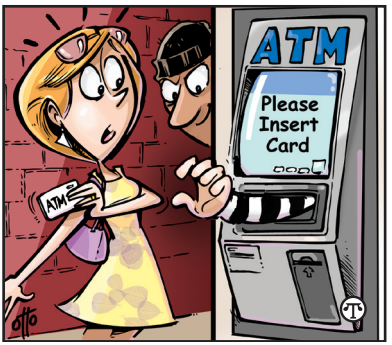
SAFETY SENSE

Don't Let High-Tech Thieves "Skim" Your Bank Account

(NAPSA)—The next time you use your credit or debit card at an automated teller or payment machine, be careful. High-tech thieves can use phony card scanners and tiny cameras to steal your personal data and your money.

"Card-skimming" thieves use hidden devices to "skim" off account numbers and personal identification numbers (PINs) from debit and credit cards. Armed with your information, the fraudsters can swiftly clean out your bank account or make unauthorized purchases. Skimming can occur nearly everywhere you use a card—ATMs, gas station pumps or any machine used to process card purchases.



Skimming can occur nearly everywhere you use a card—ATMs, gas pumps or any card-processing machine.

Experts at the Office of the Comptroller of the Currency suggest ways to avoid becoming a card-skimming victim:

- Do not use a machine if you notice something suspicious. Report the problem immediately.
- Watch out for signs asking you, for example, to swipe your card before inserting it into the ATM.
- Inspect objects near ATMs that do not seem to belong there.
- Keep your PIN secure at all times and enter it discreetly by holding your hand over the keypad or screen when entering it.
- Beware of strangers who offer help with an ATM that is not functioning properly.
- Review your account transactions regularly and check for irregular activities.
- Report any irregular activity, suspected losses and loss or theft of your card right away. Prompt reporting makes you less likely to be legally liable for any losses.

How Card Skimming Works

To steal information, thieves attach a card-skimming device to the ATM or payment-processing machine. It could be as simple as a curved plastic shell placed over the real card slot. When you insert or swipe a card, the skimmer reads the magnetic strip or computer chip and stores or transmits the information.

To steal PINs, thieves often use hidden cameras to record your fingers entering your password. A brochure holder, light fixture or other attachment can conceal a wireless camera, which may be used with a swiping device.

Vulnerable Card Readers

Card skimming may take place at any ATM or payment-processing machine, but machines in public areas, such as airports, convenience stores and hotel lobbies, are most vulnerable. Owners tend to inspect these machines less frequently and thieves have more time to execute their schemes.

The Federal Trade Commission provides information on what to do if your card is 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 www.HelpWithMyBank.gov.