PRESS RELEASE from Twin Cities Organized Retail Crime Association

February 9, 2017

Gas pump skimming is a major public safety issue, and the criminals that steal our citizen's identities are getting away with it.

Over the past year regional jurisdictions have noted a substantial increase in skimming activity at area gas station pay-at-the-pump terminals. This press release is intended to provide an overview of skimmer technology, and tips for citizens to protect themselves and their livelihood.

A skimmer is a small device that scans and stores credit or debit card data from the card's magnetic stripe. If a card is run through the skimmer, the data is stored, and the criminal can later use that information. Criminals often install a skimmer onto a gas pump and then collect it a day or two later.

New skimmers have emerged that utilize Bluetooth technology, allowing the metadata to be uploaded remotely and removing the need to have the device physically taken out of the payment terminal for the sake of downloading the data.

For debit cards, criminals sometimes place small cameras that secretly record as the cardholder enters his or her Personal Identification Number (PIN) into the keypad. The cameras are usually a small "pinhole" camera that can be hidden in a manner that blends in with the machine. Recently, new skimmers have been recovered from gas pump terminals that also capture the PIN data from EMV-enabled cards without the assistance of a video-recording device.

Criminals can then either sell the information over the internet (i.e. "Dark Web") or create counterfeit AKA "Cloned" cards to use for money laundering purposes. Creating cloned cards require specific equipment, to include a computer (laptop/desktop), thermal printer, embosser, encoder, and card blanks.

Criminals will often purchase high value property to re-sell on the black market or purchase large amounts of prepaid or gift cards in order to extract the monetary value at a later time (AKA trade-based money laundering). Often times, the card holder does not know about the theft until they get their card statement and they are confused because they still have physical possession of their bank card.

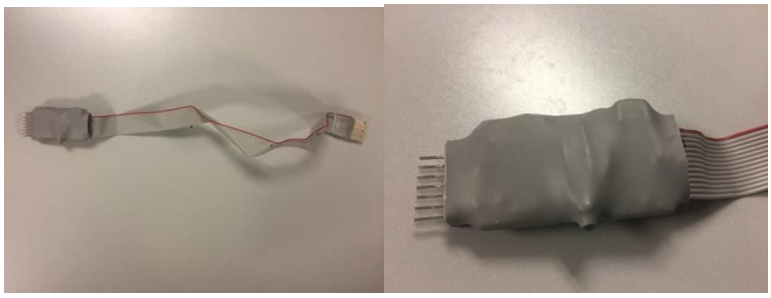
Under Minnesota State Statute 609.527, subdivision 5b (2016) it is a felony offense (5 yr. /$10k) to merely possess the devices noted in this informational bulletin:

Unlawful possession or use of scanning device or reencoder:

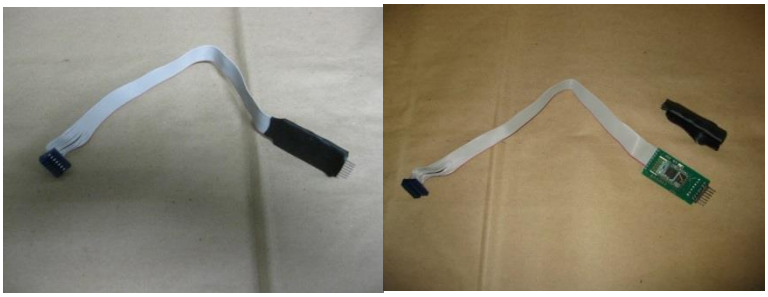
A person who possesses, with the intent to commit, aid, or abet any unlawful activity, any device, apparatus, equipment, software, material, good, property, or supply that is designed or adapted for use as a scanning device or a reencoder is guilty of a crime.

The following photos represent the items described in this bulletin:

Gas Pump Skimmer:



Bluetooth-enabled Gas Pump Skimmer:



Those involved in gas pump skimming MUST gain access to the interior of the gas pump terminal in order to implant the skimming device. Most gas station pump terminals are universally keyed.

Example of gas pump terminal keys:

While some gas stations now install site-specific locks on gas pump terminals, there are many convenience store gas pump terminals that are still universally keyed. Minnesota and Wisconsin-based Holiday, Super America, and Kwik Trip gas stations have either installed site specific locks or are working to convert older terminals to site-specific locks. Many so-called "mom and pop" or older franchise stores have gas pump terminals that are universally keyed and are especially susceptible to compromise.

States like Florida have enacted legislation (SB 912) that mandates the placement of security tape on gas pump terminals where the terminal meets the payment slot. A recent investigation by local news organizations found that a significant number of gas stations (close to 600!), especially "mom and pop" and older franchise stores, were out of compliance with the state law. Unfortunately, enforcing the law has been problematic.

While we encourage municipalities to mandate security tape, and applaud gas stations that do so as a part of their company policy, security tape alone treats a symptom but doesn't present a cure.

In order to stop skimmers being implanted in gas pump terminals, the terminals themselves MUST be secured with site-specific locks. While we support those companies that are taking steps to install or convert terminals to site-specific locks, we encourage legislators to pursue public policy initiatives that would make site-specific locks mandatory.

According to law enforcement and consumer advocate sources, each skimmer device can capture between 100 to 5,000 people's payment card data. With an average loss of $1,000 per victim, it's easy to extrapolate the economic cost, not to mention the stress and frustration of dealing with identity theft. Even if banks ultimately absorb the loss (oftentimes raises rates in other areas to compensate for fraud losses), the individual citizen feels an enduring victimization and uncertainty of future identity security.

There are a few things that consumers can do to decrease the chance of their financial information being compromised at the pump:

- Patronize stations that you know have site-specific locks.
- Only use pumps that are within eye sight of store station employees (avoid fringe pump locations).
- Use your other hand to cover up the entry of your PIN.
- Look for security tape. If it looks ripped or tampered with, move to a different pump and alert gas station employees.
- Use only one card for gas station purchases, and check your financial accounts regularly for discrepancies.
- Use cash.

There are other emerging trends that are increasing the threat of identity theft at ATMs and regular point-of-sale devices that consumers use every day. We at TCORCA will address some of those issues in future communications, however we feel that the rate of compromise and impact uniquely affecting gas pump terminals warrants immediate address.

The Minnesota Commerce Department's Weights & Measures Division, since March 2016, has been specifically looking for credit card skimmers and signs of tampering as part of its regular inspections of gas pumps statewide. To date, these inspections have turned up 29 skimmers on gas pumps in Minnesota. Whenever a skimmer is found at a pump, the Commerce Fraud Bureau pursues a criminal investigation in cooperation with other law enforcement agencies.

Anyone with information on gas pump skimmers should contact the Minnesota Department of Commerce Fraud Bureau at 1-888-FRAUDMN (372-8366) and the Weights and Measures Division at 651-539-1555. Any person that witnesses suspicious activity at gas pump terminals should contact 911 if the act is in-progress.

For press inquiries and media availability regarding this press release, please contact TCORCA Executive Director Charles Anderson, (Mobile) 651-592-9449, (Email) admin@tcorca.org, (Twitter) @TCORCA.

Related sources:

https://mn.gov/commerce/industries/retailers/card-skimmers.jsp

http://www.abcactionnews.com/longform/floridas-new-skimming-law-is-it-working

http://www.startribune.com/3-floridians-charged-with-identity-theft-from-credit-card-skimming-at-mpls-gas-station/401693545/

https://www.flsenate.gov/Session/Bill/2016/0912

https://www.youtube.com/watch?v=3z2lQSjSHb0

https://www.youtube.com/watch?v=0QMcs0MEMQw

###