

The US Secret Service estimates that annual losses from ATM skimming total about \$1 billion each year, or \$350,000 a day.

Just as various cities and regions of the country take their turns weathering unusual increases in bank robberies, so do they experience fluctuation-sometimes large ones-in other crimes. Take San Luis Obispo, California. A recent spike in debit card fraud has local detectives and regional US Secret Service agents fit to be tied. The crime of choice? Skimming. Fraudsters have hit so many gas stations that the law officers have resorted to driving around and inspecting pumps, looking for alien adjuncts to the standard pump automatic pay equipment.

There are essentially two ways in which identity thieves skim your card:

1. A criminal places a small, hard-to-notice card reader called a skimmer over the card slot of an ATM or automated gas pump (and occasionally at cash registers). The device is often used in conjunction with a hidden pinhole camera. The skimming device gathers data from the magnetic strip on the back of the card and the camera records how you enter your PIN. Sometimes a fake keypad that slips over the existing keypad and transmits the numbers is used. The skimmer transmits the stolen information via a wireless modem to the fraudster, or the fraudster returns to remove the skimming equipment and the information they contain. With this information, this highly successful criminal makes a duplicate of your card and uses it to withdraw money from your account and/or make purchases and perhaps sell the goods on the black market.
2. In the second method, the identity thief finds temporary employment at such places as restaurants, cafes, hotels or other retail businesses. When you make your payment, the fraudster swipes your plastic through the legitimate payment system and also surreptitiously through a small card skimmer which can be easily concealed in the pocket, apron, or palm of the hand. Either way, the skimmer does not interfere with the processing of the legitimate transaction and you will not find out that you've been had until you receive your monthly statement. As difficult to believe as it may seem, skimmers are easy to come by. They can be purchased on the Internet for about \$300. Some fraudsters purchase the equipment necessary to make counterfeit cards, the next step. This is the expensive: about \$10,000. Others sell the card information to the counterfeiters.

Commercial Customers

Business owners, franchise operators, and employees are reminded to:

- Treat the point of sale terminal with the care you would exercise if it were a pile of cash.
- Allow the POS terminal to be accessible only when it is used.
- Lock the POS terminal up at night.

Other Customers

- Check ATMs and other POS sites for anything about the site that appears unusual, and obviously in the vicinity of the card slot.
- Shield your PIN with your hand or body when conducting transactions at an ATM or point-of-sale site. Remember, you want to block the view not only of potential shoulder surfers and those with high-powered lenses (movie cameras; binoculars), but also the view of a pinhole camera pointed down at the keypad.
- Keep your payment card in sight at all times!
- Tear up or, better, shred all receipts, slips, and statements after using them.
- Do not keep a written copy of your PIN, especially with your card.
- Never leave a payment card lying around.
- Check your financial statements regularly.
- Contact your financial institution immediately if you detect any unusual activity reflected on a statement.

Tips for spotting Skimmers:

- Be aware of your surroundings whenever making an automated card transaction. Choose only highly visible, well-lighted machines.
- Pay attention to the front of machines. If a machine looks different from others in the area (for example, if it has an extra mirror on the face), has sticky residue on it (potentially from a device attached to it), or extra signage, use a different machines and notify bank management about your concerns.
- Be aware of how it feels to type in your PIN. If it's difficult to strike the keys, or if you feel a strange resistance, it could indicate the presence of a keypad overlay.
- If you think the area around the card entry slot looks peculiar, try pulling on it. If it loosens or comes off, do not use the device, alert bank management, and try to leave the machine as close as you can to the way you found it. Leaving the evidence in place will help the authorities.
- If you find a skimming device, in addition to notifying bank management, notify local law enforcement.