Exclusive: Target hackers stole encrypted bank PINs - source

By Jim Finkle and David Henry

BOSTON/NEW YORK Wed Dec 25, 2013 12:44am EST

http://www.reuters.com/article/2013/12/25/us-target-databreach-idUSBRE9BN0L220131225

U.S. Senator Charles Schumer, is pictured through a Target shopping cart, as he holds a news conference about the massive credit card hack that has affected 40 million Target customers, in the Harlem area of New York December 22, 2013.

Credit: Reuters/Carlo Allegri

(Reuters) - The hackers who attacked Target Corp and compromised up to 40 million credit cards and debit cards also managed to steal encrypted personal identification numbers (PINs), according to a senior payments executive familiar with the situation.

One major U.S. bank fears that the thieves would be able to crack the encryption code and make fraudulent withdrawals from consumer bank accounts, said the executive, who spoke on the condition of anonymity because the data breach is still under investigation.

Target spokeswoman Molly Snyder said "no unencrypted PIN data was accessed" and there was no evidence that PIN data has been "compromised." She confirmed that some "encrypted data" was stolen, but declined to say if that included encrypted PINs.

"We continue to have no reason to believe that PIN data, whether encrypted or unencrypted, was compromised. And we have not been made aware of any such issue in communications with financial institutions to date," Snyder said by email. "We are very early in an ongoing forensic and criminal investigation."

The No. 3 U.S. retailer said last week that hackers stole data from as many as 40 million cards used at Target stores during the first three weeks of the holiday shopping season, making it the second-largest data breach in U.S. retail history.

Target has not said how its systems were compromised, though it described the operation as "sophisticated." The U.S. Secret Service and the Justice Department are investigating. Officials with both agencies have declined comment on the investigations.

The attack could end up costing hundreds of millions of dollars, but it is unclear so far who will bear the expense.

While bank customers are typically not liable for losses because of fraudulent activity on their credit and debit cards, JPMorgan Chase & Co and Santander Bank said they have lowered limits on how much cash customers can take out of teller machines and spend at stores.

The unprecedented move has led to complaints from consumer advocates about the inconvenience it caused from the late November Thanksgiving holiday into the run-up to Christmas. But sorting out account activity after a fraudulent withdrawal could take a lot more time and be worse for customers.

JPMorgan has said it was able to reduce inconvenience by giving customers new debit cards printed quickly at many of its branches, and by keeping branches open for extended hours. A Santander spokeswoman was not available for comment on Tuesday.

Security experts said it is highly unusual for banks to reduce caps on withdrawals, and the move likely reflects worries that PINs have fallen into criminal hands, even if they are encrypted.

"That's a really extreme measure to take," said Avivah Litan, a Gartner analyst who specializes in cyber security and fraud detection. "They definitely found something in the data that showed there was something happening with cash withdrawals."

BREAKING THE CODE

While the use of encryption codes may prevent amateur hackers from obtaining the digital keys to customer bank deposits, the concern is the coding cannot stop the kind of sophisticated cyber criminal who was able to infiltrate Target for three weeks.

Daniel Clemens, CEO of Packet Ninjas, a cyber security consulting firm, said banks were prudent to lower debit card limits because they will not know for sure if Target's PIN encryption was infallible until the investigation is completed.

As an example of potential vulnerabilities in PIN encryption, Clemens said he once worked for a retailer who hired his firm to hack into its network to find security vulnerabilities. He was able to access the closely guarded digital "key" used to unscramble encrypted PINs, which he said surprised his client, who thought the data was secure.

In other cases, hackers can get PINs by using a tool known as a "RAM scraper," which captures the PINs while they are temporarily stored in memory, Clemens said.

The attack on Target began on November 27, the day before the Thanksgiving holiday and continued until December 15. Banks that issue debit and credit cards learned about the breach on December 18, and Target publicly disclosed the loss of personal account data on December 19.

On December 21, JPMorgan, the largest U.S. bank, alerted 2 million of its debit cardholders that it was lowering the daily limits on ATM withdrawals to $100 and capping store purchases with their cards at $500.

On Monday, the bank partly eased the limits it had imposed on Saturday, setting them at $250 a day for ATM withdrawals and $1,000 a day for purchases. (The usual debit card daily limits are $200 to $500 for cash withdrawals and $500 for purchases, a bank spokeswoman said last week.)

On Monday, Santander - a unit of Spain's Banco Santander - followed suit, lowering the daily limits on cash withdrawals and purchases on Santander and Sovereign branded debit and credit cards of customers who used them at Target when the breach occurred. Santander did not disclose the new limits, but said it was monitoring the accounts and issuing new cards to customers who were affected.

The largest breach against a U.S. retailer, uncovered in 2007 at TJX Cos Inc, led to the theft of data from more than 90 million credit cards over about 18 months.

(Reporting by Jim Finkle in Boston and David Henry in New York, Additional reporting by Dhanya Skariachan in New York; Writing by Paritosh Bansal, Editing by Tiffany Wu and Grant McCool)