Credit Card Skimmer Information for Motor Fuel Retailers

BUREAU OF WEIGHTS & MEASURES

PO Box 8911

Madison, WI 53708

608-224-4942

datcp.wi.gov

RESOURCES

An electronic version of this FAQ can be found on our website here: https://datcp.wi.gov/Pages/Programs_Services/PetroleumHazStorageTanksOwnerOperatorResources.aspx

Additional resources available from NACS Association for Convenience and Petroleum Retailing: http://www.nacsonline.com/Solutions/Store-Security-Signage/Pages/Skimming-and-Payments-Security.aspx

Additional Photos and information from the Secret Service: http://multibriefs.com/briefs/cema/pumpskimming.pdf

What is a credit card skimmer?

A credit card skimmer is a small electronic device that can be attached to a card reader on a gas pump to secretly collect credit/debit card information. Some skimmers are attached externally where the card is inserted, but increasingly skimmers are attached to the card reader inside the fuel dispenser. The skimmers frequently use Bluetooth wireless technology so a criminal is able to download the stolen information onto a laptop or mobile device, or transmit it via SMS to anywhere in the world.

How do I protect my dispensers against credit card skimmers?

Fuel dispensers come from the manufacturer with universal locks and keys. You should have additional security as universal keys are easily available. The best way to protect your dispenser is by using a customized lock and key. Many dispensers are designed for padlock use as well. Control who has access to the keys, and always know where the keys are.

Pressure sensitive security seals are also a widely used, good option. These seals are specially designed to clearly show if they have been compromised, such as the word void appearing if they are opened. Security seals should be placed over the gap on a non-hinge access panel to detect if it has been opened. It is most effective to use customized security tape so criminals cannot simply replace it with their own identical tape after they have installed a skimmer. Seals should be checked at least daily by the station to ensure there has been no tampering.

What should I do if I find a suspected credit card skimmer?

1. Do not touch the device or attempt to remove it. It is evidence of a crime.
2. Shut down the fuel dispenser. Do not let customers use it.
3. Immediately call the police and report the skimmer. The device should be removed by law enforcement.
4. Save any surveillance video footage from before the device was discovered.

What do skimmers look like?

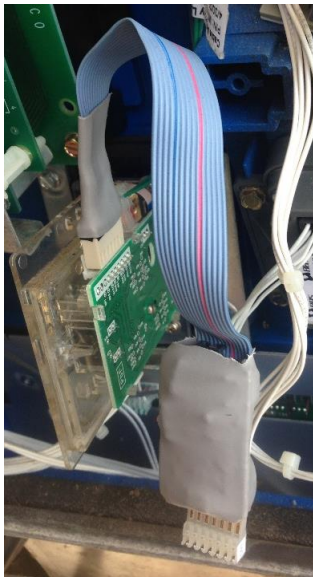
External Skimmers fit over the outside of the card reader. They may stick out further, be a different color or material, or appear newer or older than the other card readers. Often they will feel loose or come off when you try to wiggle them.

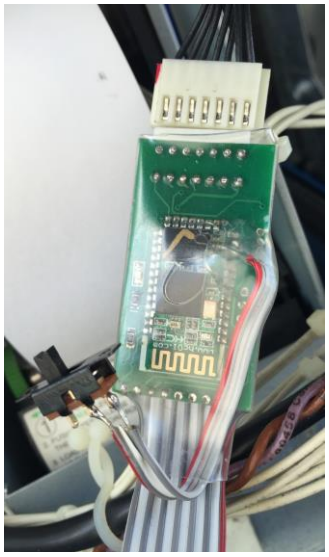
Credit Card Skimmer Information for Motor Fuel Retailers

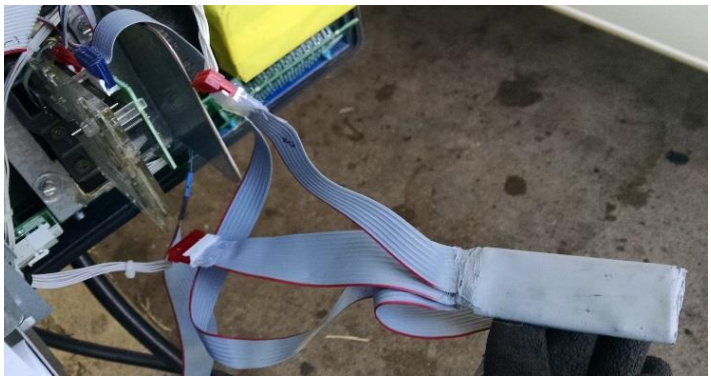
What do skimmers look like? (cont'd)

Internal Skimmers are installed inside the dispenser cabinet and are typically either a 7-wire cable with an in-line recording device or are in the form of a circuit board. They may be attached to the communication cable, the main board, or the card reader board

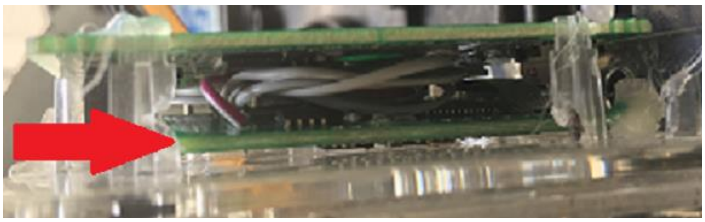
Skimmers on a 7-wire cable are plugged into the card reader on one end. The device's native communications cable is attached to the other end and runs to the unit's main board. Conversely, the false cable could be connected to the main board on one end with the native communications cable on the other running to the card reader.







Skimmers may also appear to be a second circuit board in the card reader unit, but they plug in to the communications cable port on the native board instead of being directly connected to the actual card scanner. Dispensers that have not been altered will not have this extra board.



Unaltered reader

Reader with extra board

Criminals may also try to capture PIN numbers. Look for cameras aimed at the keypad, false keypads placed over the real keypad, or connections from the keypad to an internal skimming device.