Weak US card security made Target a juicy target

December 22 2013, by Jonathan Fahey

In this Jan. 18, 2008 file photo, a customer signs his credit card receipt at a Target store in Tallahassee, Fla. The U.S. is the juiciest target for hackers hunting credit card information. And experts say incidents like the recent data theft at Target's stores will get worse before they get better. That's in part because U.S. credit and debit cards rely on an easy-to-copy magnetic strip on the back of the card, which stores account information using the same technology as cassette tapes. The breach that exposed the credit card and debit card information of as many as 40 million Target customers who swiped their cards between Nov. 27 and Dec. 15 is still under investigation. (AP Photo/Phil Coale, File)

The U.S. is the juiciest target for hackers hunting credit card information. And experts say incidents like the recent data theft at Target's stores will get worse before they get better.

That's in part because U.S. credit and debit cards rely on an easy-to-copy magnetic strip on the back of the card, which stores account information using the same technology as cassette tapes.

"We are using 20th century cards against 21st century hackers," says Mallory Duncan, general counsel at the National Retail Federation. "The thieves have moved on but the cards have not."

In most countries outside the U.S., people carry cards that use digital chips to hold account information. The chip generates a unique code every time it's used. That makes the cards more difficult for criminals to replicate. So difficult that they generally don't bother.

"The U.S. is the top victim location for card counterfeit attacks like this," says Jason Oxman, chief executive of the Electronic Transactions Association.

The breach that exposed the credit card and debit card information of as many as 40 million Target customers who swiped their cards between Nov. 27 and Dec. 15 is still under investigation. It's unclear how the breach occurred and what data, exactly, criminals have. Although security experts say no security system is fail-safe, there are several measures stores, banks and credit card companies can take to protect against these attacks.

Companies haven't enhanced security so far because it can be expensive. And while global credit and debit card fraud hit a record $11.27 billion

last year, those costs accounted for just 5.2 cents of every $100 in transactions, according to the Nilson Report, which tracks global payments.

Another problem: retailers, banks and credit card companies each want someone else to foot most of the bill. Card companies want stores to pay to better protect their internal systems. Stores want cards companies to issue more sophisticated cards. Banks want to preserve the profits they get from older processing systems.

Card payment systems work much the way they have for decades. The magnetic strip on the back of a credit or debit card contains the cardholder's name, account number, the card's expiration date and one of two security codes. When the card is swiped at a store, an electronic conversation is begun between two banks. The store's bank, which pays the store right away for the item the customer bought, needs to make sure the customer's bank approves the transaction and will pay the store's bank. On average, the conversation takes 1.4 seconds.

During that time the customer's information flows through the network and is recorded, sometimes only briefly, on computers within the system controlled by payment processing companies. Retailers can store card numbers and expiration dates, but they are prohibited from storing more sensitive data such as the security codes printed on the backs of cards or other personal identification numbers.

Hackers have been known to snag account information as it passes through the network or pilfer it from databases where it's stored. Target says there is no indication that the three or four-digit security codes on the back of customer credit cards were stolen. That would make it hard to use stolen account information to buy from most internet retail sites. But because the magnetic strips on cards in the U.S. are so easy to generate, thieves can simply reproduce them and issue fraudulent cards

that look and feel like the real thing.

"That's where the real value to the fraudsters is," says Chris Bucolo, senior manager of security consulting at ControlScan, which helps merchants comply with card processing security standards.

Once thieves capture the card information, they check the type of account, balances and credit limits, and sell replicas on the Internet. A simple card with a low balance and limited customer information can go for $3. A no-limit "black" card with the security number printed on the back of the card can go for $1,000, according to Al Pascual, a senior analyst at Javelin Strategy and Research, a security risk and fraud consulting firm.

To be sure, thieves can nab and sell card data from networks processing cards with digital chips, too, but they wouldn't be able to create fraudulent cards.

Credit card companies in the U.S. have a plan to replace magnetic strips with digital chips by the fall of 2015. But retailers worry the card companies won't go far enough. They want cards to have a chip, but they also want each transaction to require a personal identification number, or PIN, instead of a signature.

"Everyone knows that the signature is a useless authentication device," Duncan says.

Duncan, who represents retailers, says banks want to preserve the higher profits they can get when a signature is needed because there are fewer signature processing networks, and less price competition. The higher profits outweigh the cost of fraud, Duncan says.

"Compared to the tens of millions of transactions that are taking place

every day, even the fraud that they have to pay for is small compared to the profit they are making from using less secure cards."

Even so, there are a few things retailers can do, too, to better protect customer data. The most vulnerable point in the transaction network, security experts say, is usually the merchant.

"Financial institutions are more used to having high levels of protection," says Pascual. "Retailers are still getting up to speed."

The simple, square, card swiping machines that consumers are used to seeing at most checkout counters are hard to infiltrate because they are completely separate from the Internet. But as retailers switch to faster, Internet-based payment systems they may expose customer data to hackers.

Retailers need to build robust firewalls around those systems to guard against attack, security experts say. They could also take further steps to protect customer data by using encryption, technology which scrambles the data so it looks like gibberish to anyone who accesses it unlawfully. These technologies can be expensive to install and maintain, however.

Thankfully, individual customers are not on the hook for fraudulent charges that result from security breaches. But these kinds of attacks do raise costs —and, likely, fees for all customers.

"Part of the cost in the system is for fraud protection," Oxman says. "It costs money, and someone's going to pay for it eventually."