Don't Get Scammed by Skimmers

By Louis E. Conrad II

- Unfortunately, your hard-earned cash can be lost through the unscrupulous actions of skimmers.
- This article describes what skimming is and what actions you can take to protect your cash and financial data.

When automated teller machines (ATMs) were introduced in the 1970's, they were heralded as a means of providing greater customer convenience —access to cash 24 hours a day, 7 days a week. And while attempts have been made during the intervening years to bypass the security of ATMs and unlawfully access the cash they house, a high tech scam called skimming has become more prevalent recently. In addition to ATMs, skimming is also occurring at gasoline stations from credit and debit cards.

Skimming your Cash

According to the Federal Bureau of Investigation, ATM skimming is a scheme favored by Eurasian crime groups, which may be costing U.S. banks hundreds of millions of dollars each year. In one case in the fall of 2010, two Bulgarian nationals were charged with using skimming devices to steal over $1.8 million from more than 1,400 customer accounts at two New York City area banks.

ATM skimming involves the installation of (1) an electronic device over the ATM's card slot, which reads the account information on the card's magnetic strip, and (2) a miniature camera that captures the user's personal identification number (PIN) when entered on the ATM's keypad. The electronic device will either save the information on a small, attached laptop or cellular phone, or send the account information wirelessly to thieves waiting nearby. Most often such devices, attached with double-sided tape to the ATM and designed to look like the existing terminal, are only in place for a few hours before they are removed by the criminals. Once thieves have the account information and PINs, they encode blank cards with the stolen data and withdraw cash from customer accounts.

Two types of ATM skimming devices exist: one that interferes with the ATM's operation and one that does not. If the former type of device is in place, then the bank customer will not be able to withdraw any cash, while the other type of device can be skimming your account information and allowing you to make withdrawals at the same time.

Skimming your Credit/Debit Cards

Credit and debit card users of pay-at-the-pump terminals at gasoline stations can meet a fate similar to ATM users. Pay-at-the-pump skimming devices can be installed either inside or outside of the gas pump. Internal installations intercept the credit or debit card information that is scanned by the external card reader. These types of installations are generally performed with the participation of a gas station employee. Small cameras are used to capture and wirelessly transmit PIN numbers that are entered for debit card purchases.

Safeguards to Take

Though financial institutions will typically credit your account for fraudulent withdrawals or charges, you can take steps to protect yourself: (1) Examine an ATM, gas pump, or credit card reader before using it and be suspicious of anything that looks out of the ordinary. Be especially careful of ATMs in tourist areas, which tend to be popular with thieves. (2) When entering your PIN, shield the keypad. (3) If your ATM card is not returned at the end of the transaction, immediately contact the financial institution that issued the card. (4) For gasoline purchases, go into the gas station to process your transaction and sign the credit card receipt. (5) Check your statements to ensure there are no unauthorized transactions. (6) Contact law enforcement if you believe any fraudulent activity has occurred.

Although convenient, ATM, credit, and debit cards require your diligence to protect the privacy of your account information and your financial security.