Attached Credit, Debit Card Skimmers Pose Identity Theft Risks at Gas Pumps & ATMs

By Denise Richardson

Police around the country continue to warn the public to be on the lookout when they use their credit or debit cards to get cash or to pay for gas at the pump. In cities from here in S Florida to the state of Washington, police and bank officials have found skimmers, electronic devices that swipe your bank card info when you swipe your card, attached to ATMs and gas pumps.

Thieves using skimmers had managed to steal more than $1 billion (with a B) by 2009, and, according to authorities, the losses are mounting at the rate of millions of dollars a month.
Just how widespread is skimming fraud and identity theft?

In Boynton Beach, Florida, ATM technicians found skimmers attached to ATM machines throughout the town. In Vancouver, Washington, police arrested a young man who had attached a skimmer to a local ATM. In Savannah, Georgia, police found a skimmer attached to the ATM located inside a bank.

Banks and ATMs aren't the only place to be wary, though. In fact, police and security experts warn that fraud and identity theft will increase at gas pumps and other places where you swipe your card. Gas station pumps are especially vulnerable, because they weren't designed with security in mind.

Most pumps, for example, can be opened with the exact same key. This makes them a sitting target for thieves who can open the pump and insert the credit card skimmer without leaving any outward sign that the pump has been tampered with.

In just the past few months, thieves in Honolulu used skimmers attached to gas pumps at four local mini marts to steal over $150,000 from local residents. On Long Island, a gas station attendant was indicted for using a skimmer to steal data from customers. And in Utah, police found skimmers attached to gas pumps in 180 stations between Provo and Salt Lake City.

I would say that once again it proves that criminals are always at least one step ahead of us. It's important to be alert when using debit and credit cards when filing up your car or trying to get cash at an ATM. Experts on ATM-related crime

say that skimming has become more lucrative for criminals than drugs. Some believe that is because ATM skimming, much like identity theft, is viewed as a low risk -high reward crime.
How It Works

Thieves attach their own credit card scanner to an ATM or gas pump, usually fitting it over the machine's own card slide. When you swipe your card through the slot, the card reader grabs the data from the magnetic strip and either stores it or transmits it wirelessly to a nearby computer.

At the same time, a camera mounted above the keypad - sometimes in the light that illuminates the machine or attached to a pamphlet rack, captures your fingers inputting your PIN into the machine.

The equipment takes only minutes to install, and just like that, thieves are able to capture everything they need to make copies of your card and use it to access your bank account or make purchases with your money -before you are even aware of it.
Five Tips to Protect Yourself from ATM Card Skimming

While the equipment and techniques used by credit card skimmers is getting more sophisticated, there are ways to protect yourself and your bank account from identity theft through skimming.

1. Choose ATMs in well-trafficked areas or those that are in view of a clerk or attendant at all times. It's harder for a thief to access a supervised machine to attach the skimming equipment.

2. Wiggle the card reader and make sure that it's securely attached to the ATM. If it gives, it may not be a legitimate piece of the machine. Use another ATM, and report the machine to the local police so they can check it out.

3. Check for glue on the face of the machine, and look for plastic overlays over keypads. If you find glue or glue residue around the corners, avoid that ATM and report it.

4. Cover the keypad when entering your PIN. Simply cupping your other hand over the keypad can prevent a camera from capturing your PIN.

5. Check your bank and credit card statements carefully to spot anything out of the ordinary, and report them immediately to your bank or Credit Card Company.
For more info on card skimmers see:

ATMS rigged with "Skimming" Devices for identity theft; steal $500G (video included)

And, be sure to see this earlier blog to avoid falling victim to a rogue waiter or store clerk who uses handheld skimming devices to steal your credit or debit card info while you are dining at a local restaurant or shopping at the mall.

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.