Anti-Skimming Tool Kit

Anti-Skimming Tool Kit

Credit card skimming continues to be a major problem at fuel dispensers across the United States. Every site should be aware of the information below in order to mitigate the risks of skimming. The merchant could be held responsible for a bank's losses, cost of reissuing cards, fines, etc., if the bank attempts to recoup their losses from a site that has been accused of being a skimmer victim. Losses attributed to credit card skimmers at service stations usually average $50,000 to $100,000 per incident.

Skimming FAQs

Q ***What is skimming?***
A Skimming is the act of using a skimming device to illegally collect data from the magnetic strip of a credit, debit or ATM card. This information is then copied onto another piece of plastic and used by the thief to make purchases or withdraw cash in the name of the actual account holder.

Q ***Where are skimmers found at service stations?***
A Skimmers can be found in multiple places in a service station. Some are hand-held and used by dishonest employees to capture data when customers present the cards. The most prevalent place for skimmers is inside the fuel dispenser. Overlay skimmers, which are becoming more common, are found on top of the external card reader at the pump or snapped on top of the existing pin pads inside the store. (see photos on Pages 7 and 8).

Q ***What do I do if I find a skimmer in a dispenser?***
A First, **DO NOT TOUCH THE DEVICE**. Immediately shut down the dispenser, call local law enforcement and call the Phillips 66 Fraud Hotline at 888-482-1838.

Q ***Will I be held responsible if a skimming incident happens at my location?***
A It's possible that you could be held liable for fraud losses caused by the credit card data stolen by way of a skimming device at your location. Visa and MasterCard, as well as other card issuers, use thorough analysis to determine where credit card information may have been compromised, and they have the right to go back to the merchant where the data was compromised and seek restitution.

Q ***What can I do to secure my fuel dispensers?***
A See Phillips 66 Best Practices for Dispenser Security on page 4.

Phillips 66 Best Practices for Dispenser Security

Inspections

- Become familiar with the inside of your dispensers, take photos for future reference or compare to other dispensers if you find anything that looks abnormal.
- Inspections of all devices inside the store and at the dispensers should be completed while wearing gloves. Devices will be inspected for forensic evidence once they are turned over to law enforcement.
- Open and inspect dispensers at least daily, preferably at the start of each shift, for any sign(s) of tampering or any foreign devices installed, particularly around the card reader. Pull all cables to ensure skimmers are not hidden below sight level (see photos on Page 4).
- The appearance of skimmers is always changing, so be suspicious of anything that looks unusual (see photos on Pages 5-9).
- Nonoperating or faulty operating card readers can be a sign that the dispenser has been tampered with, so inspect dispensers thoroughly if any card reader problems occur.
- If foreign devices are found inside the dispensers, on the external card reader of the dispensers or on top of the pin pad inside the store, **DO NOT TOUCH THE DEVICE**, shut down the pump and call local law enforcement and call the fraud hotline at 888-482-1838.
- A reward program is available through Phillips 66 for sites that recover a skimming device during inspections. See information on Bizlink, under Credit Cards/Fraud Prevention.
- For further information on how to properly inspect pumps, see the video, “How to Inspect Pumps for Skimmers” on Bizlink under Credit Cards/Fraud Prevention.

Locks

- Replace factory-installed locks with high-security locks that require a unique key that is specific to the location (see Phillips 66 recommended locks on Page 10).

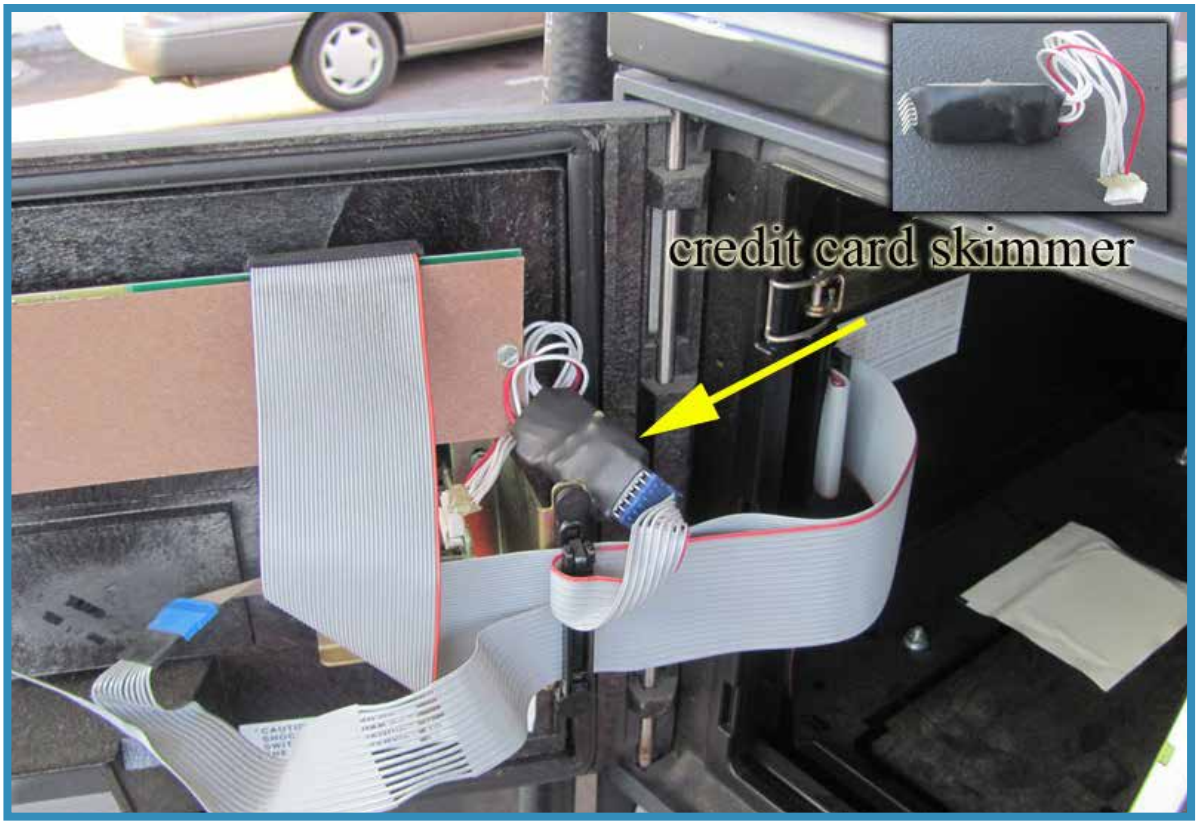
Security Tape

- Use serialized security tape on all dispensers. Security tape should be placed over the crind door so the tape will either break or show “void” if the thief attempts to reattach. The use of branded security tape is now part of the Mystery Shopper program (see photos and info on Page 12).
- Phillips 66 is making it easier and cheaper to secure your dispensers by providing up to 75 percent of the expense for new high security locks as well as branded security tape through the Co-Op Fund Program.

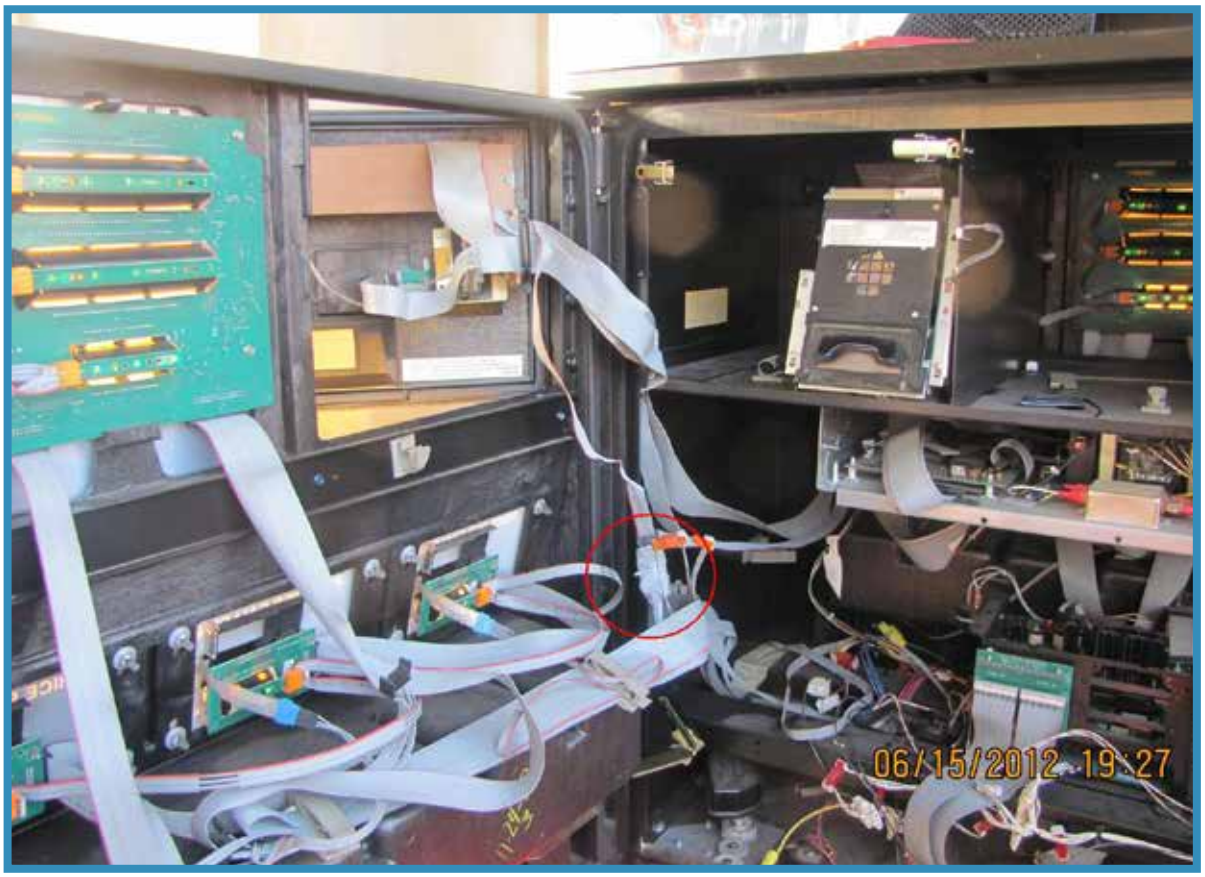
Surveillance

- Be suspicious of vehicles parked for a long time at the fuel island, especially on the outside pumps. If the site is not open 24 hours, all dispensers should be inspected as part of opening procedures. Newer skimming devices have wireless capability, so the thieves do not have to remove the skimmer to obtain credit card data.
- Use of video surveillance cameras at the fuel islands to deter criminals and to identify criminal activity is recommended.

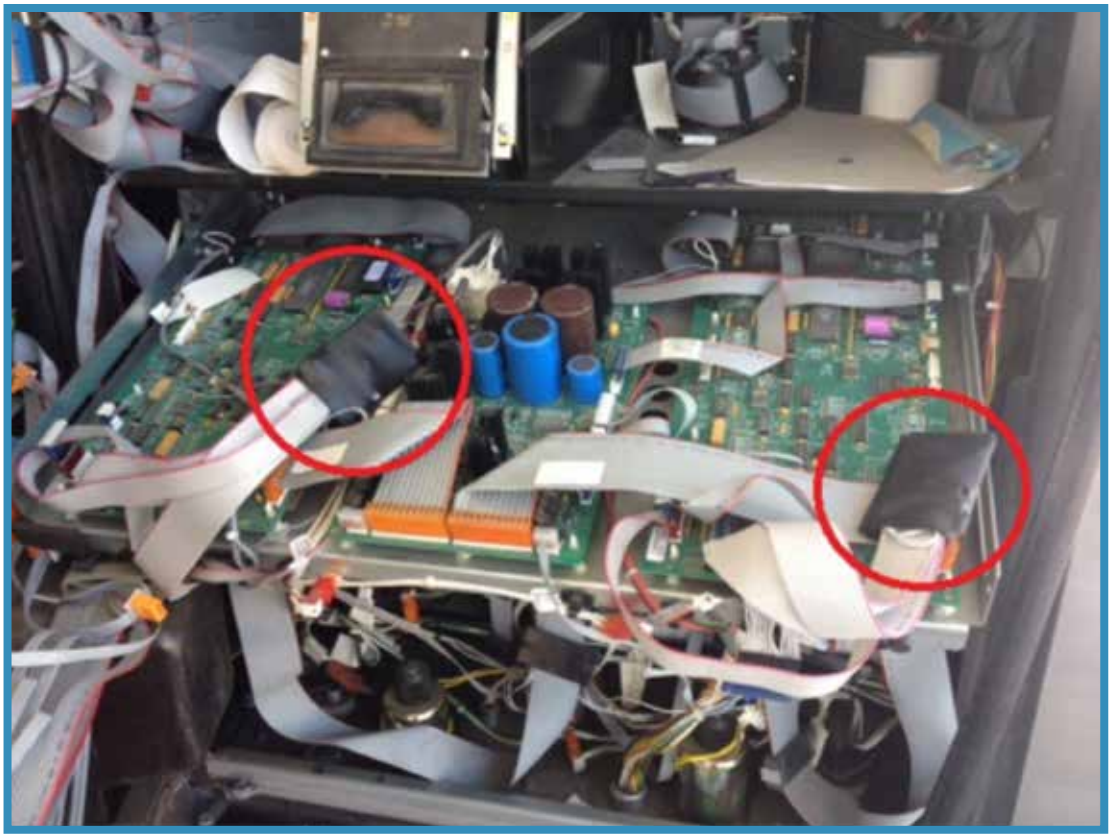
COMPLETING INSPECTIONS, UPGRADING LOCKS AND USING SECURITY TAPE IS THE MOST EFFECTIVE WAY TO SECURE DISPENSERS. YOU REMAIN VUNERABLE BY ONLY UTILIZING ONE OR TWO OF THE THREE SOLUTIONS.



An example of a skimming device installed directly behind the card reader and wrapped in black electrical tape.



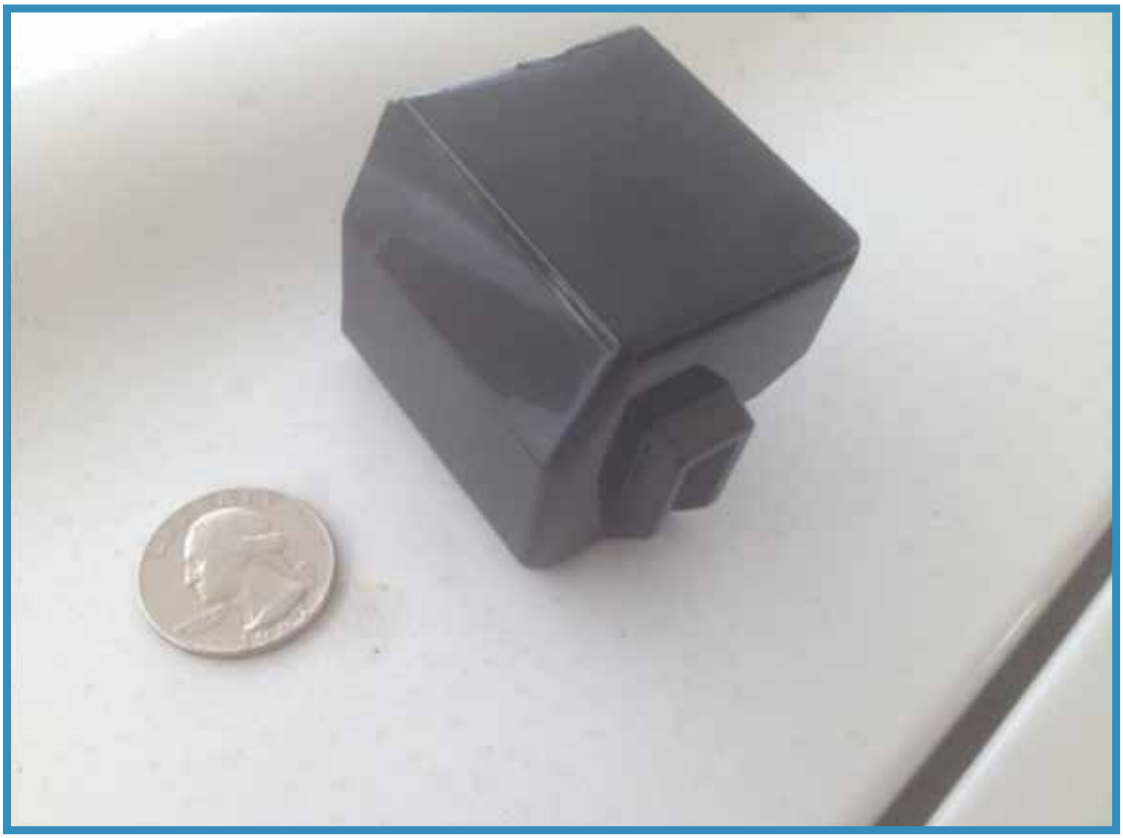
An example of a skimmer wrapped in grey electrical tape that was attached to a longer cable and dropped down below the crind door. This device is undetected when only the crind door is opened during inspections.



An example of two skimmers wrapped in black electrical tape and installed down by the motherboard of each side of the dispenser, below the card reader door and receipt paper. This was detected by a technician that opened the “refrigerator” door and pulled out the tray that holds the boards and cables.

An example of a very thin skimmer covered in a plastic coating that can be hidden easily. It is thin enough that it can be slid in between cables and spaces that may go undetected if the ribbon cable is not traced from end to end.

An example of an overlay card reader skimmer that snaps on top of the existing exterior reader.



These can be detected by checking for a loose connection. Pull on it, compare original photos of the card reader and look for distinct differences such as marks or scratches. Missing or voided security tape on the card reader would be a good indication that it has been tampered with.

These skimming devices are becoming more common inside the store and are installed within seconds if a cashier is distracted. Utilizing hologram labels that are visible to the cashier will determine if an overlay skimmer has been placed on top of your existing pin pad. A missing or voided label is a good indication the pin pad has been compromised. (see labels on page 12).

In the photo above, a suspect is attempting to install a pin pad overlay skimmer on top of the existing Verifone pin pad. The cashier was distracted by another customer when the suspect approached the counter. Beware of customers trying to distract your attention away from the the point of sale equipment!

The threat of credit card skimming is always changing. Be familiar with the inside of your pumps! New styles of skimming devices can be overlooked due to the similarities of an altered card reader and a nonaltered card reader. The photo above shows an altered card reader on the right, which includes an additional board for capturing data from each card that is swiped. Having photos of the inside of each dispenser is very important when inspecting your pumps. Comparing past photos of what your pump ***should*** *look like and what you are inspecting will make foreign devices more easily identified.*

This wrench and this key will open over 80 percent of fueling dispensers in the United States. It is imperative that the dispenser locks be upgraded as criminals have access to both the Wayne wrench and Gilbarco universal key.

Proper Use of Labels

Placement of tape on a Wayne dispenser.

Placement of tape on a Gilbarco dispenser.

Phillips 66 Best Practices for Dispenser Security

Inspections

- Become familiar with the inside of your dispensers, take photos for future reference or compare to other dispensers if you find anything that looks abnormal.
- Inspections of all devices inside the store and at the dispensers should be completed while wearing gloves. Devices will be inspected for forensic evidence once they are turned over to law enforcement.
- Open and inspect dispensers at least daily, preferably at the start of each shift, for any sign(s) of tampering or any foreign devices installed, particularly around the card reader. Pull all cables to ensure skimmers are not hidden below sight level (see photos on Page 4).
- The appearance of skimmers is always changing, so be suspicious of anything that looks unusual (see photos on Pages 5-9).
- Nonoperating or faulty operating card readers can be a sign that the dispenser has been tampered with, so inspect dispensers thoroughly if any card reader problems occur.
- If foreign devices are found inside the dispensers, on the external card reader of the dispensers or on top of the pin pad inside the store, **DO NOT TOUCH THE DEVICE**, shut down the pump and call local law enforcement and call the fraud hotline at 888-482-1838.
- A reward program is available through Phillips 66 for sites that recover a skimming device during inspections. See information on Bizlink, under Credit Cards/Fraud Prevention.
- For further information on how to properly inspect pumps, see the video, "How to Inspect Pumps for Skimmers" on Bizlink under Credit Cards/Fraud Prevention.

Locks

- Replace factory-installed locks with high-security locks that require a unique key that is specific to the location (see Phillips 66 recommended locks on Page 10).

Security Tape

- Use serialized security tape on all dispensers. Security tape should be placed over the crind door so the tape will either break or show "void" if the thief attempts to reattach. The use of branded