St. Thomas Federal Credit Union

10 Ways Criminals Get Debit Card Data

Criminals are more sophisticated than ever before. Attacks on ATMs and card terminals can range from the simplistic to highly organized efforts involving hundreds of fraudulent cards and criminal gangs spanning the globe.

So, how do criminals get members' debit card data? Here are 10 different ways:

1. Steal Cards

The simplest way for a criminal to get card data is to steal someone's card. To get the PIN, the thief might shoulder surf or guess a weak password, such as a birthdate.

2. Steal machines

A criminal might decide to steal either an ATM or POS terminal. Cash can be pulled from the ATMs, but both types of machines could store card numbers if misconfigured. A stolen machine is also valuable in order to learn about weaknesses or ways to physically attack it.

3. Offline account takeover

Breaking into mailboxes and stealing account statements or other personal information can let criminal conduct identity theft. Often they'll try to change the victim's mailing address with the credit union, order a new card, and activate it. If the CU has good processes in place that are adhered to, then this type of attack can be stopped.

4. Separate skimming device

If a deft criminal can get a hold of a card for a few seconds, then they can swipe it through a reader and get its data.

5. Overlaid skimming devices

In this case, the criminal places a card reader over the machine's intrinsic reader. They might also attach a video camera or a pin-pad overlay to capture the PIN.

6. Internal skimming devices

More capable criminals could place a skimming device inside a terminal, such as at a gas pump. The skimmer intercepts messages on the data lines, and is tough to detect without opening up machines.

7. Hijacked terminals

A terminal can be hijacked by replacing the operating system with a compromised one. An avenue of attack might be available for those ATMs with remote control capabilities that are left in the default (and insecure) settings. Stolen machines might also be modified and then used to replace an existing, non-compromised terminal.

8. Ghost ATMs and fake fronts

Why add a skimming device to a real terminal when you can just use your own fake one? Criminals have been known to place fake, modified terminals in public spaces where victims will use their cards but receive communication error messages. In reality the terminal has captured card data and PIN, and stored it for later retrieval.

9. Buying the data

With so many attacks, there is a glut of card information on the market. Lazy criminals can simply buy card data, starting at $1 or less. Quality costs extra, but in the underground marketplace there are products for everyone.

10. Data breaches

Capable hijackers are able to crack the security on merchants and other card data holders, and access large volumes of card data. With the heightened awareness of cybercrime, the industry has made strides in using more secure techniques for strong data. This has made it harder for criminals, but there are still many opportunities for attacks.

St. Thomas
Federal Credit Union

Ways to Protect Against Debit Card Fraud

Can you be a victim of credit or debit card fraud if you still have the physical card? You betcha! Card skimming incidents, such as those we experienced in the Virgin Islands recently, should serve as a reminder to protect your cards every time you swipe.

Criminals can find out what your PIN is by setting up a camera or watching as you key in your code. The following are a few tips on how to protect your credit and debit cards:

1. Check your Credit Union statements immediately. Make sure all payments are yours.
2. Periodically check your account balance and transactions, by utilizing online banking, by telephone, or printing interim statements at the ATM.
3. Contact St. Thomas Federal Credit Union immediately if your card is lost, stolen or subject to fraudulent use.
4. Keep a record of card numbers, PINs, expiration dates and 1-800 numbers for all financial institutions so you can contact the issuing institution easily in cases of theft.
5. Memorize you PIN number. Do not use your birth date, address, phone number, or social security number. Never store your PIN with your card, and do not make it available to others.
6. Keep your receipts. You'll need them to check your statement. If they have your account number on them, tear up or shred receipts before throwing them away.
7. Mark through any blank spaces on debit slips, including the tip line at restaurants, so the total amount cannot be changed.
8. Know your limits. Many issuers limit daily purchases and withdrawals for your protection.
9. Do not use an ATM if it looks suspicious, it could be a skimming device.
10. Be wary of those trying to help you, especially when an ATM "eats" your card, they may be trying to steal your card number and PIN.
11. Do not give your PIN number to anyone over the phone, often thieves steal the cards and then call the victim for their PIN, sometimes claiming to be law enforcement or the issuing bank.
12. Let issuers know your travel dates and destination. If your card gets swiped at an unusual location, the card issuer may decline the suspicious transaction.
13. As you key in your PIN, cover the keypad with your other hand to block anyone, or a camera, from viewing the numbers you type.
14. Do not use ATMs with unusual signage, such as a command to enter your PIN twice to complete a transaction.

Federal law doesn't protect debit cards to the same degree as credit cards when it comes to fraud. If you notify St. Thomas Federal Credit Union within two days of discovering the card was lost or stolen, your loss is limited to $50. After two days, this amount jumps to $500, and after 60 days of receiving the statement with the fraudulent charges, your loss may be unlimited.