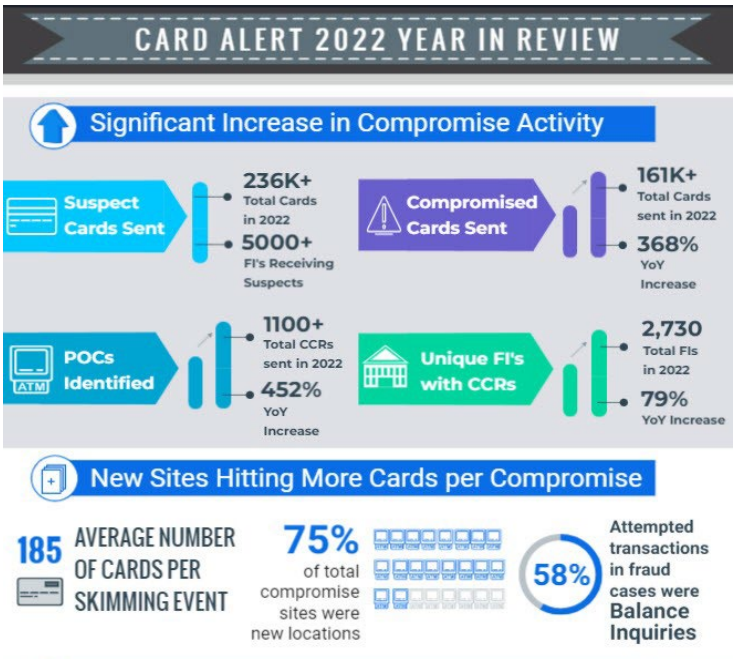
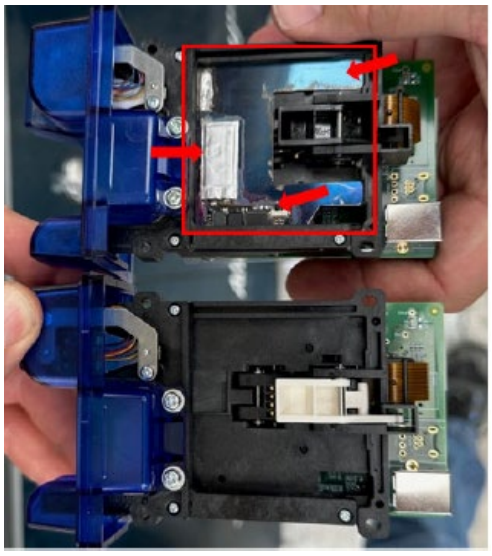
Vigilance and fast action can help deter ATM skimming fraud

ATM skimming attacks continue to occur at alarming levels. In 2022, there were over 161,000 cards compromised and 2,730 separate financial institutions were affected due to skimming activity according to data from FICO. That number increased nearly five times from the year before. Financial institution ATMs and gas pumps continue to be the most common targets for fraudsters.



Nebraska credit unions have not been immune from skimming attacks. The following pictures were received from a Nebraska credit union that recently discovered a skimming device during a preventative cleaning of one of their ATM machines.

To the normal eye, a credit union member would not know that a skimming device resides inside the card reader. Cards inserted into the machine may have felt “tight” being inserted into the machine but otherwise unnoticeable. Upon closer examination, you can see a thin piece of metal in the machine which is the internal skimmer. The device is inserted into the machine just as a normal debit card but is designed to remain inside.



After the entire card reader was removed by the technicians, you could see the internal skimmer. The blue horseshoe shaped metal piece, a silver metal piece (possibly battery supply) and electronics all make up the skimming device. More than likely, this skimmer would remain in the machine and data would be electronically transmitted via Bluetooth to the fraudster.

A false trim piece was applied to the front of the machine. The colors blended very well with the machine. The false trim was covering a built-in light on the machine.

The false trim piece was applied with an easy to remove adhesive.

Once removed, a very small camera with

battery supplies and SD card were discovered. A hole in the bottom of the false trim was pointed at the keypad recording PIN entries.

The devices were removed from the ATM machine and turned over to the proper authorities. Based on information from the FBI, they believe they know who the fraudsters are but have been unable to apprehend them. They tend to work in one area for so long and then move on.

After years of evolution and perfection, it is easy to see that these skimming devices can look like a legitimate part of an ATM unit. They tend to be very sophisticated operations that may contain blue tooth technology capable of retrieving information remotely, eliminating the need for the fraudsters to reapproach the ATM, making it very difficult to catch them in the act.

No ATM is safe from these fraudsters. ATM custodians should make an extra effort to closely and frequently examine the front of every ATM for unusual attachments that may be disguised as native equipment.

Examine the façade of the ATM equipment for sticky tape of Velcro residue. The presence of similar sticky adhesive may indicate that an ATM parasite was attached prior to examination.

It may also be helpful to photograph ATM equipment to aid in any physical security inspection.

Finally, contact local law enforcement if you suspect any tampering with your credit union's ATM equipment.