

Scam Alert: No PIN at the Pump

You swipe your debit card, and `skimmers' swipe your money

It's becoming a familiar scenario: Soon after filling up at the gas pump, a motorist learns that his bank account has been emptied.

What happened? Another case of "skimming", in which crooks place a portable card-reading device readily available over the Internet inside the pump. When the customer inserts his debit card and enters the required personal identification number, the device captures both the data from the card's magnetic stripe and the PIN.

Skimming was first reported by Scam Alert four years ago. But back then, skimmer devices were most often used at ATMs, usually in convenience stores, airports and shopping centers. In those locations, unlike a bank lobby, there were no cameras watching as crooks installed their equipment: a card reader that fits neatly atop the ATM's card slot and a tiny camera to record the customer entering a PIN on the keypad.

Later, the devices are retrieved, and the stolen data is used to create a duplicate card to raid the victim's bank account.

Debit cards an increasing target

Skimming is a bigger threat than ever, especially now that debit cards are estimated to account for nearly 60 percent of all "plastic" purchases.

Although ATMs are still a target, the bigger danger these days is at gas stations, where skimmers can be placed inside the pumps and never be noticed by consumers.

"There are only a couple of manufacturers of gas pumps, so typically if you have a key to open one pump, it can open others at different stations," says Avivah Litan, a security analyst at Gartner Research, which tracks fraud trends. "And because gas pumps tend to be unattended, crooks have easy access to place a skimmer without being noticed."

That was the case with one member of the Russian mob, which is often behind organized skimming rings. He took a job at an Arco station and placed a skimming device inside a gas pump. After he disappeared, authorities learned that his hidden skimmer stole \$300,000 from customers' debit cards.

"A lot of gas pumps use older technologies, so PIN codes are not encrypted," Litan tells Scam Alert. "Once they get the info from your card, and you enter your PIN, they can make a fake card and go to an ATM to take cash from your account."

How to protect yourself

There are ways to protect your PIN:

- If you use a debit card at the pump, choose the "credit" screen prompt instead of "debit" so you don't have to enter your PIN. The purchase amount will still be deducted directly from your bank account, but it's processed through a credit card network, providing greater protection if fraud occurs. Under law, you have \$50 of liability for credit card fraud. With debit cards, if you don't report an unauthorized transfer or loss within two days, you could be liable for up to \$500.
- Since it's less likely that a skimmer can be placed on a card reader at a cash register, a PIN transaction is safer when done inside the station rather than at the pump itself.

"Still, the safest way to buy gas and other purchases is with cash or credit card," says Litan. "Next safe is a signature debit transaction that doesn't require your PIN. From a security perspective, entering your PIN should be used as only a last resort."