14-CBS News-Target executive

Target executive apologizes to Congress for data breach

By Paula Reid

February 4, 2014 / 11:30 AM

/ CBS News

The retail giant's chief financial officer testifies before the Senate Judiciary Committee during a hearing on cybercrime Target CFO "deeply sorry" for data breach 02:37

Updated 2:55 p.m. ET

Target's Executive Vice President and Chief

Financial Officer, John Mulligan, apologized to the Senate Judiciary Committee Tuesday over the massive data breach that affected millions of its shoppers .

"I want to say how deeply sorry we are for the impact

this incident has had on our guests – your constituents *[Rebuild]*," Mulligan told the committee.

Target security breach much worse than first reported 02:09

The data breach affected guests who shopped at Target stores in the U.S. between Nov. 27 and Dec. 18. Payment card data was compromised for up to 40 million people and personal data, including name, mailing address, phone number or emails address, was compromised for up to 70 million guests.

Mulligan testified that "We now know that the intruder

stole a vendor's credentials to access our system and place malware on our point of sale registers." *[Rebuild]*

The malware was able to capture payment card data from

magnetic strips on credit and debit cards prior to encryption.

Committee chairman Patrick Leahy, D-Vt., opened the

hearing by warning, "If consumers lose faith in business' ability to protect their personal information, our economic recovery will falter." *[Rebuild]*

There have been reports that several other high-profile

stores have been the targets of similar attacks, including Neiman Marcus .

Neiman Marcus Senior Vice President and Chief Information Officer Michael R. Kingston, told the committee that his company is "in the midst of an ongoing forensic investigation that has revealed a cyber attack using very sophisticated malware."

He said the Secret Service has confirmed that the malware that penetrated the system was "exceedingly sophisticated." The malware was evidently able to capture card data as soon as the card was swiped and was especially difficult to detect.

Account information from transactions in 77 of their 85 stores, between July and October 2013, was potentially exposed to the malware.

Leahy added a laundry list of other companies and government agencies that have been victims to cybercrime, telling the panel, "There have been significant data breaches involving Sony, Epsilon, and Coca-Cola, as well as federal government agencies, such as the Departments of Veterans Affairs and Energy."

He also said in the past few days, there have also been

breaches at Yahoo! and White Lodging, the hotel management company for national hotel chains such as Marriott and Starwood.

Delara Derakhshani, policy counsel at Consumers Union

(the policy and action division of Consumer Reports) testified on the dire consequences for consumers who are the victims of data theft.

"Consumers have to cancel cards and must monitor their

credit reports and continue to do so in the future," *[Disappointment, Anger]* she said.

"While consumers might not ultimately be held responsible

if someone steals their debit card and pin number, data thieves can still empty out consumers bank accounts and set off a cascade of bounced checks and late feeds which victims will have to settle down the road." *[Worry]*

Derakhshani emphasized the importance of using EMV "smart

cards – which have multiple layers of security and require PINs. She also called upon lawmakers to ensure that consumers are notified when a breach occurs and asked the committee to consider shortening the timeline for notification from the 60 days currently in propose legislation to require more immediate notification.

Senators on the panel acknowledged that the purpose of

the hearing was not simply to demand answers from retailers, but for government and the private sector to work together to improve customer confidence during a time of economic recovery.

"How can government encourage private sector to improve

cyber security?" Sen. Chuck Grassley, R-Iowa, the committee's top Republican, asked the panel.

Fran Rosch, Senior Vice President of Mobility at Symantec

told the committee, “This is an ongoing war – the types of threats are changing all the time – we are constantly raising the bar. The legislation needs to be flexible.” *[Anger]*

Leahy agreed saying, “You couldn’t tell me to my

face what will be the greatest threat 18 months from now.” *[Anger]*

Sen. Dianne Feinstein, D-Calif., pressed the retail executives on how they notified customers of the breach *[Anger]*.

She noted that she shops at Neiman Marcus, but was never notified of the breach *[Anger]*.

“I would have shopped during that time. When would I have gotten a notification?” *[Anger]* she asked.

She also criticized Target for not notifying individual

customers *[Anger]*. Mulligan told the senators

that Target decided to do a “broad disclosure” through the media based on the scale of the breach. *[Rebuild]*

Feinstein was not satisfied by this method of

notification. “I believe if someone uses

their credit at your institution and their data is breached – they should be notified. *[Anger]* Public notification is vague – you really don’t know *[Anger, Disappointment]*,” she said.

Target later pointed out that the company did notify those affected and that in Mulligan’s official printed statement to the committee explained t Retail executives testify about credit card security *[Rebuild]* 01:26

hat Target “used multiple forms of communication, including a mass-scale public announcement, email, prominent notices on our website, and social media channels.” *[Rebuild]*

The non-retail members of the panel espoused the virtue

of "chip and PIN" technology which could provide additional security. These cards have a chip in each card that stores and transmits encrypted data as well as a unique PIN identifier that can change with each transaction. *[Hope]*

A recurring theme in the panel was how quickly the

threats evolve and that there are more targets available for thieves.

"Our environments are changing quickly. Today information

is everywhere – it is in a data center, in a cloud…the threats are changing and so is the attack surface," said Rosch.

Implementing more robust protections is costly and

complicated and retailers said the major impediments for stronger cybersecurity is the changing landscape.

"These recent cyber attacks are very sophisticated,

something we have not seen before. Important for all actors to adopt changes at the same time - consumers and the private sector as well, *[Hope]*" added Kingston.

Target is currently working with the Secret Service and the Justice Department on the investigation. Attorney General Eric Holder told the Senate Judiciary Committee last week that he intends to hold the perpetrators of the Target data breach "accountable. *[Hope]*"

In 2013, it is estimated the global cost of consumer cybercrime was $113 billion with 378 million victims per year.

Trending News