WHAT HAPPENED AT TARGET?

**What Happened?**

Experts can only theorize about what may have happened to Target. And while fraud expert and Gartner analyst [**Avivah Litan**](http://www.bankinfosecurity.com/interviews/insights-on-fighting-call-center-fraud-i-2074) speculates about whether an insider is to blame for the breach, many other experts say Target's compromise likely resulted from an external attack.

As fraud expert and Aite analyst [**Shirley Inscoe**](http://www.bankinfosecurity.com/interviews/clueless-consumers-need-education-i-2040) points out, Target's reference to "unauthorized access" suggests an outside hack.

"This incident appears to be tied to their [point-of-sale] system since [card not present] transactions were not impacted," she adds.

An executive with one of the leading U.S. card issuers affected by the Target attack, who asked not to be named, says he believes about 40,000 of the retailer's 60,000 point-of-sale terminals were infected with an executable file, likely [**malware**](http://www.bankinfosecurity.com/anti-malware-c-309) that was automatically downloaded from a hacked server. Once infected, the devices were instructed to store and forward mag-stripe data collected during transactions at the POS, the executive says.

"Clearly, it was an external intrusion," the executive says. "It would follow that it was done through the infrastructure that Target uses to send updates down to their POS terminals."

An executive with another leading issuer also says the breach most likely was initiated at the network level, via an external attack, given the breadth of the attack.

[**Al Pascual**](http://www.bankinfosecurity.com/interviews/report-28-breaches-lead-to-fraud-i-1834), a financial fraud analyst with consultancy Javelin Strategy & Research, says the data leak was likely caused by a POS system attack, given that expiration dates and CVVs were lost. "I seriously doubt Target transmitted that data across an open network in the clear to their processor or stored the data," he adds.

[**John Buzzard**](http://www.bankinfosecurity.com/interviews/we-expect-more-atm-cash-outs-i-1920) of FICO's Card Alert Service says most indicators suggest Target was struck by an external attack that most likely infected its network with malware.

"A compromise involving all 1,800 U.S. stores would point to more of a virtual intrusion," he says. "I don't think there were criminal minions on the ground physically visiting all 1,800 stores. I think many issuers are also wondering if they will eventually have PIN [personal identification numbers used with debit transactions] exposure around this compromise."

No significant reports of PIN fraud with a suspected connection to Target have yet been reported, Buzzard says. "But I'm sure it's on the minds of many," he adds. "FICO Card Alert Service is watching very carefully for anything that indicates that PINs are in play and being used for unauthorized ATM withdrawals, even though we are not seeing any evidence of this today."

But Gartner's Litan questions whether the compromise was linked to an outside malware intrusion.

In a [**blog**](http://blogs.gartner.com/avivah-litan/2013/12/19/what-can-we-learn-from-the-target-breach/) posted Dec. 19, just after Target confirmed the attack, Litan speculates that the compromise is most likely be connected to an insider.

"If we've learned anything from the [**Snowden/NSA**](http://www.bankinfosecurity.com/blogs/how-did-snowden-breach-nsa-systems-p-1578) and [**Wikileaks/Bradley Manning**](http://www.bankinfosecurity.com/cybersecurity-legislation-whats-next-a-6063) affairs, it's that insiders can cause the most damage because some basic controls are not in place," she writes. "I wouldn't be surprised if that's the case with the Target breach - i.e. that Target did a great job protecting their systems from external intruders, but dropped the ball when it came to securing insider access."

Litan also says she thinks the card data was most likely stolen from Target's switching system for authorization and settlement, and was not intercepted because of malware that was remotely installed.

**Outdated Mag-Stripes to Blame**

Regardless of how the card data was compromised, the outdated magnetic-stripes on payment cards, which are vulnerable to skimming, contributed to the breach, security experts say.

"Bottom line: It's time for the U.S. card industry to move to chip/smart cards and stop expecting retailers to patch an insecure payment card system," Litan notes in her blog.

And [**Randy Vanderhoof**](http://www.bankinfosecurity.com/interviews/emv-outlook-for-2014-i-2136), executive director of the Smart Card Alliance, which supports a move in the U.S. toward chip payments that conform to the [**Europay, MasterCard, Visa standard**](http://www.bankinfosecurity.com/interviews/how-emv-will-change-banking-fraud-i-2122), says CVV data would not have been accessible from a chip-based transaction.

"EMV chip cards are more secure and replace static CVV values with dynamic CVVs, which stops criminal from counterfeiting cards with stolen transaction data," Vanderhoof says. "This breach shows that despite best efforts by major retailers to protect cardholder data generated from magnetic-stripe card transactions, criminals will find a way to get this data. The U.S. market needs to adopt secure EMV chip cards as most of the world has already done, including Canada."

**Advice for Banks**

For now, banking institutions should focus on informing their customers about monitoring accounts for fraudulent activity and taking advantage of fraud alerts offered by institutions, Pascual says.

"Twenty-eight percent of the consumers affected by this breach will likely have their cards misused to commit fraud," he says. "This is another example of why financial institution executives want retailers held to a higher standard. How many more of these need to happen before we get national legislation off of the ground?"

Already, some banking institutions have taken the initiative to alert their customers. TD Bank, for example, has posted "Security Alert: Target Store data issue" atop its online banking login page. "TD wants to advise customers that Target announced a data compromise at its US stores from Nov. 27 - Dec. 15," the alert reads, pointing customers to Target's corporate site for more details.

Buzzard says the Target breach offers a fertile ground for social-engineering schemes, such as phishing attacks, smishing/texting attacks and phone calls that fool consumers into divulging personal information.

"Make sure that you are clear on how your organization will reach out to customers so that they can identify legitimate communication," he says. "This is an excellent time for everyone to leverage their secure online banking websites to communicate with customers. If consumers want to have their cards replaced, it's critical that you manage their expectations closely. This isn't the time of year to close a card before a replacement arrives in the mail."

And Mary Ann Miller, managing director of fraud consulting and industry relations for security solutions firm NICE Actimize, says banks should remind consumers that they are not responsible for fraudulent charges, but they are responsible for monitoring their accounts.

"Banks should also recommend that their customers change their PINs [personal identification numbers] associated with their cards, continue to closely monitor their bank statements for unauthorized charges and report fraudulent transactions immediately if they are spotted," she says.

**Who is affected?**

Target says 40 million credit and debit cards may have been compromised. If you shopped at a U.S. Target store between November 27 and December 15, you should assume you’re at risk and keep a close watch on your account statements. It’s not clear whether every Target store was affected, but at least one card issuer says it’s seeing signs of fraud all over the United States, [according to Krebs on Security](http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/comment-page-3/#comment-215937). You’re not in any danger if you shopped at Target’s website, or one of the company’s Canada stores.

**What information was taken?**

Target says the attackers gained access to customer names, credit card or debit card numbers, card expiration dates and CVV security codes. Krebs on Security and the [*Wall Street Journal*](http://online.wsj.com/news/articles/SB10001424052702304773104579266743230242538) report that the thieves accessed data from the magnetic stripes stored on the back of credit and debit cards.

**What’s the risk for Target shoppers?**

The attackers could use magnetic stripe data to create counterfeit payment cards. The Wall Street Journal notes that crime rings often use these counterfeits to purchase gift cards at major retailers, and then convert them back to cash. The attackers could also withdraw cash from ATMs if they managed to steal PIN data from debit transactions, Krebs on Security notes.

**What the heck? How did this happen?**

Security breaches often involve hacking into a company’s servers and making off with the data, but the Target breach appears to be different. According to the Wall Street Journal, this theft “may have involved tampering with the machines customers use to swipe their cards when making purchases.” How the thieves were able to compromise payment terminals on such a large scale is unclear.

**What should Target shoppers do now?**

Target recommends keeping an eye on your credit or debit card statements and calling your bank or card provider if you see any fraudulent activity. As a general rule, you should get a copy of your credit report periodically by visiting [AnnualCreditReport.com](http://www.annualcreditreport.com/) or calling (877) 322-8228. You can also set up a fraud alert through the three nationwide credit reporting agencies, [Equifax](http://www.equifax.com/answers/set-fraud-alerts/en_cp), [Experian](https://www.experian.com/fraud/center.html) and [Transunion](http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page).

The problem, as one Krebs on Security commenter [points out](http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/comment-page-3/#comment-215937), is that automatic fraud detection could fail if the thieves are able to localize the stolen card details and make purchases near where cardholders live. The only guaranteed way to avoid fraud is to cancel your card and get a new card number, but that might not be necessary if you keep a close watch on your statements.

**What is Target doing about the breach?**

The retailer says it has ”moved swiftly to address this issue so guests can shop with confidence,” and has also hired a third party forensics firm to investigate. The [Secret Service](http://topics.time.com/secret-service/) is also investigating, as it often does for large-scale credit card data hacking.

**How common is this sort of thing?**

Too common, unfortunately. A 2007 security breach at T.J. Maxx resulted in the theft of card numbers and personal data for roughly [90 million customers](http://www.nbcnews.com/id/21454847/ns/technology_and_science-security/t/tjx-breach-could-top-million-accounts/#.UrMYQvRDuSo). Worth noting in that case is that the original estimate was just 45.7 million affected customers — still enough to be the largest payment card security breach ever at the time. Federal prosecutors are also still investigating a group of security breaches that resulted in more than 160 million stolen credit and debit card numbers, from companies including J.C. Penney, 7-Eleven and JetBlue. A breach of Heartland Payment Systems in 2009 resulted in stolen data on more than 130 million cards.

Read more: [The Target Credit Card Breach: What You Should Know | TIME.com](http://techland.time.com/2013/12/19/the-target-credit-card-breach-what-you-should-know/#ixzz2qgJQWIj3) <http://techland.time.com/2013/12/19/the-target-credit-card-breach-what-you-should-know/#ixzz2qgJQWIj3>