ATM and Gas Pump Skimmers

From the Office of Minnesota Attorney General Keith Ellison

Criminals are constantly inventing new types of technology to steal consumers' credit and debit card information. By being aware of these methods, consumers can better protect their money and credit. For instance, some criminals attach credit or debit card readers, known as "skimmers," to ATMs and gas pumps.

So what are "skimmers?" And how can you protect yourself?

What are "skimmers?"

A skimmer is a small device (often smaller than a deck of cards) that scans and stores credit or debit card data from the card's magnetic stripe. If a card is run through the skimmer, the data is stored, and the criminal can later use that information. Criminals often install a skimmer onto an ATM or gas pump and then collect it a day or two later.

For debit cards, criminals sometimes place small cameras that secretly record as the cardholder enters his or her Personal Identification Number (PIN) into the keypad. The cameras are usually a small "pinhole" camera that can be hidden in a manner that blends in with the machine.

Criminals can then either sell the information over the internet or create counterfeit cards to use for shopping sprees. Often times, the card holder does not know about the theft until they get their card statement. The newer credit cards that have security chips installed still have information on the magnetic strips that can be recorded by a skimmer.

Is this a crime?

Yes. Stealing the data stored on the magnetic strip of another person's credit or debit card is a crime under Minnesota law. Under a law supported by the Attorney General's Office, just possessing a skimmer or equipment to create counterfeit cards is a felony under Minnesota Statues Section 609.527, subdivision 5b (2017).

How can you tell if a skimmer is attached to a gas pump or ATM?

One way is to look at other nearby gas pumps or ATM machines. They should all have the same set-up. If the card reader at the gas pump or ATM you are using looks different from the others or looks like it has been tampered with, do not use it.

Look for security tape. Many gas stations now put a piece of security tape over where the card reader is installed. The security tape is modified so that any tampering will be obvious to the casual observer.

Look for tampering. Some criminals have the time and expertise to break into the gas pump or ATM and install the skimmer inside the machine. However, there will usually be signs of the break-in: different colored parts that don't match the rest of the pump or ATM, graphics that are not lined up, or signs of tampering at keypad or card reader itself.

Wiggle everything. If you cannot see any visual differences, push at different parts of the machine, especially the card reader. ATMs and gas pumps are solidly constructed and should not have parts that are loose.

Use your Smartphone's Bluetooth function. Many skimmers contain Bluetooth technology to transmit stolen information. When you are standing near a pump, activate your Smartphone's Bluetooth function. If you see a long string of numbers trying to connect with your phone, that is a sign of a nearby skimmer.

Use your best judgment. If you suspect that either an ATM or gas pump have been altered, do not use it. Notify the bank that operates the ATM or the gas station employees of your concerns. When dealing with banks, ask for their Corporate Security Department that deals directly with the security of the ATMs.

Minnesota Attorney General's Office • 445 Minnesota Street, Suite 1400, St. Paul, MN 55101
Twin Cities Calling Area: (651) 296-3353 • Outside the Twin Cities: (800) 657-3787 • Minnesota Relay: (800) 627-3529
www.ag.state.mn.us

How can you protect yourself?

When you go to a gas station, try to choose a pump that is close to the main building or one that the gas station attendant can clearly see. Criminals often choose pumps they can easily access undetected to install skimmers.

If paying with cash inside the gas station is not an option, only use a credit card at the gas pump or choose the credit card option for your debit card. There is significantly more fraud protection for credit cards than debit cards. Also, by using the credit card option for your debit card, you will not have to enter your PIN.

When using your debit card at an ATM, use your other hand to cover the keypad as you enter your PIN. That should block any cameras from recording your PIN.

If you believe your card information was stolen by a skimmer, report it immediately to your bank or credit card company and the police. Reporting the matter as soon as possible can limit your liability for any fraudulent transactions.

Regularly review your bank and credit card statements for any unauthorized charges to your account. If you think someone has fraudulently used your card information, contact your bank or credit card company as soon as possible. There are laws to protect you from certain unauthorized charges if you promptly report them.

For help with a consumer problem, contact the Attorney General's Office at:

Office of Minnesota Attorney General
Keith Ellison
445 Minnesota Street, Suite 1400
St. Paul, MN 55101
(651) 296-3353 (Twin Cities Calling Area)
(800) 657-3787 (Outside the Twin Cities)
www.ag.state.mn.us

This document is available in alternative formats to individuals with disabilities by calling
(651) 296-3353 (Twin Cities Calling Area), (800) 657-3787 (Outside the Twin Cities), or through the Minnesota Relay Service at (800) 627-3529.

The Minnesota Attorney General's Office values diversity and is an equal opportunity employer.