'Skimmers' siphon credit card data at the gas pump

The Kansas City Star (MATT CAMPBELL)

Posted: 01/14/2013 10:58 AM

A gasoline pump dispenses fuel, but it can also siphon your bank account — for a lot more than the price of a fill-up.

Several area residents have become victims of a scheme that is called "skimming" because it involves a device that can be hidden inside a gas pump to skim the data from your credit card when you insert it.

Then you drive away not knowing you've been violated.

The crime has been more prevalent on the East and West coasts, but now it has arrived here.

"We've taken five or six reports in the last two days," William Burke, a detective with the Leawood Police Department, said late last week.

Members of one Leawood family discovered that someone had drained about $3,800 from their accounts through ATMs in Southern California before their bank alerted them. Family members retraced their purchases and found the common link was a gas station on State Line Road.

Burke said all the incidents reported to Leawood occurred on the Missouri side, but the victims contacted his department because they reside in Leawood. The cases were referred to federal authorities because they involve interstate fraud. A spokesman for the U.S. attorney's office in Kansas City said he could not confirm a pending investigation, but prosecutors elsewhere have built cases against skimmers.

"People don't expect when they swipe their credit card at a gas station they are handing over their credit card information to crooks," said U.S. Attorney Sally Quillian Yates, whose office in the Northern District of Georgia recently secured a conviction on conspiracy, credit card fraud and aggravated identity theft in a skimming case that involved more than 175 victims.

Skimmers have targeted ATM machines and still do, but gas pumps are increasingly favored because they are easier to tamper with, and there is less surveillance coverage.

Estimates have placed the scope of the crime nationally from $350,000 a day to $3 billion a year. Law enforcement officials say the perpetrators may be acting alone, with equipment that can be found online, or they may be part of conspiracies.

What is particularly aggravating is that the victims usually could not have known the gas pump was stealing their data because the skimming device is concealed within the machine.

Typically, the crooks unlock or pry open the pump and attach an electronic reader that captures the information from the credit card's magnetic strip. They may also include a tiny camera to capture a PIN as it is typed on the keypad.

The devices can store data from hundreds of hapless victims over several days. The thieves may then return to retrieve the skimmer or they may access the information through wireless technology. Often the skimmer is not detected until the pump undergoes maintenance or the receipt-paper roll is replaced.

Once the thieves have the data, it can be encoded on counterfeit credit or gift cards that can be used to make purchases or to withdraw cash.

As in the case of the Leawood family, banks will usually cover the loss for their customers once the theft has been discovered. But it still costs the economy, and it can be a major inconvenience for a victim who receives a huge credit card bill or discovers that an account has less money than expected.

Look for a Band-Aid-like seal on the gas pump. It usually will be on the edge where the door opens and can reveal if the pump has been tampered with.

- Choose the credit rather than debit option at the pump to avoid revealing your PIN, or pay inside.

- Watch your bank and credit statements closely or even check them online for unauthorized activity. Notify your bank immediately.