Identity Theft

CARD SKIMMING

Credit and debit card skimming is when potential thieves steal or "skim" your card information. They use it to create an illegal copy of your card (called "cloning") or to charge items to your card over the phone or online. Or they may sell it to others to do the same.

Thieves use skimming devices that are small, easily portable and hard to detect. Certain types are illegally installed on ATMs and sales terminals such those on gas pumps.

Card skimmers fit over original card readers. As you insert your card, the account information stored on it is skimmed by the device. Keypad overlays are placed on top of factory-installed keypads. The circuitry inside the overlay stores your keystrokes, such as those you make when you enter your PIN. Thieves also may install hidden cameras to record your entering your PIN. These devices are more often installed on non bank ATMs.

At an ATM or sales terminal, check to see if the colors and materials used match up. Look for an extra piece of plastic or anything that appears added on, wrong or out of place. These can be signs of skimming devices.

Don't use the machine if anything looks suspicious. It's better to be safe than sorry. And remember, if anything looks funny or doesn't feel right, walk away.

Pay it Safe

Whether you are running errands or just out for fun, be vigilant about payment card safety.

- Observe the person you're paying. Make sure that person isn't holding anything like a portable skimmer and that your card doesn't leave your sight. When you receive your card back, double check that it is indeed yours and was not swapped for another.
- Insist on privacy when entering your PIN.
- Check sales vouchers carefully before signing.
- Never leave a line blank on a receipt. Draw a squiggly line through any blank space to prevent an unwanted amount being added.
- Be sure a transaction is complete before you walk or drive away from an ATM machine.
- Always take card sales receipts or ATM transaction slips. Never leave them near the ATM or sales terminal. Save them to compare against account statements. Shred them when no longer needed.
- When eating at a restaurant, ask to pay your bill up front at the sales terminal instead of giving your card to a server, or pay at the table when available.
- Consider using Apple Pay or Google Pay with your mobile device. Cashiers can't see your card number, and the process is secure.
- Consider using RFID-blocking card carriers and protectors. Although rare, skimming devices can scan, read and capture information from payment card embedded with RFID tags just by being near them.