08/29/2014

By: Mark Pribish, Special for The Arizona Republic, June 5, 2014, used by permission of the author

When you swipe your credit or debit card, there is always a risk of giving ID-theft criminals what they need to steal your money through what is known as "skimming." Criminals install electronic devices at locations at which we use cards, such as an ATM, a grocery store or a gas pump. As you use your card for valid transactions, the device copies your credit or debit account information in the magnetic strip on the back of your card. This is skimming.

Recent news reports have shown that ID-theft criminals are installing card skimmers at bank ATMs and point-of sale-terminals. They deliver an opportunity to conduct illegal transactions — in your name, from your accounts.

The prize that ID-theft criminals value most is capturing debit card data complete with personal identification numbers. This allows them to make counterfeit cards to withdraw cash directly from your bank accounts at ATMs.

That said, credit and debit card transactions continue to be a big target for ID-theft criminals. These four types of skimming fraud lead the way:

• Pay-at-the-pump skimming. Devices are secretly placed inside the gas pump. Often these devices include a small video camera that records you as you enter your PIN or billing ZIP code. To make matters worse, currently there are approximately four universal keys that open the majority of gas pumps in the US. Criminals are aware of this and often duplicate these keys to install the skimmers.

• ATM skimming. Unlike gas pumps, financial institution’s ATMs require unique keys and codes. However, law enforcement has documented multiple methods of ATM skimming where

criminals replace PIN pads on ATMs with manipulated devices that collect card details and PINs as customers use their cards.

• Point-of-sale skimming. POS skimming may occur at retail stores where customers swipe their credit/debit cards using point-of-sale terminals. If tampered with by ID-theft criminals, the skimmer can record all information for every credit and debit card processed through the card reader.

• Magnetic-card reader skimming. This occurs when your card is out of your sight, such as at a restaurant or in a drive-through, as a dishonest employee can swipe your card through a card reader that stores the information from the magnetic strip, allowing for the creation of a fraudulent credit/debit card.

Here are recommendations to reduce the risk of being a skimming victim:

• Never allow your debit card to be swiped away from your view.

• Cover PIN and ZIP code entries when in public.

• When using a debit card, do not type in your PIN; instead, select the credit option as consumers have greater protection under credit-card transaction laws.

Mark's most important: Be aware that skimming is happening, and do your part to reduce the chances that you'll become a victim.

Mark Pribish is vice president and ID-theft practice leader at Merchants Information Solutions Inc., a national ID-theft and background-screening provider based in Phoenix.