

Bankers Beware! Skimmers Found in Nebraska

Everyday tasks such as filling up the car with gasoline or stopping to get cash at an ATM could result in one of your customer's bank accounts being emptied. Area law enforcement have reported that crooks are attaching card skimmers to gas pumps and ATM machines and capturing unsuspecting people's debit and credit card information. Several cases have recently been reported in Omaha.

Here are a few tips from the FBI in order to avoid being skimmed. Feel free to share these with your customers.

- ★ Inspect the ATM, gas pump, or credit card reader before using it. Be suspicious if you see anything loose, crooked, or damaged, or if you notice scratches or adhesive/tape residue.
- ★ When entering your PIN, block the keypad with your other hand to prevent possible hidden cameras from recording your number.
- ★ If possible, use an ATM at an inside location (less access for criminals to install skimmers).
- ★ Be careful of ATMs in tourist areas. They are a popular target of skimmers.
- ★ If your card isn't returned after the transaction or after hitting "cancel," immediately contact the financial institution that issued the card.

If your bank or business customer finds a skimmer on any machine, contact the U.S. Secret Service in Omaha immediately at 402-965-9670. Do not remove the unit as the Secret Service will want to examine how it is hooked up and collect fingerprints if at all possible.

Always remember to use common sense when using an ATM. If you are uncomfortable or observe ANY suspicious activity, leave immediately.

ATM Skimming

Skimming is an illegal activity that involves the installation of a device, usually undetectable by ATM users, that secretly records bank account data when the user inserts an ATM card into the machine. Criminals can then encode the stolen data onto a blank card and use it to loot the customer's bank account.

1 Hidden camera

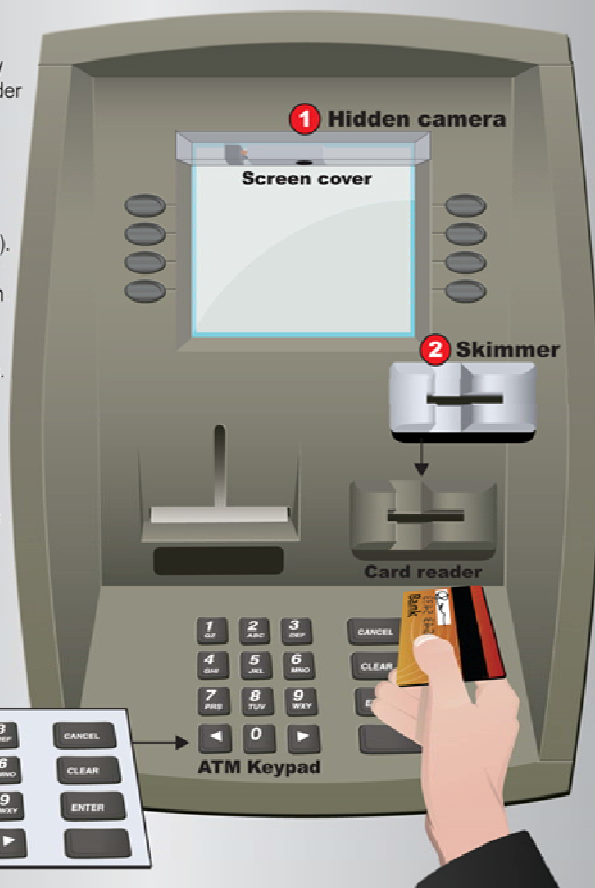
A concealed camera is typically used in conjunction with the skimming device in order to record customers typing their PIN into the ATM keypad. Cameras are usually concealed somewhere on the front of the ATM—in this example, just above the screen in a phony ATM part—or somewhere nearby (like a light fixture).

2 Skimmer

The skimmer, which looks very similar to the original card reader in color and texture, fits right over the card reader—the original card reader is usually concave in shape (curving inward), while the skimmer is more convex (curving outward). As customers insert their ATM card, bank account information on the card is "skimmed," or stolen, and usually stored on some type of electronic device.

3 Keypad overlay

The use of a keypad overlay—placed directly on top of the factory-installed keypad—is a fairly new technique that takes the place of a concealed camera. Instead of visually recording users punching in their PINs, circuitry inside the phony keypad stores the actual keystrokes.



Source: www.fbi.gov