ATM SECURITY- PROTECT YOURSELF AGAINST SKIMMING

ATM Security Precautions

February, 2013

According to KrebsonSecurity.com, the U.S. Secret Service estimates that annual losses from ATM fraud totaled about $1 billion in 2008 or about $350,000 each day. Card skimming accounts for more than 80 percent of ATM fraud.

ATM (Automated Teller Machine) security generally falls into two categories, physical security and electronic security. Physical security includes protecting your ATM card from loss or theft, while electronic security focuses on emerging threats such as digital account takeover. While physical security might often seem the more obvious danger, electronic dangers such as "skimming" are generally more threatening because they are more difficult to detect and often more difficult to avoid. Fortunately, there are a few key things you can do to help protect yourself from these threats.

WHAT IS SKIMMING?

Skimming is a form of card fraud which can affect both credit and debit cards. ATM tampering is just one of the ways in which a criminal may perform "skimming". ATM skimming occurs when criminals put a device over the card slot of an ATM. In most cases, this device looks like a legitimate part of the ATM machine. This device then reads the magnetic card strip when inserted by the owner. These card readers are often used in conjunction with a miniature camera which records the user's PIN (Personal Identification Number) at the same time. Thieves can then put your card's information on a counterfeit card and use your pin number to steal the money from your account. Organized crime rings, often at the heart of ATM skimming, may also sell the information online.

Are all ATMs at risk?

Although all machines are potential targets, according to the FBI, ATMs in airports, convenience stores, hotel lobbies, and other well-traveled, public places may be most vulnerable to skimmers. In general, open ATMs located outdoors are at higher risk of exposure.

If you feel you have accessed a compromised ATM, change your PIN number as soon as possible.

What can I do to reduce my risk?

Trust your instincts. If something seems suspicious, it may indicate a problem. If you are prompted to enter your PIN twice for no apparent reason, or if you notice unusual messages on the screen, go to another ATM. Other tips include:

- **Visual Inspection.** Look over the ATM for possible skimming devices. Potential indicators can include evidence of an adhesive, such as sticky residue, used by criminals to affix the device to the ATM. Other giveaways include damaged or crooked pieces, scratches, loose or extra attachments on the card slot, or noticeable resistance when pressing the keypad.
- **Check for cameras.** All ATM machines have cameras, but they should not be positioned in a way that has a view of your fingers on the keypad. Fraudulent cameras are installed by the criminals to capture your PIN number. Covering the keypad with your other hand while you enter

your PIN may prevent the camera from capturing your PIN number.

- **Pull on the card slot.** Skimming devices are usually placed over the top of the existing card reader, and may be loose and actually come off in your hands. Since most criminals do not have a lot of time to install the skimmers, tape, glue, scratch marks and other "tells" may indicate a problem. Many times, a legitimate card reader will have an illuminated entry slot. Skimming devices will cover this slot, removing the lighted feature.
- **Wiggle the keypad.** Although most low-tech skimming ploys use cameras to record PIN numbers, some more advanced schemes use actual keypads to record your PIN entry. Like the card readers, these keypads will need to be installed quickly over the top of the existing ATM equipment, which may leave signs. If the keypad feels loose, or appears to be detaching from the corners, find another ATM.
- **Check your Statements**. Take your receipts with you and be sure to check your statements and account activity on-line to quickly spot discrepancies. Immediately notify Northern Trust if you notice unusual withdrawals.