

BEWARE OF CREDIT CARD SKIMMERS

Technology often makes life easier for us, but it can also lend its usefulness to criminals intent on defrauding us. One of the many ways identity theft can happen is through credit card skimmers.

A credit card skimmer is a device that criminals use to capture the data found on the magnetic strip of your ATM, debit or credit card. The two most common types are a reader (which reads the card when it is swiped) and a camera (which records your PIN when you enter it). Thieves often use both at the same time, thus obtaining both your personal information and your PIN.

Skimmers are designed to look like a real part of an ATM, cash register, gas pump or other self-service machine, or they can be concealed and used secretly by a criminal that you willingly hand your credit card, like a cashier. Criminals attach skimmers to ATMs and other machines to harvest data from users. Skimmers can be high-tech: Many skimmers are designed to wirelessly transmit the information they gather to the thieves.

Skimmers attached to self-service machines are usually placed over the slot where you insert your card. When you put your card in the machine, it runs across the skimmer as it enters the machine. Cameras are usually placed above the keypad, although they are sometimes hidden outside the machine. Sometimes, the thieves will even replace the keypad with a keypad that will record your PIN, eliminating the need for a camera at all.

It can be difficult to tell if a machine you are using has been tampered with. For obvious reasons, criminals try very hard to hide what they are up to. Look at the machine and see if anything looks out of place. Check for obvious signs, such as scratches, tape or glue residue, or a card slot that looks unusual that might show that the machine has been tampered with. Also, get to know the self-service machines that you use regularly, which can help you detect tampering.

Most ATMs have a light where you insert the card: Do you see one? If not, it may be because a skimmer has been placed over the slot. Look above the keypad. Is there a hole for a camera? If you suspect a machine that accepts a card has been tampered with, DO NOT USE IT. Report the matter to the bank or the owner of the machine. A good rule of thumb for protecting yourself from a concealed credit card skimmer is to avoid letting your credit card out of your sight and control. Pay at the register instead, if possible, where you can keep an eye on your card, and cover your hand whenever you enter your PIN on any keypad.

It pays to be aware and educated about the ways technology can be used against us, so we can be wise about the ways in which we use technology.

R. Michael Shickich is the founder of the Injury Law Firm located in Casper. The focus of his practice is personal injury and wrongful death cases.

The Wyoming State Bar does not certify any lawyer as a specialist or expert. Anyone considering a lawyer should independently investigate the lawyer's credentials and ability, and not rely upon advertisements or self-proclaimed expertise.