How to protect yourself from credit card fraud 1:52

Ed Fritz from the Boise Police Department gives tips on how to keep your bank accounts tied to debit and credit cards from getting drained. **John Sowell** - jsowell@idahostatesman.com

BUSINESS

JUNE 05, 2017 5:48 PM

You've got a chip card. But if your store makes you swipe it, you're still at risk.

BY JOHN SOWELL
jsowell@idahostatesman.com

A spending spree by two men visiting Boise from Michigan in early January played out in familiar fashion.

Devin A. Searcy, 23, and Juwuan D. Gordon, 27, went into at least seven stores, including Lowe's, TJ Maxx and Dick's Sporting Goods. They used stolen credit card numbers to buy gift cards and prepaid debit cards.

Boise police later detained the pair, who were found with a dozen counterfeit credit and debit cards and more than 100 purchased cards. Authorities later tied the two men to similar scams in Utah, Colorado and Oklahoma the month before.

Over the past two years, police have arrested dozens of people — nearly all of them flying in from out of state — for similar crimes. The fraud is pretty simple: Stolen card numbers are embedded on blank plastic cards, and the thieves swipe the cards through retailers' payment terminals.

At one point in April 2015, the Boise Police Department arrested four different groups in a one-week period, from Arizona, California, Florida and Mexico. While the department doesn't separately track this type of fraud, authorities believe things are changing.

"We're not seeing that same activity, but without a doubt it's still going on at some level," said Ed Fritz, crime prevention officer for the Boise Police Department.

New plastic cards, embedded with a microchip meant to be impossible to duplicate, were supposed to completely wipe out this kind of crime. The chip creates a unique transaction code every time the card is used. Stealing the transaction number wouldn't help a thief because any subsequent transaction using the same number is denied.

Chip-bearing cards were supposed to become standard in the United States in October 2015, under deadlines set by Visa and MasterCard. However, some banks lagged behind in issuing them. Many retailers balked at buying compatible payment terminals despite a threat from card issuers to make any merchants without them liable for losses from fraud.

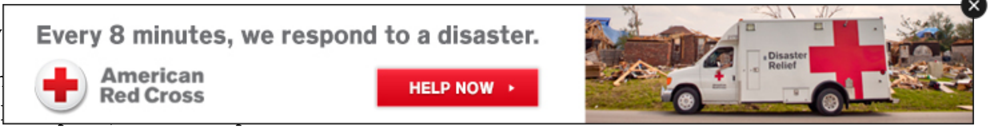
As a result, just less than half of U.S. retailers still rely on machines that require a payment card to be swiped. Thieves can still use those machines to exploit stolen card numbers.

Security varies worldwide

Worldwide, plastic card fraud losses totaled $21.8 billion in 2015. Nearly 40 percent of those losses took place in the United States despite the country only accounting for 23 percent of sales, according to the Nilson Report, a trade newsletter that covers the card industry.

More than just the U.S. chip card adoption rate drives that figure. For example, In Europe, users of chip cards must punch in a PIN in order to complete a transaction, regardless of the type of card. In America, PINs are not required for credit cards.

MasterCard is currently testing a new security feature in South Africa that embeds an encrypted copy of a card user's fingerprint into the card. When paying, the user puts the card into the chip reader and then also places their finger on the embedded sensor. If the print matches, the purchase goes through.



The company

The European
significantly.

percent of the region's total losses in 2008; by 2013 it had climbed to 66 percent, according to a report issued in March by the U.S. Payments Forum, an industry group that supports the adoption of the chip card.

Online and phone fraud accounted for 45 percent of total U.S. card fraud in 2014. As more chip readers come into play, that percentage is expected to rise to the European levels, analysts say.

Committing fraud online is easier and less risky than trying to pass a card in public. There are no cameras to snap a criminal's photo and no security officers to detain them.

"That's going to be on the consumer, the victim, to notice the charge on their card. It's not as obvious that it's going on. Hopefully, they're notifying police and filing a report," Fritz said.

How to spot a skimmer at a gas pump or ATM

Eric Vitale, fraud investigation specialist with the San Luis Obispo Police Department, demonstrates how to spot a card skimmer on an ATM, gas pump or other card reader. He also offers advice for keeping your PIN and card information safe.

David Middlecamp - The Tribune

Idaho relies on retailers helping police

Last month, Target agreed to pay $18.5 million to settle claims brought by Idaho and 46 other states after a 2013 data breach that affected millions of U.S. customers' card information. Idaho will receive nearly $193,000 to cover its investigative expenses and other fees.

Many stolen card numbers, such as those taken from Target, end up on "dark web" internet sites that sell them to thieves like those caught in the Treasure Valley.

While the number of incidents here has dropped, attempts to exploit card-swipe readers still continue. Authorities in Southwest Idaho believe they have an effective system in place to counter them.

Retailers work closely with police, notifying them whenever they see suspicious spending on gift cards and prepaid debit cards. Store surveillance video helps identify suspects, and security officers are often able to provide license plate numbers of cars used by the thieves.

"We've had good cooperation from businesses in the past in calling law enforcement immediately. Boise police and Ada County are able to get on it and put a case together and apprehend the suspects before they leave the area," said Aaron Lukoff, an assistant U.S. attorney for Idaho.

Federal prosecutors are handling the case involving Searcy and Gordon, who pleaded guilty this spring to conspiracy to commit wire fraud. They are scheduled to be sentenced in July.

Ada County is currently prosecuting three men from Florida, Alabama and Georgia who were arrested by Garden City police in March.

"We haven't seen the rash that we saw last year. I don't know if that's because the weather was so crummy for this winter," Lukoff said. "It would be premature to say that the issue is no longer an issue here. I wouldn't be able to say that until the end of this year."

John Sowell: 208-377-6423, @IDS_Sowell

HOW DOES A CHIP CARD WORK?

The computer chip embedded in modern credit and debit cards holds information securely until accessed by a chip-reading terminal at a store or restaurant. A unique code is created each time the card is used to prevent the card from being counterfeited, as can happen with cards containing a magnetic strip.

The reason a chip transaction takes longer is because the chip performs several security operations to ensure the transaction is legitimate, according to EMVCo, a consortium set up by Europay, MasterCard and Visa to oversee the technology. While not foolproof, it is largely regarded as a significant step forward for security.

Chip cards are based on technology developed in France. French banks began field trials in 1984 and 10 years later, all of the country's bank cards carried a chip.

Chips embedded in credit/debit cards have changed the way consumers make their transactions — unless retailers haven't fully upgraded their terminals. **Darin Oswald** - doswald@idahostatesman.com

1 of 3

SUGGESTED FOR YOU

COMMENTS