

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

JOHN L. MICA, FLORIDA
MICHAEL R. TURNER, OHIO
JOHN J. DUNCAN, JR., TENNESSEE
PATRICK T. McHENRY, NORTH CAROLINA
JIM JORDAN, OHIO
JASON CHAFFETZ, UTAH
TIM WALBERG, MICHIGAN
JAMES LANKFORD, OKLAHOMA
JUSTIN AMASH, MICHIGAN
PAUL A. GOSAR, ARIZONA
PATRICK MEEHAN, PENNSYLVANIA
SCOTT DESJARLAIS, TENNESSEE
TREY GOWDY, SOUTH CAROLINA
BLAKE FARENTHOLD, TEXAS
DOC HASTINGS, WASHINGTON
CYNTHIA M. LUMMIS, WYOMING
ROB WOODALL, GEORGIA
THOMAS MASSIE, KENTUCKY
DOUG COLLINS, GEORGIA
MARK MEADOWS, NORTH CAROLINA
KERRY L. BENTIVOLIO, MICHIGAN
RON DESANTIS, FLORIDA

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

FACSIMILE (202) 225-3974

MINORITY (202) 225-5051

<http://oversight.house.gov>

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACKIE SPEIER, CALIFORNIA
MATTHEW A. CARTWRIGHT, PENNSYLVANIA
L. TAMMY DUCKWORTH, ILLINOIS
ROBIN L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TONY CARDENAS, CALIFORNIA
STEVEN A. HORSPORD, NEVADA
MICHELLE LUJAN GRISHAM, NEW MEXICO
VACANCY

LAWRENCE J. BRADY
STAFF DIRECTOR

November 12, 2014

Frank Blake
Chairman and CEO
The Home Depot
2455 Places Ferry Road NW
Atlanta, GA 30339

Dear Mr. Blake:

I am writing to request information about a significant data breach recently reported by Home Depot.

According to a report issued by Home Depot on November 6, hackers breached the company's computer systems using "unique, custom-built malware" that compromised approximately 56 million payment cards.¹ Home Depot reported that "approximately 53 million e-mail addresses were also taken during the breach."² This breach of payment data systems is believed to be "the largest known breach of a retail company's computer network."³

Although it is not clear how many instances of fraud may be traced to the Home Depot breach, media reports indicate that the "large data breach at Home Depot, Inc. has started to trigger fraudulent transactions that are rippling across financial institutions and, in some cases, draining cash from customer bank accounts."⁴ Shortly after the breach was exposed, a federal credit union "caught roughly \$20,000 worth of attempted fraudulent transactions tied to cards that were exposed from the Home Depot breach."⁵ In the wake of this breach, several banks

¹ The Home Depot, *The Home Depot Reports Findings in Payment Data Breach Investigation* (Nov. 6, 2014) (online at <https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf>).

² *Id.*

³ *Home Depot Data Breach Could Be the Largest Yet*, New York Times (Sept. 8, 2014) (online at http://bits.blogs.nytimes.com/2014/09/08/home-depot-confirms-that-it-was-hacked/?_php=true&_type=blogs&_r=0).

⁴ *Fraudulent Transactions Surface in Wake of Home Depot Breach*, Wall Street Journal (Sept. 23, 2014) (online at <http://online.wsj.com/articles/fraudulent-transactions-surface-in-wake-of-home-depot-breach-1411506081>).

⁵ *Id.*

reported “seeing fraudulent activity that stems from cards that were used both at Home Depot’s traditional cashier lines and self-service checkout lanes.”⁶

The increasing number of cyber-attacks and data breaches is unprecedented and poses a clear and present danger to our nation’s economic security. Each successive cyber-attack and data breach not only results in hefty costs and liabilities for businesses, but exposes consumers to identity theft and other fraud, as well as a host of other cyber-crimes. Your ability to protect consumers and safeguard their personal information is central to earning and maintaining consumer confidence in our economic system.

The increased frequency and sophistication of cyber-attacks on both public and private entities highlights the need for greater collaboration to improve data security. Your company’s knowledge, information, and experience with this recent data breach will be helpful as Congress examines federal cybersecurity laws and any necessary improvements to protect sensitive consumer and government financial information. To aid in this oversight, I request that Home Depot provide the following information:

- (1) a description of the manner and method by which your company first discovered that its payment data systems were under cyber-attack in 2014;
- (2) the approximate number of consumers that may have been affected by the breach;
- (3) the findings from forensic investigation analyses or reports concerning the breach, including findings about vulnerabilities to malware, the use of data segmentation to protect personally identifiable information, and why the breach went undetected for the length of time it did;
- (4) the individuals or entities suspected or believed to have caused the data breach, and whether they have been reported to the appropriate law enforcement agencies;
- (5) a description of data protection improvement measures your company has undertaken since discovering that its payment data systems had been breached in 2014;
- (6) an estimate of the number and value of fraudulent transactions that were connected to payment cards exposed in the data breach, including the approximate number of federal, state, and local government customers whose information was exposed during the data breach at issue, as well as the number and value of fraudulent transactions that were connected to payment cards from federal, state, and local government customers exposed in the data breach;
- (7) a description of the data security policies and procedures that govern your company’s relationships with vendors, third-party service providers, and subcontractors, including the manner by which your company ensures that entities

⁶ *Id.*

Mr. Frank Blake

Page 3

performing work on your behalf have reasonable data security controls in place to thwart cyber-attacks; and

- (8) any recommendations for improvements in cybersecurity laws or the coordination of efforts to identify and respond to emerging trends in cybersecurity risks to help prevent future data breaches.

Please provide the requested information by December 19, 2014. We also request a briefing from your Chief Information Security Officer or similar chief IT security professional by November 25, 2014. If you have any questions about this request, please contact Timothy D. Lynch at (202) 225-0312. Thank you for your cooperation in this matter.

Sincerely,



Elijah E. Cummings
Ranking Member

cc: The Honorable Darrell E. Issa, Chairman