

15-NBC News-Target confirms encrypted

Target confirms encrypted PINs stolen in data breach

Link copied

Dec. 27, 2013, 7:20 PM UTC

By Jim Finkle and Dhanya Skariachan

People shop inside a Target store during Black Friday sales in Brooklyn on Nov. 29, 2013. Target confirmed Friday that encrypted PINs were stolen in a breach of payment card data in the first three weeks of the holiday shopping season.ERIC THAYER / Reuters

Target Corp. said Friday that PIN data of its customers' bank ATM cards were stolen as part of the massive data breach at the third-largest U.S. retailer, but it was confident that the information was "safe and secure."

[Diminish]

The stolen PIN data was "strongly encrypted" when it was removed from Target's systems, and the "key" necessary to decrypt data is not within its system and could not have been taken during the breach, spokeswoman Molly Snyder said in a statement. "We remain confident that PIN numbers are safe and secure."

[Diminish]

Snyder declined to say how the criminals accessed the personal identification numbers.

[Deny]

While Target downplayed the significance of the PIN theft [Diminish], some security experts warned that it exposed customers to a higher level of risk than previously known.

[Worry]

“It means there is potential for gaining access to debit card accounts,” said Shane Shook, an executive with the cyber security firm Cylance Inc., who has investigated some of the biggest cyber breaches.

While it is virtually impossible to decrypt a PIN without the digital key to unlock it, Shook said many debit card holders choose easy-to-guess numbers like 1234. He said that in some investigations he has found that more than 20 percent of PINs could easily be guessed.

Criminals can identify PINs by using online systems some banks offer that allow customers to access their accounts using their debit card numbers and PINs, he said.

Madeline Aufseeser, a credit card analyst with Aite Group, said she does not believe the hackers could unscramble the PINs [Neutral], but still advises all Target customers whose accounts have been compromised to replace their cards immediately.

“Smart consumers are calling their banks and getting them reissued,” she said. “Better safe than sorry.”

Target has so far said little about how the cyber crooks accessed its network or stole the data in the attack, which breached 40 million payment card numbers at unprecedented speed.

[Disappointment]

The attack began Nov. 27, the day before the Thanksgiving holiday, and continued until Dec.ember 15, making it the second-largest data breach in U.S. retail history.

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.

Related story: