



## **The Home Depot Completes Malware Elimination and Enhanced Encryption of Payment Data in All U.S. Stores**

\* \* \*

### **Provides Further Investigation Details, Updates Outlook**

**ATLANTA, September 18, 2014** -- The Home Depot<sup>®</sup>, the world's largest home improvement retailer, today confirmed that the malware used in its recent breach has been eliminated from its U.S. and Canadian networks. 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. Roll-out of enhanced encryption to Canadian stores will be complete by early 2015. Canadian stores are already enabled with EMV "Chip and PIN" technology.

The company said its fiscal third quarter sales, including sales in September, are on plan. Additional guidance is provided below.

#### **Investigation Details**

The investigation into a possible breach began on Tuesday morning, September 2, immediately after The Home Depot received reports from its banking partners and law enforcement that criminals may have breached its systems.

Since then, the company's 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, resolve the problem and provide information to customers.

The company's ongoing investigation has determined the following:

- 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.
- The cyber-attack is estimated to have put payment card information at risk for approximately 56 million unique payment cards.
- The malware is believed to have been present between April and September 2014.

To protect customer data until the malware was eliminated, any terminals identified with malware were taken out of service, and the company quickly put in place other security enhancements. The hackers' method of entry has been closed off, the malware has been eliminated from the company's systems, and the company has rolled out enhanced encryption of payment data to all U.S. stores.

There is no evidence that debit PIN numbers were compromised or that the breach has impacted stores in Mexico or customers who shopped online at HomeDepot.com or HomeDepot.ca.

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. Customers who wish to take advantage of these services can learn more at [www.homedepot.com](http://www.homedepot.com) or by calling 1-800-HOMEDEPOT (800-466-3337). Customers in Canada can call 800-668-2266.

“We apologize to our customers for the inconvenience and anxiety this has caused, and want to reassure them that they will not be liable for fraudulent charges,” said Frank Blake, chairman and CEO. “From the time this investigation began, our guiding principle has been to put our customers first, and we will continue to do so.”

### **Payment Security Enhancements**

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.

The encryption project was launched in January 2014. The rollout was completed in all U.S. stores on Saturday, September 13, 2014. The rollout to Canadian stores will be completed by early 2015.

EMV “Chip and PIN” technology, which began rolling out in early 2013 and already exists in Canadian stores, will be deployed to all U.S. stores by the end of the year, well ahead of a 2015 deadline established by the payments industry.

These projects required writing tens of thousands of lines of new software code and deploying nearly 85,000 new pin pads to stores.

### **Updated Guidance**

Based on its fiscal third quarter results to date, the company confirmed its previous fiscal 2014 sales growth guidance of approximately 4.8 percent. The company also revised its fiscal 2014 diluted earnings-per-share growth guidance and expects that fiscal 2014 diluted earnings per share will grow by 21 percent to approximately \$4.54, versus the company’s prior guidance of \$4.52.

The company’s fiscal 2014 diluted earnings-per-share guidance includes estimates for the cost to investigate the data breach, provide credit monitoring services to its customers, increase call center staffing, and pay legal and professional services, all of which are expensed as incurred in a gross amount of approximately \$62 million, partially offset by a \$27 million receivable for costs the company believes are reimbursable and probable of recovery under its insurance coverage. Further, the company’s fiscal 2014 diluted earnings-per-share guidance includes a

pre-tax gain of approximately \$100 million related to the sale of 3.6 million shares of HD Supply common stock, which occurred and will be recognized in the third quarter of fiscal 2014. The company's ownership of HD Supply is now approximately 8.2 million shares.

The company's fiscal 2014 diluted earnings-per-share guidance does not include an accrual for other yet-to-be determined estimated probable losses related to the breach. At this time, other than the breach-related costs contained in the company's updated fiscal 2014 diluted earnings-per-share guidance, the company is not able to estimate the costs, or a range of costs, related to the breach. Costs related to the breach may include liabilities to payment card networks for reimbursements of credit card fraud and card reissuance costs; liabilities related to the company's private label credit card fraud and card reissuance; liabilities from current and future civil litigation, governmental investigations and enforcement proceedings; future expenses for legal, investigative and consulting fees; and incremental expenses and capital investments for remediation activities. Those costs may have a material adverse effect on The Home Depot's financial results in the fourth quarter and/or future periods.

The Home Depot is the world's largest home improvement specialty retailer, with 2,266 retail stores in all 50 states, the District of Columbia, Puerto Rico, U.S. Virgin Islands, Guam, 10 Canadian provinces and Mexico. In fiscal 2013, The Home Depot had sales of \$78.8 billion and earnings of \$5.4 billion. The Company employs more than 300,000 associates. The Home Depot's stock is traded on the New York Stock Exchange (NYSE: HD) and is included in the Dow Jones industrial average and Standard & Poor's 500 index.

###

*Certain statements contained in this release constitute "forward-looking statements" as defined in the Private Securities Litigation Reform Act of 1995. These forward-looking statements are based on our current assumptions and expectations (which may change) and may relate to, among other things, (a) the impact of the breach on our results of operations, including (i) costs related to the breach (including any costs not currently reflected in our guidance), the related ongoing investigation and resulting liabilities, (ii) the outcome of our ongoing investigation, including our potential discovery of new information related to the breach, such as the discovery that additional information has been stolen, and our customers' and other stakeholders' reaction to that new information, (iii) our ability to recover any proceeds under our insurance policies, (iv) the uncertainty regarding the outcome of any current or future civil litigation, governmental investigations and enforcement proceedings, and their impact on our financial performance and operations, (v) loss of customer confidence in our ability to protect their information and the adverse impact this loss of confidence may have on sales, and (vi) our ability to effectively or timely implement adequate payment security enhancements and other remediation efforts and our potential inability to prevent future attacks; (b) the demand for our products, services and credit offerings; (c) net sales growth; (d) comparable store sales; (e) state of the credit markets; (f) continuation of share repurchase programs at previously announced levels; (g) net earnings performance; (h) earnings per share; (i) guidance for fiscal 2014 and beyond; and (j) financial outlook. Forward-looking*

*statements are based on currently available information and our current assumptions, expectations and projections about future events. You should not rely on our forward-looking statements. These statements are not guarantees of future performance and are subject to future events, risks and uncertainties – many of which are beyond our control or are currently unknown to us – as well as potentially inaccurate assumptions that could cause actual results to differ materially from our expectations and projections. These risks and uncertainties include but are not limited to those described in Item 1A, “Risk Factors,” and elsewhere in our Annual Report on Form 10-K for our fiscal year ended February 2, 2014, in our subsequent Quarterly Reports on Form 10-Q and in any other materials or reports we file with the Securities and Exchange Commission (the “SEC”).*

*Forward-looking statements speak only as of the date they are made, and we do not undertake to update these statements other than as required by law. You are advised, however, to review any further disclosures we make on related subjects in our periodic filings with the SEC.*

**For more information, contact:**

*Financial Community*

Diane Dayhoff

Vice President of Investor Relations

770-384-2666

[diane\\_dayhoff@homedepot.com](mailto:diane_dayhoff@homedepot.com)

*News Media*

Stephen Holmes

Director of Corporate Communications

770-384-5075

[stephen\\_holmes@homedepot.com](mailto:stephen_holmes@homedepot.com)