Comptroller of the Currency
Administrator of National Banks
US Department of the Treasury

Answers for customers of
national banks at
HelpWithMyBank.gov

Consumer Advisory

Avoiding 'Card Skimming' at ATMs and Other Money Machines

Be wary when you use automated teller machines (ATMs) and other payment processing machines. Thieves may be using high-tech tools in scams to capture your account information to steal your money.

These scams, known as "card skimming," involve attaching devices to money machines that read the information on your debit and credit cards when you swipe them. When combined with a nearby concealed camera to record your personal identification number (PIN), the thieves can get everything they need to drain your account or to make unauthorized purchases. In addition to using the information directly, thieves may sell your information to others.

ATMs and automated payment machines in airports, convenience stores, hotel lobbies, and other well-traveled, public places may be most vulnerable to thieves who may think these machines are not regularly inspected by the machine owners. However, card skimming may take place at any ATM or card processing machine, including those on bank premises. As technology makes these devices smaller and more powerful, the risk of card skimming grows.

How High-Tech Thieves Operate

Thieves have many ways to steal your account information. They may attach a card skimmer that looks and acts like a genuine part of the ATM or other type of money machine. The device may be a simple, curved plastic sheath over the card slot. The skimmer reads the magnetic strip or computer chip on your card and transmits your account information to the thieves or saves the information until the skimmer is retrieved.

Thieves may also use a wireless camera concealed nearby in a box holding brochures or in a light fixture. The camera photographs or videotapes your fingers as they enter your PIN on a keypad or screen. Like a card skimmer, the camera can transmit images instantly or save them until the thieves retrieve the camera later. A camera and card skimmer can be used together.

Safeguarding Your Personal Bank Account Information

To help protect you, banks and retailers take measures to minimize the risk of fraudulent use of your debit or credit card, particularly when those purchases are made by telephone or online.

Before approving telephone purchases, retailers typically confirm your identity by asking for personal information. They may ask for your address, the last four digits of your social security number, or answers to security questions you created when you set up your account. Retailers also may ask for the three-digit security code printed on the front or back of your debit or credit card. To protect your online transaction from electronic fraud, many commercial Web sites require you to unscramble a word or a number displayed as a fuzzy or distorted image that is difficult for software to read.

Protecting Yourself With Common Sense Security Measures

Ultimately, you must protect yourself against thieves and the tools they use to access your accounts to steal from you. To protect yourself, follow these common-sense precautions.

- Walk away from an ATM if you notice someone watching you or if you sense something wrong with the machine; immediately report your suspicions to the company operating the machine or a nearby law enforcement officer.

- Before using an ATM, examine nearby objects that might conceal a camera; check the card slot for a plastic sheath before inserting your card.
- Never keep a written copy of your PIN in your wallet or purse as it could be stolen; instead memorize your PIN and keep a paper record hidden at home.
- When entering your PIN, stand close to the machine and hold your hand over the keypad or screen to make it more difficult for a person or camera to watch you.
- Beware of strangers offering to help you with an ATM that appears disabled and notify someone responsible for the security of the machine.
- Regularly review your account statements, either online or on paper, and check for unauthorized withdrawals and purchases. If you find one, immediately contact your bank or credit card provider, as this will limit your financial liability for fraudulent charges.

Federal laws limit your liability from debit and credit card fraud. Two federal laws, in particular, protect you.

The Truth in Lending Act generally limits your liability to $50 for any unauthorized use of your credit card. However, you are not responsible for unauthorized charges on your account—if you report a lost or stolen credit card before the card is used. Also, you are not responsible if the fraud results from someone using your credit card number alone rather than your credit card.

The Electronic Fund Transfer Act also limits your liability for unauthorized use of your debit or ATM cards—if you quickly report the lost or stolen card. You are not held responsible for unauthorized charges if you report the fraud before unauthorized transactions are made. If unauthorized transactions occur before you report your card missing or compromised, your liability depends on how quickly you report the loss.

Additional Information

The Federal Trade Commission provides more information on what to do if your card is lost or stolen in its fact sheet "Credit, ATM and Debit Cards: What to Do if They're Lost or Stolen," at www.ftc.gov/bcp/edu/pubs/consumer/credit/cre04.shtm.

The Office of the Comptroller of the Currency has answers about what to do about unauthorized charges and other banking issues at HelpWithMyBank.gov.

Card Skimming: How It Works