Wisconsin Crime Prevention Practitioners Association

Skimming Devices

WORKING TOGETHER TO KEEP WISCONSIN SAFE

Connect with us

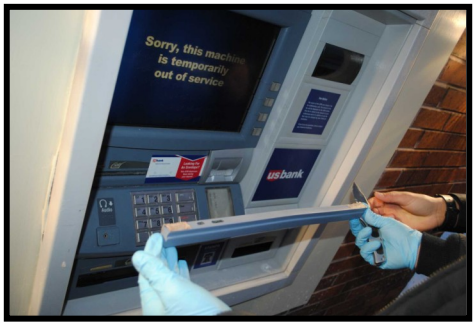
In the past couple of years there have been a few incidents reported to law enforcement across Wisconsin of skimming devices being placed on automated teller machines (ATM).

What is this?

A method used by criminals to capture data from the magnetic stripe on the back of a credit/debit card. Once that data is stolen, criminals will use it to make a cloned card, online purchases or sell the information on the internet.

What does a skimmer look like?

Devices used are smaller than a deck of cards and are often fastened in close proximity to, or over the top of the ATM's factory-installed card reader. In addition to skimming the card info, the scammer needs your PIN. They will strategically attach/ position cameras and other imaging devices to ATMs to fraudulently capture PIN numbers. Once captured, the electronic data is put onto a fraudulent card and the captured PIN is used to withdraw money from accounts.



Skimmer attached over actual card reader

Small camera attached to brochure holder to capture PIN

How it works?

Criminal installs skimming device and camera on ATM

User uses ATM and enters PIN. Devices capture both.

Devices are removed and info is downloaded.

Skimmers tactics

- These devices will normally be attached to ATMs or card readers that are located in less traveled areas so to avoid detection. The criminals will visit these locations either late at night or very early in the morning.
- The devices will only be attached for a short period of time, typically a day or less so as to not attract attention.
- As shown in the photos on the other page, oftentimes there is a camera nearby in order to capture the user's PIN.
- The criminals may hang out nearby to observe customers & remove equipment after several people have used the ATM.
- There also have been skimming devices that have been left on machines and the criminal will download the info from the device.

Prevention

- Familiarize yourself with the ATM or card reader. Check the actual card slot to see it is loose or wiggles. That is an indication that something may have been attached.
- Many locations are now installing security tape over the card readers and access panel. Check to see if that tape is tampered.
- If anything seems amiss with the machine DO NOT use it and contact the business and law enforcement.
- Look for ATMs in highly traveled areas or ones inside of a business. It is less likely that those machines are compromised due to too many people around.
- Monitor your accounts online routinely. Look for any out of the ordinary transactions. Don't just focus on large transactions, criminals have been known to make small charges on hundreds of cards in the hopes that they won't be detected for a period of time.

Steps to take if you've been a victim

- If you find a fraudulent transaction notify your financial institution immediately and file a report with your local law enforcement agency.
- Place a fraud alert on your credit report. What this does is force businesses to contact you and confirm your identity before approving any credit applications in your name.