FBI busts multistate card-skimming ring

Consumer Watch
Bill Moak
Columnist

As you gas up your car during holiday trips, the FBI is warning consumers to watch out for credit card skimmers on gas pumps, which could be used to steal your money and identity.

The FBI and a U.S. attorney this week announced they had busted a multistate ring that had installed skimmers on gas pumps across Kentucky, Ohio and Indiana. Officers collared eight people in an operation that included more than 30 law enforcement agencies across the three states, after the thieves made off with more than 7,000 card numbers and about $3.5 million.

"This form of identity theft is causing untold losses to both financial institutions and individuals who are merely filling their tanks at the gasoline pump. As we begin the busiest travel season of the year, consumers need to pay special attention to where and how they pay for gasoline as criminals are using new and more sophisticated technologies," noted U.S. Attorney Russell Coleman.

Skimmers are becoming increasingly sophisticated, and thieves have gotten proficient at making them look close enough to the real thing to fool all but the savviest customers. Thieves install the devices over the card-swipe device on the pump, and in some cases, replace the pump's original card reader. When unwitting customers swipe their cards to pay for gas, the device reads the card number and other information, which is then used to raid the customer's bank account or steal their identity.

You may recall that police last year found a skimmer installed on gas pumps in the Clinton area, resulting in arrests and indications the activity was part of a larger ring operating across several states.

In the case announced this week, the FBI reported the thieves installed the devices inside the gas pumps, then later retrieved them. The stolen financial information was then re-encoded, transferred, or cloned on to the magnetic strip of other plastic cards that were sold or used to purchase merchandise.

Although skimming is not a new phenomenon, it is getting harder to detect. PC Magazine's Max Eddy wrote about the technology last year, noting the devices are now smaller than a deck of cards, and can be placed on an ATM or point-of-sale terminal easily. Often, he notes, thieves will also place a camera nearby to record Personal Identification Numbers of customers, but in some cases, they have installed fake keypads as well.

Spotting a skimmer is not always easy, but Eddy gives a few pointers:

- **Watch for mismatched colors or styles.** If the overall color in the area where you insert your card is black, for example, but the card reader is yellow, that could be a sign that it's fake. Also, watch for mismatches in lettering or the materials used.
- **Wiggle everything.** Since readers have to be hastily installed so the thieves won't get caught, they don't usually have much time to make sure everything fits perfectly. Eddy advises pulling at the reader and keypad to ensure nothing moves.
- **Look around.** Cover the keypad with your hand, to prevent anyone from seeing your fingers as they enter the PIN. Many devices now have a little shield over the top of the keypad to prevent someone seeing your fingers as they enter the numbers, or recording your movements from a distance. Still, covering the keypad as you enter can prevent thieves from getting the all-important PIN.
- **Use the EMV chip.** Since most newer card readers accept EMV (Europay, Mastercard, Visa) chips that require your card to be inserted, this option gives you more security and requires thieves to install devices inside the reader.
- **Pay inside.** It's less convenient to pay inside the store, but generally more secure.

It's also a good idea to keep up with your purchases. Most banks now have apps that allow you to keep up with transactions, so if you notice any activity you didn't authorize, report it immediately.

Contact Bill Moak at moakconsumer@gmail.com.