***Target Struck in the Cat-and-Mouse Game of Credit Theft***

**By**[**NICOLE PERLROTH**](http://www.nytimes.com/by/nicole-perlroth)DEC. 19, 2013

[Continue reading the main story](http://www.nytimes.com/2013/12/20/technology/target-stolen-shopper-data.html#story-continues-1)Share This Page



A Target store in Miami on Thursday. Cybercriminals appear to have targeted the point-of-sale systems in Target’s retail stores, which collect information from customers’ credit and debit cards. CreditJoe Raedle/Getty Images

SAN FRANCISCO — Target may have been an easy bull’s-eye for criminal hackers intent on stealing credit card information, but the theft of records for 40 million store customers was hardly the worst security breach among big retailers in recent years. And the incident revealed on Thursday is unlikely to be the last.

Security experts say the Target hack is a reminder of security problems facing many retailers that won’t easily go away: There are weaknesses in the way payment information travels between retailers and banks. There is plenty of money to be made on the black market selling stolen credit card numbers, which can go for as little as a quarter or as much as $45 each. And American companies have been reluctant to adopt smart-chip cards, a type of credit card widely used in Europe that provides better security.

Target said that from Nov. 27 to Dec. 15 hackers stole customer names, credit or debit card numbers, expiration dates and three-digit security codes for 40 million customers who had shopped in its stores. It is currently working with a forensic team from Verizon to investigate the breach, according to one person involved in the inquiry. But there was no word as to who was behind the attack, how they got in, or what the total cost to Target may be. Thursday, visitors to the retailer’s website found a site festooned in red and green save for [a stark black-and-white security notice](http://www.target.com/) at the top. Complicating matters, Target was hit during the holiday shopping season, when fraud detection systems have a hard enough time telling legitimate transactions from fake ones.

“This is the perfect storm” for vulnerability to hackers, said Paul Kocher, president of Cryptography Research, a company that develops technologies to prevent fraud.

It may be of little comfort to its customers, but the Target hack was dwarfed by a similar break-in six years ago at T. J. Maxx, which resulted in stolen data for 90 million customers, and a breach of the card processor Heartland Payment Systems in 2009 — the biggest on record — which resulted in 130 million stolen card numbers.

Security experts said that even if Target had installed the most cutting-edge security — and it’s not clear how Target was protecting this data — it would not be shocking if hackers found a way in.

“It’s a game of cat and mouse,” said Steven M. Elefant, a managing director of Soaring Ventures, who was chief security officer at Heartland Payment Systems when it was breached in 2009. “We’re dealing with sophisticated bad guys that have many ways to attack.”

Mr. Elefant said the Heartland breach should have been a wake-up call to large financial institutions and retailers that they needed to increase defenses and encrypt data as it moved from the cash register to card issuers and banks. But hackers, at least, do not appear to be dissuaded by whatever changes retailers have made since then.

Target has not said how its systems were compromised and a spokeswoman declined to say whether the company’s point-of-sale systems had been encrypted. Mr. Elefant said, however, that most systems still transmit credit and debit card data “in the clear,” security speak for plain text without encryption that can easily be intercepted.

Photo



Target took to Twitter, as well as other social media and the company’s website, to alert customers about the data theft.

When shoppers pay for store purchases with credit cards, their payment data moves from the store’s terminal through the retailer’s network to the acquiring bank and credit card issuer. “At every hop it could be vulnerable,” said Mr. Kocher. “There have been attacks at every stop along the way.”

Even when the data is encrypted, experts say there are plenty of other weak spots criminals can target. “Cash registers used to be just cash registers,” said Dan Kaminsky, the chief scientist at White Ops, a security consulting company. Today, they are computers of sorts, as vulnerable to hackers as a PC.

And those hackers do have an incentive. Credit and debit card numbers often sell in bulk on black market websites. Platinum cards can fetch as much as $35 and corporate cards $45. That stolen data — someone’s financial identity — can be burned onto magnetic strips on counterfeit cards that can be used for fraudulent purchases, or to buy gift cards that can be exchanged for cash.

Experts also question why — with breaches recurring regularly and credit card fraud rampant — American credit card issuers have not embraced smart-chip technology. The United States accounts for more than 47 percent of global credit card fraud, while generating only 24 percent of card spending, according to the Nilson Report, a card industry newsletter. More than 80 countries around the world use chip technology, but less than 1 percent of credit cards in the United States have chips.

Unlike magnetic-stripe credit cards, which serve the same data every time they are swiped, chip cards offer a different encrypted mathematical value, making it harder for criminals to use stolen data for future purchases.

“The U.S. is the only world region where counterfeit fraud continues to rise,” said David Robertson, the Nilson Report publisher. The absence of this chip technology at the physical point of sale is a large contributing factor, he added.

Europe started migrating to chip cards in 2002, when Europay, MasterCard and Visa partnered on a standard for chip technology. In 2005, the card companies also shifted liability for fraud to merchants in cases where they accepted a fraudulent payment from a magnetic-stripe card, instead of a chip card. As adoption of chip cards increased, fraud levels in Europe, which peaked in 2008, began to decline, according to Euromonitor International, a research company.

“The U.S. is still the only market using these 1960s magnetic-stripe cards,” said Mr. Kocher.

Last year, major credit card companies, including Visa and MasterCard, set October 2015 as the date that merchants will be subjected to new chip card standards, which shift the burden for fraudulent magnetic-stripe transactions from issuers to merchants.

It is unclear whether Target’s breach will accelerate the process. Seth Eisen, a spokesman for MasterCard, said the decision to move to the more secure cards will continue to be made by each card company and merchants.

In the meantime, breaches continue.

“The most important thing to realize is that 500 of the Fortune 500 are under constant attack,” said Mr. Kaminsky. “Nobody should be saying ‘I can’t believe Target got attacked’ because the reality is that everybody is getting attacked.”

**Part 2:**

***Target Missed Signs of a Data Breach***

**By**[**ELIZABETH A. HARRIS**](http://www.nytimes.com/by/elizabeth-a-harris)**and**[**NICOLE PERLROTH**](http://www.nytimes.com/by/nicole-perlroth)MARCH 13, 2014

[Target](http://topics.nytimes.com/top/news/business/companies/target_corporation/index.html?inline=nyt-org) acknowledged on Thursday that its computer security system had alerted it to suspicious activity after hackers infiltrated its network last year, but the company ultimately decided to ignore it, allowing what would become one of the largest data breaches ever recorded to proceed without a hitch.

“With the benefit of hindsight, we are investigating whether, if different judgments had been made, the outcome may have been different,” Molly Snyder, a spokeswoman for Target, said in a statement.

Before the attack, Target installed security software designed by FireEye, a security firm based in Milpitas, Calif., according to two researchers who spoke on the condition of anonymity, citing client confidentiality.

FireEye’s software, as it turns out, worked as designed. It isolates incoming web traffic and looks for suspicious activity. In Target’s case, the software sounded multiple alarms as criminals uploaded tools to siphon out customers’ credit and personal data.

“Like any large company, each week at Target there are a vast number of technical events that take place and are logged,” Ms. Snyder said. “Through our investigation, we learned that after these criminals entered our network, a small amount of their activity was logged and surfaced to our team. That activity was evaluated and acted upon.

“Based on their interpretation and evaluation of that activity, the team determined that it did not warrant immediate follow-up,” she said.

On Dec. 19, in the final days of the holiday shopping season, Target confirmed publicly that credit and debit card information for 40 million of its customers had been compromised. A few weeks later, the company said an additional trove of personal information, like email and mailing addresses, from some 70 million people had been exposed as well.

The company has said that when the news became public, its traffic and sales took an immediate and substantive hit, from which it has yet to fully recover. The company spent $61 million related to the breach in the fourth quarter, and executives have said they expect those charges to continue.

The security alerts were [first reported](http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data) by Bloomberg Businessweek.

Since the data theft at Target became public, several other retailers have acknowledged breaches of their own, including Neiman Marcus and the arts and crafts store Michaels. Those two breaches are believed to have come from the same Eastern European group that attacked Target, and may have attacked as many as six other retailers.

Last week, Beth M. Jacob, Target’s most senior technology executive,[resigned from the company](http://www.nytimes.com/2014/03/06/business/a-top-target-executive-resigns.html) in what appeared to be a response to the breach and the company’s continuing investigation. She was the first high-level executive to leave after the attacks.