In-depth security news and investigation

18 Dec 13 http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/

Sources: Target Investigating Data Breach

Nationwide retail giant **Target** is investigating a data breach potentially involving millions of customer credit and debit card records, multiple reliable sources tell KrebsOnSecurity. The sources said the breach appears to have begun on or around Black Friday 2013 — by far the busiest shopping day the year.

Update, Dec. 19: 8:20 a.m. ET: Target released a statement this morning confirming a breach, saying that 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013.

Original story;

According to sources at two different top 10 credit card issuers, the breach extends to nearly all Target locations nationwide, and involves the theft of data stored on the magnetic stripe of cards used at the stores.

Minneapolis, Minn. based **Target Brands Inc.** has not responded to multiple requests for comment. Representatives from **MasterCard** and **Visa** also could not be immediately reached for comment.

Both sources said the breach was initially thought to have extended from just after Thanksgiving 2013 to Dec. 6. But over the past few days, investigators have unearthed evidence that the breach extended at least an additional week — possibly as far as Dec. 15. According to sources, the breach affected an unknown number of Target customers who shopped at the company's bricks-and-mortar stores during that timeframe.

"The breach window is definitely expanding," said one anti-fraud analyst at a top ten U.S. bank card issuer who asked to remain anonymous. "We can't say for sure that all stores were impacted, but we do see customers all over the U.S. that were victimized."

There are no indications at this time that the breach affected customers who shopped at Target's online stores. The type of data stolen — also known as "track data" — allows crooks to create counterfeit cards by encoding the information onto any card with a magnetic stripe. If the thieves also were able to intercept PIN data for debit transactions, they would theoretically be able to reproduce stolen debit cards and use them to withdraw cash from ATMs.

It's not clear how many cards thieves may have stolen in the breach. But the sources I spoke with from two major card issuers said they have so far been notified by one of the credit card associations regarding more than one million of cards total from both issuers that were thought to have been compromised in the breach. A third source at a data breach investigation firm said it appears that "when all is said and done, this one will put its mark up there with some of the largest retail breaches to date."

Some of the largest retailer breaches to date may help explain what happened in this case. In 2007, retailer TJX announced that its systems had been breached by hackers. The company later learned that thieves had used the store's wireless networks to access systems at its Massachusetts headquarters that were used to store data related to payment card, check and return transactions at stores across the country, and that crooks had made off with data from more than 45 million customer credit and debit cards.

In 2009, credit card processor Heartland Payment Systems disclosed that thieves had broken into is internal card processing network, and installed malicious software that allowed them to steal track data on more than 130 million cards.