August 2015

COMBAT SKIMMING

AT THE FUEL DISPENSER

GILBARCO VEEDER-ROOT

GILBARCO VEEDER-ROOT

Combat Skimming.

"Skimming" is the illegal collection of your credit card information. This collection typically occurs at retail sites, and gas pumps are a prime target - primarily due to the unmanned, self-service nature of most sites.

Skimming typically involves the placement of a false or foreign device on or near the credit card terminal, and, with a little ingenuity and lots of scheming, criminals acquire all they need to charge their goods or sell the numbers on the black market. Experts suggest that 37% of all fraudulent transactions in 2014 originated from a counterfeit card, many of these made as a result of skimming.

Skimmers have been a longstanding problem for retailers but as technology improves so do these fraudulent practices. Many times the devices are so small, or so cleverly placed out of sight, that they are imperceptible. It is important to note that both Credit and Debit Cards are susceptible to these fraudulent practices.

HOW DOES IT WORK?

In order to work, the skimming devices need access to the card's magnetic stripe from which they read and retain information from the card's magnetic stripe. It is important to note that most skimmers do not interrupt the transaction to the bank, they merely piggyback on the read of the card.

Criminals have come up with many varieties and forms for skimming, including an card reader overlay, a Bluetooth reader, a camera mounted to the reader, and many more. The customers inserts his/her card into the reader and inadvertently allows the skimmer to capture the information.

Once the data has been collected, the thieves either use the data to create a counterfeit copy of the card or sell the info to someone else. With a counterfeit or cloned card, the user is free to shop at will, and at the expense of your customer who isn't aware until they are either contacted by their financial institution or receive their statement.

WHERE DOES IT HAPPEN?

As stated previously, gas pumps are a primary target for skimming activities but it can happen anywhere. In addition to ATMs, other locations where card skimming is seen frequently include restaurants, taxis or other businesses where an employee physically handles the card to process the charge. In hand-held cases, the thief has fitted the card reader with a skimmer, or uses a hand-held skimmer hidden in a pocket.

CONVENIENCE STORES

In the retail petroleum environment, card skimming devices have been found inside and outside of the gas pump. In each method, criminals use a small electronic device and/or camera to collect card data.

Inside

Internal devices are particularly difficult to detect and can go hidden until a retail employee or maintenance opens the dispenser door. We strongly recommend that each retail site thoroughly inspect each dispenser on a routine and regular basis for signs of tampering or foreign objects.

Splicing

A common internal skimming method is known as "splicing." With this measure, the thief splices a reader into the ribbon cables of the card reader and/or to other critical electronic boards. The device is then deposited inside the dispenser. This device does the same as others; it captures and stores data for future transfer to another device at a later time.

Bluetooth Technology

Using a Bluetooth device the data can be retrieved by driving by or pulling into parking lot and simply pressing a button. The stolen data is then transferred electronically. This is the most common method of moving data from point to point.

Receiver/Transmitter

Data is transmitted to a receiver (typically a wireless device) placed in close proximity to the dispenser, followed by a runner who periodically retrieves/replaces it with another receiver. One retailer discovered a transmitter and antenna device placed inside the dispenser alongside a receiver in a paper bag located in a trash bin adjacent to the pump.

Outside

Outside or external pump devices are typically disguised as part of the dispenser structure and are well-placed. We strongly recommend that each retail site thoroughly inspect each dispenser on a routine and regular basis for signs of tampering or foreign objects.

Card Reader Overlay

A card reader overlay is engineered to duplicate the look of a standard reader as installed by authorized technicians. The overlay sits on top of the authorized reader but can be detected if the employees are vigilant in checking the equipment on a routine basis.

While designed to look like the original, many are produced using 3D printing technology and may not have the exact coloration or design. The use of security tape can help identify tampering of the card readers.

Cameras

In combination with card skimmers thieves also employ camera devices that read and store the Personal Identification Number (PIN) of the card holder. There are many well-documented cases of cameras installed at gas pumps and ATMs.

Keypad Overlays

Other means of capturing PIN data is with keypad overlays on top of the normal card terminal keypads. Devices are positioned such that they capture the data as it is being entered before encryption takes place.

continued...

Active Security Options for Gilbarco Dispensers

1. Secure your pump with the following:

- Encrypted Pulser (Standard Flow Encore)
- Custom door locks
- Unauthorized Door Entry Detection
- Consider adding Secure Card Readers (enhanced encryption technology)
- Upgrade the dispenser CRIND® to FlexPay™II (EMV-compliant)

2. Other steps for consideration.

- Use video surveillance on the forecourt
- Use roamers on large forecourts
- Upgrade lighting on the forecourt for a brighter overall environment

SUMMARY

Skimmers come in many shapes and forms and every retail site is a potential target. These skimmers are engineered to work around Gilbarco Veeder-Root encrypting technology and as a result put customer transactions and information at risk.

EMV, with its new chip and pin security, will greatly reduce counterfeiting and fraud and counterfeiting. However until magnetic stripes have been completely replaced with the new smart chip cards, every retailer must be vigilant in protecting their site, reputation, and customers.

OTHER RESOURCES

NACSOnline We Care Program PCATS Best Practices for Dispenser Security

PCI Convenience Store Employee Data Security Training Manual

8 Low Cost Solutions

1. Monitor your dispensers – look for devices and high bad card reads
2. Create a reference sheet for your cashiers – what to look for and post near the POS
3. Be suspicious of :
   A. Vehicles on the forecourt for a long time
   B. Technicians showing up for unscheduled service work
4. Be alert to any "off-line" message on the POS – investigate
5. Train your personnel to perform daily checks on the forecourt
6. Use security strips on the dispenser doors
7. Inspect locks and panels for tampering daily
8. Utilize a technician for periodic examination for skimming devices inside and outside the dispenser.

NEXT STEPS

1. First and foremost…be sure to follow all policies and procedures as defined by your brand or ownership… if you are not sure if you have any, ask!

2. Don't try to remove or tamper with the device in any way!

3. Do not allow anyone to use the dispenser! Turn off the pump, place an "OUT OF SERVICE" notice on the dispenser, and block the island access to the dispenser.

4. Take pictures of the suspected device. Ensure the images are in focus as the authorities might want to use them as evidence later.

5. Contact local law enforcement.

6. Contact the authority with jurisdiction – usually the local Fire Marshal or the local Weights and Measures office.

7. Run a copy of the receipt for the last transaction on that pump to establish a timeline.

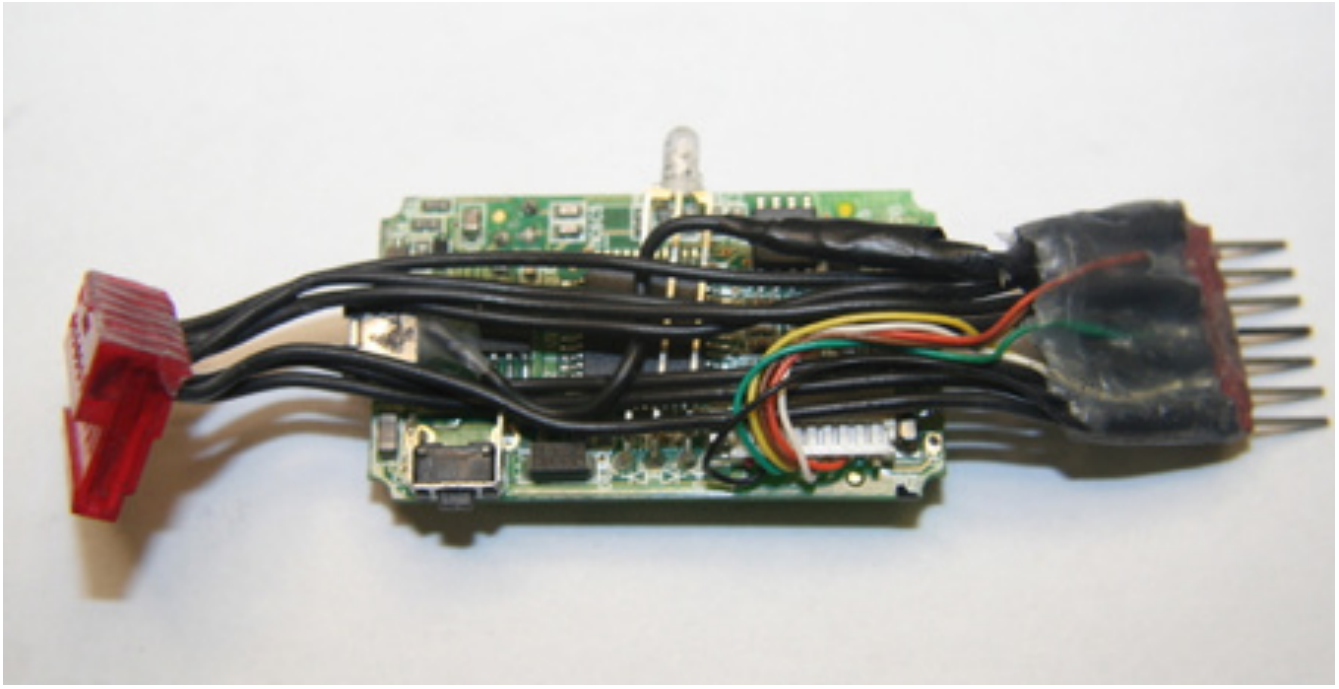
8. Save all video from your security cameras.

9. Interview your store personnel to determine if they have seen any suspicious activity.

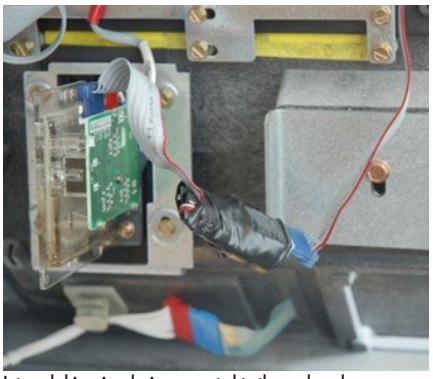
10. Contact your preferred service contractor about past service visits and inquire with the techs to determine if they saw anything suspicious.

11. Consider contacting your local Gilbarco Authorized Service Contractor to inspect for other non-OEM devices that may be installed on other equipment on your sites.

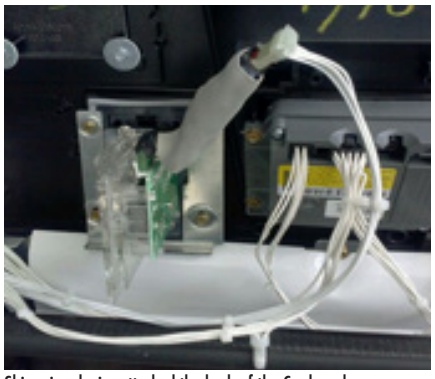
IMAGE GALLERY



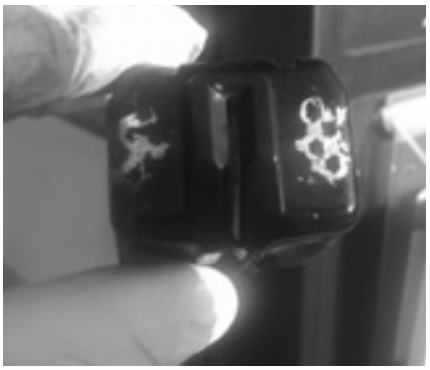
Internal skimming device.



Internal skimming device connected to the card reader.



Skimming device attached the back of the Card reader inside the dispenser.



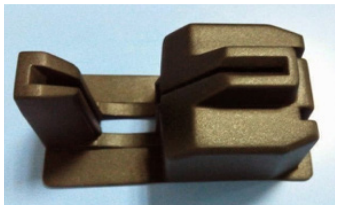
Skimming device is attached to the back of a card reader cover on the outside of dispenser.

Camera located above the keypad below.

Close-up of camera device.

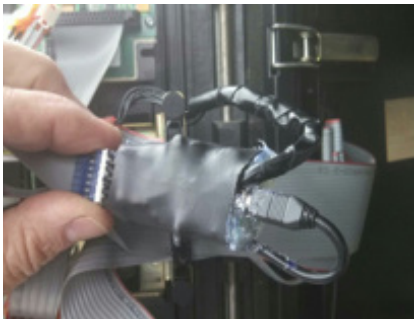
Keypad overlay.

IMAGE GALLERY

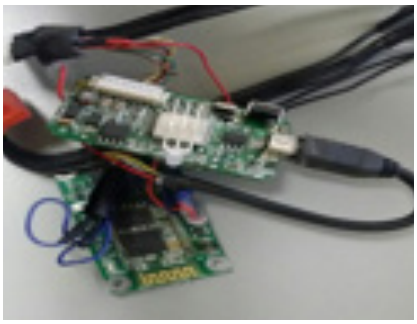


Card reader cover for concealing a skimmer on the outside of a gasoline dispenser card reader

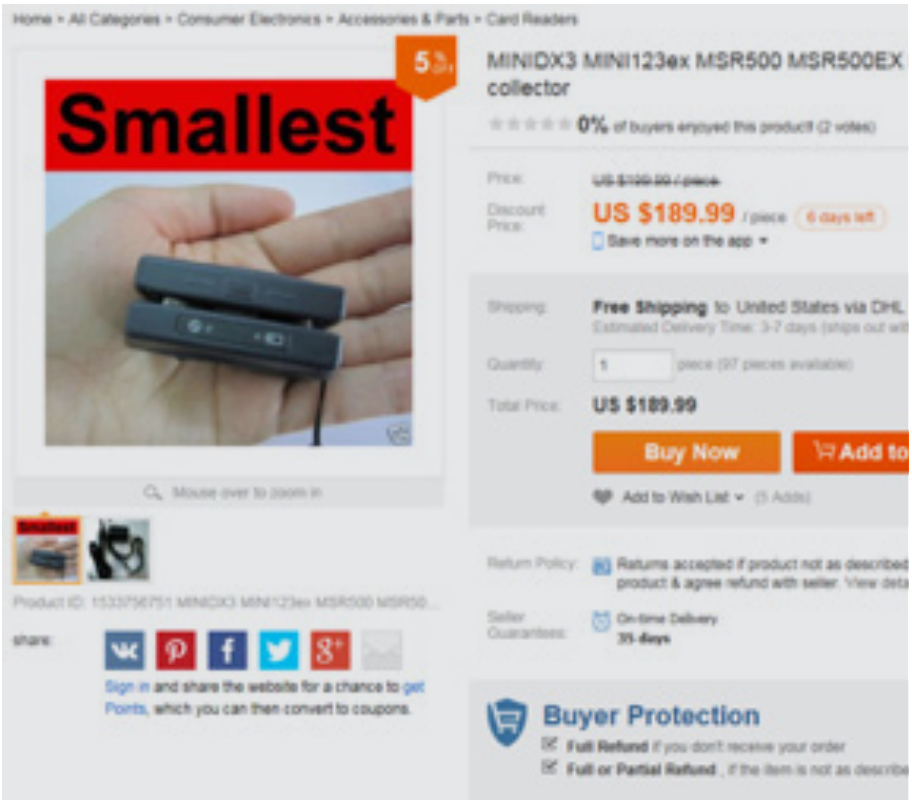
Ultra small skimming device located inside the cover of the card reader.



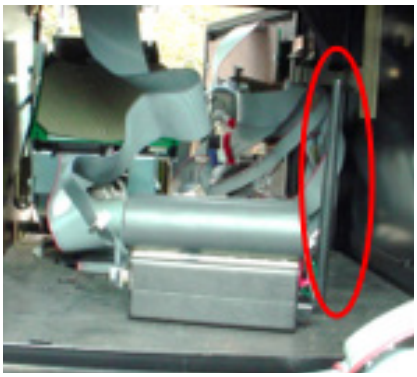
Skimmer spliced into the ribbon cables of the card reader



Skimmer spliced into the ribbon cables of the card reader



Micro SD Card Reader/Skimmer Collector from CHINA. For sale on the internet.



Device is inside the dispenser

Security Tape used to indicate when a dispenser's electronic doors have been opened.

SP-3922 | Combat Skimming | Gilbarco Veeder-Root | 7300 W. Friendly Ave., Greensboro, NC 27410