

13-CNN Business-Target

Target credit card hack: What you need to know

by Gregory Wallace @gregorywallace December 23, 2013: 11:43 AM ET

Who hacked Target?

The major hack of discount retailer Target that stole credit and debit card data from 40 million accounts was still reverberating several days later.

Target (TGT) acknowledged the hack on Thursday — three weeks after customer data was first scooped up on Black Friday.

On Sunday, Target spokeswoman Molly Snyder said the company had notified millions of affected customers for whom it had email addresses.

[Rebuild]

Major banks and card issuers said they were monitoring customer accounts. JPMorgan Chase (JPM) said it would limit the amount customers could withdraw from ATMs and spend in stores.

Related: Which is safer, credit or debit?

Two U.S. senators jumped in with demands for investigations.

Chuck Schumer called on the Consumer Financial Protection Bureau to report on whether retailers should be required to encrypt customer card data. Richard Blumenthal called for a Federal Trade Commission probe, saying “it appears that Target may have failed to employ reasonable and appropriate security measures to protect personal information.”

[Disappointment]

Meanwhile, plaintiffs in California sought to bring a class action and said Target “failed to implement and maintain reasonable security procedures

and practices.” [Disappointment] Local media reported that another lawsuit was filed in a Rhode Island federal court.

What was stolen? The hack affected customers who shopped at U.S. Target stores between November 27 and December 15, Target said.

Customer names, credit or debit card numbers, expiration dates and CVVs were involved in the information theft, Target said. The CVV — the card verification value, also known as the security code — is a three or four-digit number typically requested by retailers when making purchases online or over the phone.

Hackers could use this data to make card replicas. Robert Ahdoot, a lawyer for the California plaintiffs, said he spoke to customers who claimed unauthorized ATM withdrawals had been made from their accounts.

PIN numbers, other customer information like Social Security numbers, and employee records were not compromised, Target said. [Diminish]

What is Target doing? Target said it would offer affected customers a free credit monitoring service and set up a telephone hotline. [Rebuild] It also offered a store-wide 10% discount on Saturday and Sunday. [Rebuild] (Retail consulting firm Consumer Growth Partners estimated that customer transactions at Target stores declined on Saturday compared to the same weekend last year.)

The company said it “began investigating the incident as soon as we learned of it” through a “leading third-party forensics firm. [Rebuild]” The company said it also notified banks and law enforcement. [Rebuild]

The Secret Service, which safeguards the nation’s financial systems, said it was investigating, and on Friday, New York Attorney General Eric Schneiderman pledged to investigate.

CEO Gregg Steinhafel said “the cause of this issue has been addressed and you can shop with confidence at Target.” [Reinforce] He did not say how he knew customer data was no longer being stolen, nor how the hackers managed to swipe the credit card data. [Deny]

How do you know if you were hacked? The easiest way to spot unauthorized purchases is to regularly check your paper or online statement. Sometimes hackers ping an account for only few cents to verify they have an active account.

Behind your stolen credit card

Hacked or not, what should you do? If you shopped at Target between November 27 and December 15, you should call your credit card company , bank and Target. Request a replacement card — if one isn't already on the way — and change your PIN.

Customers typically aren't liable for unauthorized purchases on their accounts that they report promptly. Major banks and credit card companies — including American Express (AXP), Discover (DFS), Bank of America (BAC), Wells Fargo (WFC) and PNC (PNC) — said they were monitoring customer accounts.

J.P. Morgan Chase said it was temporarily limiting ATM withdrawals to \$100 a day and purchases to \$300 a day for customers whose accounts were at risk.

How did this happen? Many questions remain unanswered. But security experts believe hackers had access to the point-of-sale data, which means they either accessed the terminals where customers swiped credit cards or collected data as it moved from Target to credit card processors.

— CNNMoney's Emily Jane Fox, Jose Pagliery, James O'Toole and Julianne Pepitone and CNN's Evan Perez contributed to this report.

CNNMoney (New York) First published December 22, 2013: 3:09 PM ET