plaintiff's and Class members' rights by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, and failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' Personal Information.

9. Plaintiff, on behalf of himself and others similarly situated, asserts claims for violations of the California Consumer Records Act, Civil Code Sections 1798.81.5 and 1798.82, and violations of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. ("UCL").

JURISDICTION AND VENUE

10. This Court has 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 Plaintiff and Defendant are citizens of different states. There are more than 100 putative class members.

11. This Court has jurisdiction over Home Depot because Home Depot U.S.A., Inc. is registered to conduct business in California, Home Depot has sufficient minimum contacts in California, or otherwise intentionally avails itself of the markets within California, through the promotion, sale, marketing and distribution of its products in California, to render the exercise of jurisdiction by this Court proper and necessary.

[5] <http://news.yahoo.com/home-depot-massive-credit-card-data-breach-may-105054766.html> (last visited Oct. 3, 2014).

12. Venue is proper in this District under 28 U.S.C. § 1391 because Plaintiff Joseph Moran resides in this District and a substantial part of the events giving rise to Joseph Moran's claims occurred in this District.

PARTIES

13. Plaintiff Joseph Moran, a resident of Oceanside, California, used his Navy Federal Credit Union Visa credit card to purchase goods at a Home Depot store during the period of the Data Breach. Plaintiff Moran's personal information associated with his credit card was compromised as a result of the Home Depot data breach. Plaintiff Moran was harmed by having his financial and personal information compromised. He incurred multiple unauthorized charges from overseas. Plaintiff Moran's bank froze his account and his Visa credit card was declined while attempting to pay for $1500 worth of car repairs. As a result, Plaintiff Moran was forced to pay with another card and was unable to reap the benefits of the more substantial reward points associated with his Visa card. Plaintiff Moran also felt embarrassment when his card was declined and lost access to his account funds as a result of the Home Depot Data Breach.

14. Defendant Home Depot is a Delaware corporation with its headquarters at 2455 Paces Ferry Road, Atlanta, Georgia, 30339. Home Depot operates retail stores throughout the United States.

FACTUAL BACKGROUND

Home Depot's Information Collection

15. Home Depot operates approximately 1,977 retail stores in the United States and another 180 in Canada. Home Depot is the world's largest home improvement retailer and fourth largest retailer in the United States. In 2013, Home Depot generated $78.8 billion in sales and $5.4 billion in profit.

16. When consumers make purchases at Home Depot retail stores using credit or debit cards, Home Depot collects PCD related to those cards including the

card holder name, the account number, expiration date, card verification value, and PIN data for debit cards. Home Depot stores the PCD in its point-of-sale system and transmits this information to a third party for completion of the payment. Home Depot also collects and stores PII, including but not limited to customer names, mailing addresses, phone numbers, and email addresses.

17. Home Depot uses consumers' Personal Information in ways that greatly exceed the expectations of customers. Through its Privacy Policy, which is available on its website, Home Depot identifies the categories of Personal Information it collects:

> **Information We Collect**
>
> **Contact information**
>
> We may collect the names and user names of our customers and other visitors. Additionally, we may collect your purchase history, billing and shipping addresses, phone numbers, email addresses, and other digital contact information. We may also collect information that you provide us about others.
>
> **Payment information**
>
> When you make a purchase we collect your payment information, including information from your credit or debit card, check, PayPal account or gift card. If you apply for a The Home Depot credit card or a home improvement loan, we might collect information related to your application.
>
> **Returns information**
>
> When you return a product to our stores or request a refund or exchange, we may collect information from you and ask you to provide your government issued ID. We use the information we collect from you and capture off of your government issued ID to help prevent fraud. To learn more about our Returns Policy, click here.
>
> **Demographic information**
>
> We may collect information about products or services you like, reviews you submit, or where you shop. We might also collect information like your age or gender.

Location information

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

Other information

If you use our websites, we may collect information about the browser you are using. We might track the pages you visit, look at what website you came from, or what website you visit when you leave us. We collect this information using the tracking tools described here. To control those tools, please read the Your Privacy Preferences section.[6]

18. Home Depot collects Personal Information not only from 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."[7]

19. The information is used for any number of purposes including "[e]ntering you into a sweepstakes or sending you prizes you might have won;" for "security purposes . . . to protect [Home Depot and its] customers;" and "for [Home Depot's] marketing." Personal information collected by Home Depot is also shared with "third parties who perform services on [Home Depot's] behalf;" "to offer financial products, such as The Home Depot credit card and home improvement loans;" for "Data Sharing for Catalog Mailings" and even to "protect [Home Depot] . . .if [Home Depot] suspect[s] fraud."[8]

20. Any associate of Home Depot can access complete sales data on any credit, debit, or check transaction via a browser-based terminal or point-of-sale device. Home Depot compiles and maintains files concerning consumers' financial

[6] <http://www.homedepot.com/c/Privacy_Security> (last visited Oct. 3, 2014).

[7] *Id*.

[8] *Id*.

and credit histories. Home Depot regularly engages, in part, in the practice of assembling and/or evaluating consumer credit information or other information. Home Depot supplies that information to third-parties, including banks. Defendant Home Depot's collection, maintenance and dissemination of its customers' data, relates, in part, to the customers' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, and is, from time to time, used or expected to be used or collected for the purpose of serving as a factor in establishing eligibility for credit, including for Home Depot's credit card or home improvement loans.

21. Thus, Home Depot stores massive amounts of Personal Information on its servers and utilizes this information, not to protect the Personal Information of its customers, but to maximize its profits through third-party affiliates, predictive marketing and other marketing techniques.

22. Consumers place value in data privacy and security, and they consider it when making purchasing decisions. Plaintiff would not have made purchases at Home Depot, or would not have paid as much for the goods they purchased, had they known that Home Depot does not take all necessary precautions to secure their personal and financial data.

Home Depot Failed to Comply With Industry Standards

23. Home Depot accepts customer payment for goods or services made by credit and debit cards issued by members of the Payment Card Industry, such as Visa, MasterCard, Discover, and American Express.

24. Unlike PII data, PCD (or payment card data) is heavily regulated. The Payment Card Industry Security Standards Council formed a body of security standards known as the PCI Data Security Standards ("PCI DSS") which consist of significant requirements including multiple sub-requirements which contain

numerous directives against which businesses may measure their own payment card security policies, procedures and guidelines.

25. The PCI DSS was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data and/or sensitive authentication data.[9]

26. PCI DSS requires merchants to: build and maintain a secure network and system; protect cardholder data; maintain a vulnerability and management program; implement strong access control measures; regularly monitor and test networks; and maintain an information security policy.[10]

27. Home Depot is contractually-obligated to fully comply with all of the PCI DSS requirements and individual PCI members' requirements as a condition of being permitted to process transactions through the PCI members' networks.

28. At all times relevant to this action, Home Depot held itself out as comporting with PCI DSS and was, therefore, authorized by PCI members to accept credit and debit cards for the payment of personal goods and services.

29. The PCI DSS is an industry standard for large retail institutions that accept credit card and debit card transactions. The standard consists of 12 general requirements:

a. Install and maintain a firewall configuration to protect cardholder data;

b. Do not use vendor-supplied defaults for system passwords and other

[9] <https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf> (last visited Oct. 3, 2014).

[10] *Id*.

security parameters;

c. Protect stored cardholder data;

d. Encrypt transmission of cardholder data and sensitive information across public networks;

e. Protect all systems against malware and regularly update anti-virus software or programs;

f. Develop and maintain secure systems and applications;

g. Restrict access to cardholder data by business need-to-know;

h. Identify and authenticate access to system components;

i. Restrict physical access to cardholder data;

j. Track and monitor all access to network resources and cardholder data;

k. Regularly test security systems and processes; and

l. Maintain a policy that addresses information security for all personnel.[11]

30. Despite Home Depot's awareness of its data protection obligations, Home Depot's treatment of the financial account and personally identifying information entrusted to it by its customers fell far short of satisfying Home Depot's legal duties and obligations. Home Depot failed to ensure that access to its data systems was reasonably safeguarded. Home Depot 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.

31. Home Depot did not comply with the PCI DSS or Card Operating Regulations. As a result of Home Depot's inadequate data security, cyber-criminals now possess the personal and financial information of Plaintiff and the Class. While credit card companies offer protection against unauthorized charges, the process is

[11] *Id.*

long, costly, and frustrating. Physical cards must be replaced, credit card information must be updated on all automatic payment accounts, and victims must add themselves to credit fraud watch lists, which substantially impair victims' ability to obtain additional credit.

The Home Depot Data Breach

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

33. That same day, multiple banks began reporting evidence that Home Depot stores were the likely source of a massive batch of stolen card data that went on sale that morning at rescator.cc, the same underground cybercrime shop that sold millions of cards stolen in the 2013 attack on Target.[12]

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

35. The Krebs Report explained that "experienced crooks prefer to purchase cards that were stolen from stores near them, because they know that using the cards for fraudulent purchases in the same geographic area as the legitimate cardholder is less likely to trigger alerts about suspicious transactions—alerts that could render the stolen card data worthless for the thieves."[13] The Krebs Report indicated a "staggering 99.4 percent overlap" between the unique ZIP codes

[12] <http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/> (last visited Oct. 3, 2014).

[13] <http://krebsonsecurity.com/2014/09/data-nearly-all-u-s-home-depot-stores-hit/> (last visited Oct. 3, 2013).

represented on the Rescator website and those of Home Depot stores, strongly suggesting that the source of the breached credit card data was from Home Depot.[14]

36. The ZIP code information the Krebs Report pulled from the Rescator website appears to represent the vast majority, if not all, of Home Depot's approximately 2,000 domestic retail locations. The Krebs Report further indicated that, based on conversations with affected banks, this data breach "probably started in late April or early May" and may be ongoing, potentially dwarfing the 40 million debit and credit cards affected by the recent Target data breach (which had 1,800 stores affected during a period of approximately 3 weeks).

37. After this news broke, on September 3, 2014, Home Depot released an ambiguous and uninformative statement on its corporate site (now removed and not the Internet site visited by consumers) that failed to confirm the Data Breach:

> We're looking into some unusual activity that might indicate a possible payment data breach and we're working with our banking partners and law enforcement to investigate. We know that this news may be concerning and we apologize for the worry this can create. If we confirm a breach has occurred, we will make sure our customers are notified immediately.[15]

38. On September 8, 2014, Home Depot confirmed that its systems had been breached and conceded that compromised information may include "[p]ayment card information such as name, credit card number, expiration date, cardholder verification value and service code for purchases made at Home Depot stores in 2014, from April on."[16]

39. "The stolen card data being offered for sale on [the Rescator website] includes both the information needed to fabricate counterfeit cards as well *as the*

---

[14] *Id*.

[15] <http://patch.com/massachusetts/concord/home-depot-investigating-possible-data-breach-0#.VBmySvldUjY> (last visited Oct. 3, 2014).

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

legitimate cardholder's full name and the city, state and ZIP of the Home Depot store from which the card was stolen."[17] Information pertaining to the cardholder's location allows hackers to obtain a cardholder's Social Security number and date of birth, further increasing the risk of identity theft (above and beyond fraudulent credit and/or debit card transactions) for affected Home Depot customers.

40. Thieves already are using the Personal Information stolen from Home Depot to commit actual fraud. Some thieves are using the Personal Information to change a cardholder's PIN numbers on stolen debit cards and to make ATM withdrawals from Home Depot customer's accounts. On September 8, 2014, a bank located on the West Coast reported that it "lost more than $300,000 in two hours today to PIN fraud on multiple debit cards that had all been used recently at Home Depot."[18] On that same day, the Krebs Report advised that multiple financial institutions had reported "a steep increase over the past few days in fraudulent ATM withdrawals on customer accounts."[19]

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

42. The software used in the attack was a variant of "BlackPOS," a malware strain designed to siphon data from cards when they are swiped at infected point-of-sale systems.[20] Hackers had previously utilized BlackPOS in other recent cyber-attacks, including the 2013 breach at Target. While many retailers, banks and card companies have responded to these recent breaches by adopting technology and

---

[17] <http://krebsonsecurity.com/2014/09/in-wake-of-confirmed-breach-at-home-depot-banks-see-spike-in-pin-debit-card-fraud/> (last visited Oct. 3, 2014).

[18] *Id*.

[19] *Id*.

[20] <http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/> (last visited Oct. 3, 2014).

security practices that help makes transactions and stored data more secure, Home Depot did not do so.

43. Moreover, in July 2014, the Homeland Security Department and the Secret Service issued a report warning retailers to check their in-store cash register systems for a set of malware that could evade detection of antivirus products.[21] On information and belief, Home Depot could have taken immediate action to ensure that its consumers' Personal Information would not continue to be available to hackers and identity thieves, but Home Depot chose not to take such action.

44. According to *Bloomberg*, managers within the company stated that Home Depot was using out-of-date anti-virus software on its point-of-sale devices. They noted that while Home Depot had purchased software designed to encrypt credit card data when it was being sent from POS devices to central servers, Home Depot had yet to implement the software. The sources also stated that Home Depot's technology executives were underfunding the company's information security program, leading to higher-than-average levels of security staff turnover.[22]

45. On September 19, 2014, an article in the *New York Times* entitled "*Ex-Employees Say Home Depot Left Data Vulnerable*" confirmed that former employees were raising alarms in Home Depot's cyber-security as far back as 2008.[23] The article stated that "Home Depot relied on outdated software to protect its network and scanned systems that handled customer information irregularly, those [former employees] said. Some members of its security team left as managers dismissed their concerns. Others wondered how Home Depot met industry standards

---

[21] <http://www.nytimes.com/2014/09/03/technology/home-depot-data-breach.html?_r=0> (last visited Oct. 3, 2014).

[22] <http://www.businessweek.com/articles/2014-09-12/home-depot-didnt-encrypt-credit-card-data-former-workers-say> (last visited Oct. 3, 2014).

[23] <http://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html> (last visited Oct. 3, 2014).

for protecting customer data. One went so far as to warn friends to use cash, rather than credit cards, at the company's stores."[24]

46. According to the *New York Times* article, "Home Depot's security group in recent years said managers failed to take such threats as seriously as they should have. They said managers relied on outdated Symantec antivirus software from 2007 and did not continuously monitor the network for unusual behavior, such as a strange server talking to its checkout registers. Also, the company performed vulnerability scans irregularly on the dozen or so computer systems inside its stores and often scanned only a small number of stores. Credit card industry security rules require large retailers like Home Depot to conduct such scans at least once a quarter, using technologies approved by the Payment Card Industry Security Standards Council, which develops technical requirements for its members' data security programs. The P.C.I. Council requires that approved, third-party quality security assessors perform routine tests to ensure that merchants are compliant." As noted in the article "scanning is the easiest part of compliance."[25]

47. Home Depot clearly failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Personal Information compromised in the Data Breach which directly resulted in the theft and resale of its customers' Personal Information.

Stolen Information Is Valuable to Hackers and Thieves

48. Personal and financial information is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen credit card numbers, Social Security numbers, and other personal information on a number of Internet websites. Indeed, the personal and financial information that Home Depot failed to adequately protect, including Plaintiff's identifying information, is as good as gold

[24] *Id*.

[25] *Id*.

to identity thieves because identity thieves can use victims' personal data to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

49. Plaintiff's and Class members' personal and financial information stolen from Home Depot has flooded the underground black market with card numbers selling between $9 and $50 per card, with business cards, platinum levels and American Express Centurion Cards commanding higher prices.[26]

50. 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 any blocks from banks who suspect fraud. As noted by Krebs, "[t]he card data stolen from Home Depot customers and now for sale . . . 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*."[27]

51. The ramifications of Home Depot's failure to protect Class members' data are severe. Identity thieves can use personal information such as that of Class members, which Home Depot failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of

[26] <http://www.bankinfosecurity.com/analysis-home-depot-breach-details-a-7323> (last visited Oct. 3, 2014).

[27] <http://krebsonsecurity.com/2014/09/in-wake-of-confirmed-breach-at-home-depot-banks-see-spike-in-pin-debit-card-fraud/> (last visited Oct. 3, 2014).

government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years.

52. 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.

53. It is incorrect to assume that reimbursing a consumer for fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[28]

54. Additionally, there is commonly lag time 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.[29]

55. There is a very strong probability that entire batches of stolen card data have yet to be dumped on the black market, meaning Home Depot customers could

[28] <http://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited Oct. 3, 2014).

[29] <http://www.gao.gov/new.items/d07737.pdf> (last visited Oct. 3, 2014).

be at risk of fraud and identity theft for extended periods of time, perhaps even longer than the one year of credit monitoring Home Depot has offered its customers.

56. Plaintiff and the Class have or will suffer actual injury as a direct result of the Data Breach. This not only includes experiencing fraudulent charges on their credit and debit accounts and damage to credit scores and credit reports, but also time and expense relating to:

a. Finding fraudulent charges;
b. Canceling and reissuing cards;
c. Purchasing credit monitoring and identity theft prevention;
d. Imposition of withdrawal and purchase limits on compromised accounts;
e. Inability to withdraw funds linked to compromised accounts;
f. Trips to banks and waiting in line to obtain funds held in limited accounts;
g. Resetting automatic billing instructions; and
h. Late fees and declined payment fees imposed as a result of failed automatic payments.

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

Plaintiff and Class Members Suffered Damages

58. The Data Breach was a direct and proximate result of Home Depot's failure to properly safeguard and protect Plaintiff's and Class members' Personal

Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Home Depot's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' Personal Information to protect against reasonably foreseeable threats to the security or integrity of such information.

59. Plaintiff's and Class members' Personal Information is private and sensitive in nature and was left inadequately protected by Home Depot. Home Depot did not obtain Plaintiff's and Class members' consent to disclose their Personal Information to any other person as required by applicable law and industry standards.

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

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

a. theft of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their credit/debit card and personal

information being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class members' information on the Internet card black market;

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

d. the improper disclosure of their Personal Information;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

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

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

i. the loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts.

62. Plaintiff and members of the Class also purchased products or services they otherwise would not have purchased, or paid more for those products and services than they otherwise would have paid.

CLASS ACTION ALLEGATIONS

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

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

64. Excluded from the Class is Home Depot, including any entity in which Home Depot has a controlling interest, is a parent or subsidiary, or which is controlled by Home Depot, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Home Depot. Also excluded are the judges and court personnel in this case and any members of their immediate families.

65. **Numerosity**. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, based on information and belief, it is in the millions.

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

a. Whether Home Depot owed a duty to Plaintiff and members of the Class to adequately protect their personal and financial information and to provide timely and accurate notice of the Data Breach to Plaintiff and members of the Class;

b. Whether Home Depot knew or should have known that its computer

systems were vulnerable to attack;

c. Whether Home Depot's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of millions of consumers' personal and financial data;

d. Whether Plaintiff and members of the Class suffered injury, including ascertainable losses, as a result of Home Depot's conduct or failure to act;

e. Whether Home Depot's Personal Information storage and protection protocols were reasonable under industry standards;

f. Whether Home Depot violated California Civil Code sections 1798.81 and 1798.81.5 by failing to implement reasonable security procedures and practices;

g. Whether Home Depot violated California Civil Code section 1798.82 by failing to promptly notify class members that their personal information had been compromised;

h. Whether class members may obtain injunctive relief against Home Depot under Civil Code section 1798.84 or under the UCL;

i. Whether Plaintiff and members and Class are entitled to recover actual damages and/or statutory damages; and

j. Whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement and/or other equitable relief.

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

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

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

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

71. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Home Depot's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

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

FIRST CAUSE OF ACTION
Violation of the California Customer Records Act, California Civil Code Section 1798.80, *et seq.*
(On Behalf of Plaintiff and the Class)

73. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

74. Plaintiff Moran brings this cause of action on behalf of himself and the Class who made purchases with a debit or credit card at a Home Depot store within

three years of the filing of this lawsuit through the present.

75. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted Civil Code section 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."

76. Home Depot is a "business" within the meaning of Civil Code section 1798.80(a).

77. Plaintiff Moran and members of Class are "customer[s]" within the meaning of the Civil Code section 1798.80(c) "who provide[d] personal information to [Home Depot] for the purpose of purchasing or leasing a product or obtaining a service from the business." Pursuant to Civil Code sections 1798.80(e) and 1798.81.5(d)(1)(C), "personal information" includes debit card and credit card information.

78. The breach of the data of the debit and credit card information of millions of accounts of Home Depot customers constituted a "breach of the security system" of Home Depot pursuant to Civil Code section 1798.82(g).

79. By keeping customers' personal data within its custody and control longer than necessary, and by failing to properly and adequately dispose or make customers' data undecipherable, Home Depot violated section 1798.81.

80. By failing to implement reasonable measures to protect its customers' personal data, Home Depot violated Civil Code section 1798.81.5.

81. In addition, by failing to promptly notify all affected Home Depot customers that their personal information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the data breach, Home Depot violated Civil Code section 1798.82 of the same title.

82. By violating Civil Code sections 1798.81, 1798.81.5 and 1798.82, Home Depot "may be enjoined" under Civil Code section 1798.84(e).

83. Accordingly, Plaintiff Moran requests that the Court enter an injunction requiring Home Depot to implement and maintain reasonable security procedures to protect customers' data in compliance with the California Customer Records Act, including, but not limited to: (1) ordering that Home Depot, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Home Depot's systems on a periodic basis; (2) ordering that Home Depot engage third party security auditors and internal personnel, consistent with industry standard practices, 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, consistent with industry standard practices, 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, destroy in a reasonable secure manner customer data not necessary for its provisions of services; (6) ordering that Home Depot, consistent with industry standard practices, conduct regular database scanning and securing checks; (7) ordering that Home Depot, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (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.

84. Plaintiff Moran further requests that the Court require Home Depot to

(1) identify and notify all members of the Class who have not yet been informed of the data breach; and (2) to notify affected customers of any future data breaches by email within 24 hours of Home Depot's discovery of a breach or possible breach and by mail within 72 hours.

85. As a result of Home Depot's violation of Civil Code sections 1798.81, 1798.81.5, and 1798.82, Plaintiff Moran and members of the Class have and will incur economic damages relating to time and money spent remedying the breach, expenses for bank fees associated with the breach, late fees from automated billing services associated with the breach, lack of access to funds while banks issue new cards, as well as the costs of credit monitoring and purchasing credit reports.

86. Plaintiff Moran, individually and on behalf of the members of the Class, seeks all remedies available under Civil Code section 1798.84, including, but not limited to: (a) damages suffered by members of the Class; and (b) equitable relief.

87. Plaintiff Moran, individually and on behalf of the members of the Class, also seeks reasonable attorneys' fees and costs under applicable law.

SECOND CAUSE OF ACTION

Unlawful and Unfair Business Practices Under California Business and Professions Code § 17200, *et seq.*
(On Behalf of Plaintiff and the Class)

88. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

89. Plaintiff Moran brings this cause of action on behalf of himself and the Class whose personal information was compromised as a result of the data breach announced by Home Depot in September 2014.

90. Home Depot's acts and practices, as alleged in this Complaint, constitute unlawful and unfair business practices, in violation of the Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq*.

91. Home Depot's acts and practices, as alleged in this complaint, constitute unlawful practices in that they violate the California Customer Records Act, Civil Code section 1798.80, *et seq*.

92. Home Depot's practices were unlawful and in violation of Civil Code sections 1798.81 and 1798.81.5(b) of the California Customer Records Act because Home Depot failed to take reasonable security measures in protecting its customers' data.

93. Home Depot's practices were also unlawful and in violation of Civil Code section 1798.82 because Home Depot unreasonably delayed informing Plaintiff and members of the Class about the breach of security after Home Depot knew the data breach occurred.

94. The acts, omissions, and conduct of Home Depot constitutes a violation of the unlawful prong of the UCL because they failed to comport with a reasonable standard of care and California public policy as reflected in statutes such as the Online Privacy Protection Act, Cal. Bus. & Prof. Code § 22576, and the Information Practices Act of 1977, Cal. Civ. Code § 1798, *et seq*., which seek to protect customer data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

95. By failing to take reasonable security measures to protect its customers' data, Home Depot engaged in unfair business practices and conduct that undermines or violates the stated policies underlying the California Customer Records Act. Home Depot's failure to take reasonable security measures to protect its customers' data violates the stated policy of the Legislature in that businesses are to protect the personal information of their customers.

96. In unduly delaying informing customers of the data breach, Home Depot engaged in unfair business practices by engaging in conduct that undermines or violates the stated policies underlying the California Customer Records Act and

other privacy statutes. In enacting the California Customer Records Act, the Legislature stated that: "[i]dentity theft is costly to the marketplace and to consumers" and that "victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information is imperative." 2002 Cal. Legis. Serv. Ch. 1054 (A.B. 700). Home Depot's conduct also undermines California public policy as reflected in other statutes such as the Online Privacy Protection Act, Cal. Bus. & Prof. Code § 22576, and the Information Practices Act of 1977, Cal. Civ. Code § 1798, *et seq*., which seek to protect customer data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

97. As a direct and proximate result of Home Depot's unlawful and unfair business practices as alleged herein, Plaintiff Moran and members of the Class have suffered injury in fact. Plaintiff Moran and members of the Class have been injured in that their personal and financial information has been compromised and are at risk for future identity theft and fraudulent activity on their financial accounts, which is evidenced by reports that some of the stolen credit and debit card information are being sold on the online black market.

98. While failing to implement reasonable security measures to protect its customers' personal data, Home Depot continued to unjustly enrich itself by reaping profits from its business transactions with its customers and gaining an unfair market advantage.

99. As a result of Home Depot's violations, Plaintiff Moran and members of the Class are entitled to injunctive relief, including, but not limited to: (1) ordering that Home Depot, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Home Depot's systems on a periodic basis; (2) ordering that Home Depot engage third

party security auditors and internal personnel, consistent with industry standard practices, 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, consistent with industry standard practices, 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, destroy in a reasonable secure manner customer data not necessary for its provisions of services; (6) ordering that Home Depot, consistent with industry standard practices, conduct regular database scanning and securing checks; (7) ordering that Home Depot, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (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.

100. Because of Home Depot's unfair and unlawful business practices, Plaintiff Moran and members of the Class are entitled to relief, including restitution to Plaintiff Moran and members of the Class of their costs incurred associated with the data breach and disgorgement of all profits accruing to Home Depot because of its unlawful and unfair business practices, attorneys' fees and costs, declaratory relief, and a permanent injunction enjoining Home Depot from its unlawful and unfair practices.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class set forth herein, respectfully requests the following relief:

a. That the Court certify this case as a class action pursuant to Fed. R.

Civ. P. 23(a), (b)(2) and/or (b)(3), and, pursuant to Fed. R. Civ. P. 23(g), appoint the named Plaintiff to be a Class representative and their undersigned counsel to be Class counsel;

b. That the Court award Plaintiff and the Class appropriate relief, including actual and statutory damages, restitution and disgorgement;

c. That the Court award Plaintiff and the Class equitable, injunctive and declaratory relief as maybe appropriate under applicable state laws. Plaintiff, on behalf of the Class, seeks appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing best security data practices to safeguard customers' financial and personal information and that would include, without limitation, an order and judgment directing Home to (1) encrypt all sensitive cardholder data beginning within the device to which the cards are presented for purchase (*e.g.*, PIN pad) and continuing until the data reaches Home Depot's payment processor or payment switch; (2) comply with the Payment Card Data Security Standard (PCI DDS); (3) provide to Plaintiff and Class members extended credit monitoring services; (4) equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Home Depots' wrongful conduct; and (5) relief enjoining Home Depot from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' private information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

d. That the Court award Plaintiff and the Class actual damages,

compensatory damages, statutory damages, and statutory penalties, to the full extent permitted by law, in an amount to be determined;

e. That the Court award Plaintiff and the Class pre-judgment and post-judgment interest;

f. That the Court award Plaintiff and the Class reasonable attorney fees and costs as allowable by law; and

g. That the Court award Plaintiff and the Class such other, favorable relief as allowable under law or at equity.

JURY DEMAND

Plaintiff hereby demands a jury trial in the instant action.

Dated: October 7, 2014

Respectfully submitted,

By: s/Jason M. Lindner

Jason Hartley
Jason M. Lindner
STUEVE SIEGEL HANSON LLP
550 West C. Street, Suite 1750
San Diego, CA 92101
Tel: (619) 400-5822
Fax: (619) 400-5832

Norman E. Siegel
(*pro hac vice forthcoming*)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City MO 64112
Tel: (816) 714-7100
Fax: (816) 714-7101

Counsel for Plaintiff and the Class