Senate Grills Target CFO on Data Breach

Julianne Pepitone NBC News
Feb. 4, 2014 at 11:48 AM ET

> ***Note from Pastor Kevin Lea:*** *More news showing that we are heading toward a new purchasing system that will be based on encrypted data and biometric authentication. Such a system will make it possible for biblical prophecy of the last days to be fulfilled.*

Target CFO John Mulligan faced a Senate judiciary committee on Tuesday to answer tough questions about last year's massive breach that involved 40 million credit cards.

Mulligan apologized twice in his opening remarks for the breach, saying the retailer is "deeply sorry." He reiterated that Target is "undertaking an end-to-end review of our entire network."

The hearing focused broadly on data breaches, not only the attack on Target. Sen. Chuck Grassley, R.-Iowa, noted the committee is concerned that several retailers have suffered attacks recently.

The Target breach grabbed the most headlines due to its massive size, but Neiman Marcus and possibly craft retailer Michaels also suffered breaches in similar attacks last year. The FBI reportedly warned retailers that it uncovered about 20 attacks similar to the one at Target. "This attack has only strengthened our resolve," Mulligan said in his opening statement.

At the hearing -- which also included testimony from representatives of security firms, Neiman Marcus and several government agencies -- Mulligan provided more details about the timeline of the attack. He also laid out Target's plans to boost security.

The Senate panel spoke at length about a major part of that plan: Target now plans to implement chip-and-PIN technology in its own credit cards by early 2015, about six months earlier than its previous goal. (Mulligan previewed those plans in an article he wrote for The Hill late Monday, ahead of the hearing.)

Chip-and-PIN. That chip-and-PIN technology Mulligan referenced adds a smart microchip embedded in the credit card. Customers use a PIN number — rather than a signature — to complete the transaction. If card numbers are stolen, it's more difficult for thieves to create new cards because the chips are tough to copy.

The chip-and-PIN system is widely used in Europe and Canada already. But U.S. retailers and credit-card issuers have been loath to spend the billions of dollars required to create an entirely new payment system. Target itself launched an aborted campaign for chip-and-pin cards about 10 years ago, in a pilot program that involved its own Target Visa REDcard. Target canceled the effort after three years.

A chip-based system could add a level of security, but the technology wouldn't have stopped the 2013 Target breach or others like it, Dave Aitel, the CEO of security firm Immunity told NBC News. The hackers reportedly used software to directly infect the card swipers that Target uses in its physical stores. This software, called a "RAM scraper," grabs credit card data as it is briefly unencrypted as it passes through the computer's memory.

"[Chip-and-PIN] isn't the final answer, and I think Target knows that on some level," Aitel said. "If the card data is stolen, unencrypted, [chip-and-PIN] is just as vulnerable to that type of attack...

> *To read this article in its entirety, go to:*
> http://www.nbcnews.com/technology/senate-grills-target-cfo-data-breach-2D12054052