

# Home Depot Needs Reputation Cleanup in Aisle 1

By [Shawn Paul Wood](#)  
Adweek – PR Newser  
November 7, 2014



**BREAKING NEWS (seriously):** Home Depot's image problems just got a lot worse. **More than 53 million emails were stolen** as a result of hackers purchasing credentials stolen from a third-party vendor, [according to Krebs on Security](#).

Someone, somewhere at the great orange temple of home repair did something to piss off [Anonymous](#). You may remember in September the massive data breach Home Depot experienced when ne'er-do-wells harvested information from **56 million credit and debit cards** in the United States and Canada. *And now this?!*

Wait until you here more about where the hackers found this information...

(Image: omacomp.com)

You know those secure self-checkout lanes for when you are too busy to be bothered by anyone? **Yeah, those.**

Home Depot also confirmed that thieves targeted its self-checkout systems, a pattern [first reported on this blog on Sept. 18](#). *The Wall Street Journal* reported that the intruders targeted the 7,500 self-checkout lanes at Home Depot because those terminals were clearly referenced by the company's internal computer system as payment terminals, whereas another 70,000 regular registers were identified simply by a number.

If you were a crisis pro (and many of you in the PRNewsverse are), what would you do?

There are now more than 110 million customers with compromised information and lost trust; some of them were almost certainly hit twice.

What's a brand to do? While the IT guys repair all the holes in its dam with the best silly putty salve they have, how can Home Depot repair that breach in confidence? Is it possible that you have lost them to Lowe's forever?

Unlike [Texas Presbyterian and Burson-Marsteller](#)'s Ebola crisis most such stories don't require a press release — it's cleaner, safer, and easier for businesses to manage them on their own. Shoppers want to know that the business itself is in control, and that it will not happen again. Crisis Communications 101 says to own this, and do it fast.

[Thanks to USA Today](#), we know that Home Depot has attempted to “own” the issue:

Home Depot [said](#) the e-mail addresses did not contain passwords, payment card information or other sensitive personal information. The company is [notifying](#) affected customers and offering [credit monitoring](#), though it said, “In all likelihood this will not impact you.”

Customers were warned to be alert for so-called phishing scams that try to dupe people into revealing personal information or clicking on links that may install malware on their computers. It reiterated [common tips](#) to guard against identity theft. The breach, which has cost \$62 million, began in April and went undetected for several months. Home Depot is offering customers free identity-protection services, including a year of credit monitoring.

“We apologize for the frustration and anxiety this causes our customers and we thank you for your patience and support as we work through this issue,” the company [told](#) customers.

We said it once, and we will say it again: No offense, Home Depot, but with an apology like that, we think you might need some outside help.