Protect Yourself Against Skimming!

What is Skimming?

Skimming is when scammers install devices that are placed on and inside card terminals such as ATMs, fuel pumps, and registers. These devices record and steal your card information and can record your PIN entry. This practice is illegal, and criminals will use the data they collect to create a copy of your card and make unauthorized purchases.

What are the Most Common Forms of Skimming?

The most common forms of skimming can be captured from fuels pumps, ATMs, and POS systems like those at grocery stores and self-checkouts.

How Does Skimming Work?

Skimmers look very similar to the everyday terminal that you see. They are put over the card slot and take information from the card such as your name, the card number, the expiration date, and your CVV. There may also be a keypad overlay that records your PIN entry. Sometimes, in bigger machines such as ATMs and fuel pumps, a hidden camera may be placed as well. Skimming devices are very quickly placed and installed, so it is very easy for scammers to place these devices even in high traffic areas.

What do Scammers do with my Information?

Once a scammer has your information from a skimmer, they can go on to duplicate your card to make purchases. Scammers will even sell your data to other fraudsters.

How Can I Avoid Being a Victim of Skimming?

Be vigilant and take a second to look at the card terminal before you enter your card. If anything looks suspicious, do not enter your card and inform a worker, or call a service number if provided on the machine.

Tap-to-pay when possible. Skimming devices can not capture card data when tap-to-pay is used.

Use your Apple Pay, Samsung Pay, Google Pay, or other card wallets to avoid coming in contact with a skimming device.

If you think you have been a victim of skimming, contact your financial institution immediately.

Visit https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/skimming to learn more and stay ahead of skimming scams!