TECH BRIEF

How to protect yourself from a credit card security breach

ENJOY SAFER TECHNOLOGY™

HOW TO PROTECT YOURSELF FROM A CREDIT CARD SECURITY BREACH

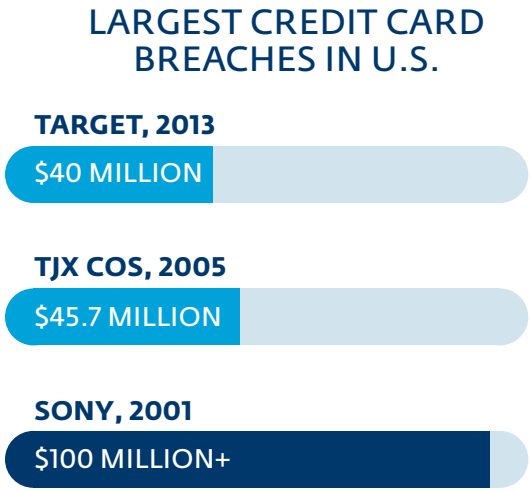
By Stephen Cobb, ESET Security Researcher

Tens of millions of credit and debit cards stolen from a national retail chain – how could that happen? That was the question on a lot of minds when noted security researcher Brian Krebs broke the news of the Target data breach on Dec. 18. Exactly how the criminals gained access to the cards is still not known, but it was known right away that some of these stolen cards were being sold on the black market for prices in the $25 to $45 range.

During this particular breach, it was not physical cards that were stolen, but rather the data stored in the magnetic stripe on the cards, such as a customer's name, card number and expiration date, plus the security code that is printed on the card. The criminals were accessing that data remotely and then selling it to people who specialize in converting card data back into cards. Buyers of this stolen card data were not slow to use them, charging things such as gift cards and high-end TV sets that can easily be converted into cash.

So what does an incident such as this mean for consumers who use cards, as well as for companies that accept cards for payment?

While the Target breach is the highest profile incident of its kind, there have been others, and there may be more. With all of the information known about how a credit card breach plays out, here are some tips on how consumers should play defense.



Check your account for suspicious activity

The first and most important thing you can do is to keep an eye on your credit card transactions. Many banks now allow you to set up email and SMS alerts for activity on your account and these can be a great warning mechanism. If there is a breach at a retailer you use, you probably want to create an alert for every transaction. For example, if you used a credit or debit card at Target during November or December make sure it is set to alert you to purchases. If your bank does not allow this, try to check the account activity regularly (perhaps via website or ATM).

What you should be looking for is card activity you don't recognize, and you should call the bank right away when you see anything suspicious. An example of this might be a large purchase in a state or country you have not visited recently. Bear in mind that criminals often "test" fake cards by making a small purchase at a gas station to see if they are declined. If that small purchase is approved it's off to

the mall. That pattern alone might be enough to trigger an anti-fraud alert at the bank (hint: don't buy gas just before you go shopping for expensive lingerie; it can get embarrassing when the card is declined).

However, don't just rely on your bank's anti-fraud measures, because many criminals know how they work. We see evidence of this in the wake of the Target breach because stolen card data that includes ZIP codes of the card holder appear to be going for a premium because knowing the ZIP code allows buyers to plan their fraudulent purchases close to the home turf of the legitimate card holder.

Keep in mind that although there are reports that some of this stolen data is already being used for fraud, the criminals may not use or sell all of the stolen data right away (in order not to flood the market and devalue the data, they may sell it over the course of several months). You will need to be vigilant with these accounts for a while.

Monitor your credit report

Using stolen card data to make fake credit cards is just one way to profit from stolen information. Criminals could also take the data they have stolen and combine it with other data to wreak more havoc, such as opening accounts in your name. It is a good idea to regularly monitor your credit report, to identify and then report any suspicious activity. You may also want to look into setting up a fraud alert or a credit freeze if you want additional protection against fraudsters trying to get credit in your name. Be aware that these steps will also mean you have to go through additional verification if you wish to get credit, for the duration of the alert or freeze. The Federal Trade Commission (FTC) has a lot of useful information on credit reports and identity theft.

Ask for a replacement debit/credit card

If you are worried that your card is included in a data breach, you may not want to wait for fraudulent activity to show up. This is especially true if the card in question is a debit card that pulls funds directly from your bank account. Just ask your card issuer for a replacement card. There is a downside to this if you have any auto-pay accounts that reference this account number because you will need to update that information. Asking for a replacement card means more outlay of time now to prevent a bigger outlay of time in the future, if your card data turns out to have been stolen.

Change PINs and passwords

If you fear your debit card has been compromised by a security breach then you may want to change your PIN. In the case of Target, the company confirmed that encrypted PINs were part of the data gathered in the breach. Encryption is an extra layer of security for criminals to have to get through, but the difficulty can largely depend on the kind of encryption program the retailer used. Of course, if you have an easy-to-guess PIN, such as 1234, you have made the criminal's job that much easier. Try changing to a stronger PIN, avoiding your birthday and other obvious choices. If your bank allows you to use a PIN longer than four digits, use it (longer equals stronger). Making this change is a small step that can greatly improve your security.