

Congress of the United States

Washington, DC 20515

September 15, 2014

Mr. Frank Blake
Chief Executive Officer
The Home Depot, Inc.
2455 Paces Ferry Rd. N.W.
Atlanta, GA 30339

Dear Mr. Blake,

According to a New York Times article entitled, “Home Depot Data Breach Could Be the Largest Yet,” the company confirmed that it has experienced a data security breach that could potentially be the largest of a retail company.¹ The article indicates that the total number of credit card numbers stolen could be near 60 million and that the breach could have “affected any customer at Home Depot stores in the United States and Canada from April to early last week.”²

Home Depot, Inc. has been growing since its inception in 1978. According to their investor facts, Home Depot, Inc. is the “world’s largest improvement specialty retailer with fiscal 2013 retail sales of \$78.8 billion and earnings of \$5.4 billion.”³ The company has more than 2,200 stores and has been increasing in locations and net sales since 2009.⁴

Data breaches have become increasingly common – and damaging – in recent years, and we applaud Home Depot, Inc. for offering free identity protection services, including credit monitoring, to concerned customers. However, as members of the Congressional Bi-Partisan Privacy Caucus and original cosponsors of H.R. 4400, the Data Accountability and Trust Act, we have some concerns regarding the data security practices at Home Depot.

While we appreciate the frequently asked questions document released by Home Depot, Inc. regarding the data breach⁵, we request more detailed responses to the questions that follow.

1. How and when did Home Depot, Inc. first learn that a data breach occurred? Please describe the indicating factors that led to such a conclusion.
2. Please describe the data security methods currently practiced by the company to protect consumers from identity theft.

¹ Perlroth, N. (2014, September 8). Home depot data breach could be the largest yet. *The New York Times*. Retrieved September 10, 2014 from http://bits.blogs.nytimes.com/2014/09/08/home-depot-confirms-that-it-was-hacked/?_php=true&_type=blogs&_php=true&_type=blogs&_r=1

² *Id.*

³ The Home Depot (2014). Investor facts & faq. Retrieved September 10, 2014 from <http://phx.corporate-ir.net/phoenix.zhtml?c=63646&p=irol-factsfaq>

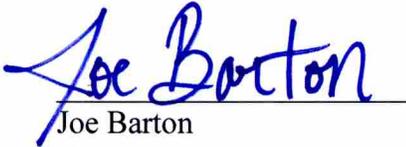
⁴ The Home Depot. (2013). *Form 10-K 2013*. Retrieved from The Home Depot website <http://phx.corporate-ir.net/phoenix.zhtml?c=63646&p=irol-reportsCurrent>

⁵ The Home Depot (2014). FAQs. Retrieved September 11, 2014 from <https://corporate.homedepot.com/MediaCenter/Documents/FAQs.pdf>

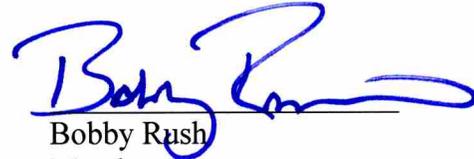
- a. Was Home Depot compliant with the Data Security Standard (PCI DSS) at the time the breach occurred? If not, why not?
 - b. Among PCI Security Standards for which the company is assessed annually, did Home Depot meet the most stringent versions published at the time of the breach? If so, please explain. If not, why not?
 - c. Prior to April 2014, did Home Depot endeavor to implement point-to-point encryption of payment card data, in which such data is immediately encrypted when swiped at the point-of-interaction devices? If not, why not?
3. In the privacy policy for Home Depot, Inc. there is a section on security. In this section, the company indicates that it uses the Secure Sockets Layer (SSL) technology to protect transactions made online, but does not really address data security practices at the register. In recent months a vulnerability known as Heartbleed was discovered in the OpenSSL cryptographic software library. What role, if any, did this vulnerability play in this data breach? Furthermore, what has Home Depot done to mitigate this vulnerability?
4. Since the establishment of Home Depot, Inc. in 1978, how many major data breaches has the company experienced? Has the company noticed a decrease in the number of major data breaches? If not, why not? If so, please explain.
5. What, if anything, did Home Depot learn from last year's breach of Target, Neiman Marcus, and other major retailers? What security measures were implemented in response to those lessons?
6. Do you know, and are you able to share at this time, how the attacker gained access to Home Depot servers? Was it through vendor credentials, like the attack at Target? If so, how were the vendor's credentials obtained by the intruder or intruders? In what capacity was the vendor employed by Home Depot, and to what internal websites, databases, or networks did that vendor have access that could have led to the data theft? What are Home Depot's procedures for screening vendors or employees of vendors before issuing them credentials that can be used to access the company's internal networks?
7. What steps is Home Depot, Inc. taking to better guard against similar future data security breaches?

Please provide responses to these questions within 20 business days or no later than October 13, 2014. If you have any questions, please contact Emmanuel Guillory in Rep. Barton's office at 202-225-2002 or by email at emmanuel.guillory@mail.house.gov.

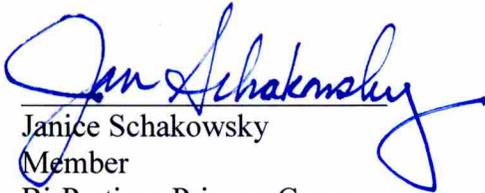
Sincerely,



Joe Barton
Co-Chair
Bi-Partisan Privacy Caucus



Bobby Rush
Member
Bi-Partisan Privacy Caucus



Janice Schakowsky
Member
Bi-Partisan Privacy Caucus