Quick Reference Guide

Protecting Payment Card Data at Your Dispensers

Prepared by CONEXXUS NACS

Introduction

This guide was developed by the Conexxus Data Security Committee. It is intended to provide informed suggestions to the convenience retailer on how to enhance the payment card security of unattended payment terminals at fuel dispensers. Fuel dispensers can be an attractive target to thieves who are becoming more sophisticated and aggressive when it comes to stealing credit and debit card information.

We encourage retailers to develop their own security plan to help prevent this type of theft and crime. No single solution will completely prevent this criminal activity, but strong security procedures can significantly reduce the opportunity.

Low Cost Steps

✓ Monitor your dispensers for high levels of invalid card read errors or problems accepting cards.

✓ Create - and post by your POS - a reference sheet of what your cashiers should look for, including:

- Be suspicious of vehicles parked on the forecourt for a long time or returning to the same pump repeatedly, especially on outside islands;
- Be suspicious of cars "blocking" the view of a particular pump;
- Be aware of customers using the "tag team" method – one customer will distract the employee while the other party installs the device;
- Be suspicious of any "technicians" performing unscheduled work on dispensers, and check their IDs; and
- Be alert to any unit off-line message at the POS; these are not common under normal operation!

✓ Train your store personnel to perform daily site-level dispenser security checks:

- Use serial-numbered tamper-evident security strips on access panels to aid store personnel in visual inspection and to assist in the detection of tampering at the dispenser. Log all serial number deviations, and disable pumps that have unexplained access security strip deviations until they can be inspected. There are free mobile apps available that you can download on your phone or tablet that will assist in tracking your pump's security seals;
- Perform daily inspection of dispensers to examine locks and panels for tampering (e.g., scratching, cuts, stripping, other damage);
- Test dispenser locks to make sure they can't be turned to unlock the dispenser without the actual key for the lock, such as with a screwdriver or nail file;
- Conduct periodic inspections of the interior of dispenser payment terminals by qualified personnel or service providers for evidence of tampering or skimming. It is helpful to take a picture of the inside of each dispenser when first installed, or when you are confident no foreign device has been installed, to use as a reference point when conducting your inspections;
- Look for small antennas mounted on or near the dispenser;
- Make sure you are inspecting all card readers – **including** NFC card readers; and
- Post pictures of what the inside of the pump looks like (without a skimmer) and what skimmers look like installed to teach store personnel what a skimmer may look like.

✓ Utilize technology when available. There are multiple apps that can detect and report on the Bluetooth signal associated with skimming devices. Note, this solution is only effective for Bluetooth skimmers.

✓ If you have wireless access points near the forecourt, turn on rogue device detection for wireless and Bluetooth. Not all access points support this. But if yours do, it is a low-cost way to detect unexpected devices.

✓ Stay current on security standards, as well as fraud and theft vulnerabilities in the convenience and petroleum retailing industry.

✓ Train your store personnel to ask for identification and confirm scheduled work before any work is done on your POS or dispensers.

✓ Create a forecourt maintenance log. Require technicians to sign-in before any work is performed on forecourt equipment. Also require them to sign-out before leaving the site. Log technician name/badge ID, company name, time-in, time-out, and identify the forecourt equipment where work was performed (e.g., Pump # 2 card reader repaired).

✓ Position your store personnel and POS in a location where there is an unobstructed line of sight to ALL dispensers to aid in observing any suspicious activity on the forecourt.

✓ If possible, during busy times, have an employee be present in your forecourt engaging with the customers.

NACS has serialized access stickers available under the "We Care" Program

If you develop or use other security measures and would like to share that information for incorporation into this document, please email info@conexxus.org.

Quick Reference Guide

Invest in Pump Security

✓ Replace common dispenser payment terminal door locks with ones that are unique to your location.
✓ Upgrade your dispenser's flat membrane keypads to PCI-compliant Encrypting PIN Pads (EPPs) with full-travel numeric keys that make it difficult to add a fake keypad overlay.
✓ Consider upgrading your dispenser's card readers to the latest PCI-compliant secure card readers. Point of Interaction (POI) devices that meet the PCI Pin Transaction Security (PCI PTS) standard provide increased physical protection.
✓ Consider using local and/or point-to-point encryption to protect payment card data after it has been captured. Encryption is not a substitute for card reader inspection, as some types of skimmers can capture card data before it is encrypted.
✓ Consider utilizing and/or offering mobile payments that adhere to the Conexxus Mobile Payment Standard.
✓ Consider installing dispenser access security kits at all sites, but especially for high risk locations (e.g., on or near interstates, high volume sites).
✓ Use video surveillance equipment to discourage unauthorized access to your dispensers – as well as to identify when such unauthorized access happens. Make equipment monitoring obvious and post signs stating monitoring is in use.
✓ Install proper lighting on the forecourt.
✓ Perform a review of your dispensers with your equipment provider to create an acceptable baseline for your location and determine an upgrade strategy that considers both the risks for your location, mandates, and your business needs.

Regulations

✓ Any breach of card data must follow reporting requirements mandated by the specific card brand(s) (e.g., Visa, Mastercard, American Express, Discover, JCB). Contact your acquirer or card brand to confirm notification process.
✓ Many oil brands, distributors, cyber insurance carriers, and other vendors enforce contractual notification requirements for operators. Consult all contracts, agreements, and terms of service to confirm notification requirements.
✓ Check for state and/or local regulations requiring specific security requirements to mitigate data security incidents both inside the store and outside at the fuel island, and any state regulatory requirements for reporting the breach of consumer information, if applicable. Note that state regulatory requirements to report breaches of consumer data may be required based on the residency of the breached consumer, and not the location where the breach of data occurred.

"When in doubt, have a technician check it out!"

Types of Skimmers

Skimming (the placing of a collection device on or within the dispenser, dispenser card reader, dispenser pin pad or other dispenser components to intercept transaction data), allows criminals access to payment card information without the cardholder's knowledge. There are three types of skimmers:

1. *Memory* - card information is stored in internal memory on the skimming device. This device must be removed from the dispenser for criminals to collect/download cardholder information.

2. *Bluetooth* – card information is transmitted in real time to the criminals via a Bluetooth signal. Retrieval of the device is not always necessary with this type of skimmer. However, due to signal strength limitations of Bluetooth, the perpetrator or a relay device must be nearby to acquire the cardholder data.

3. *Cellular* - card information is transmitted in real time via a cellular connection. This type of skimmer can transmit card information via text message or data transmission to criminals anywhere in the world using a SIM card and an integrated cellular antenna.

What to do if you Find a Skimmer

- Immediately shut off and block the pump;
- Notify local authorities, including the nearest local state police and U.S. Secret Service offices;
- Review video footage from the time of the last pump inspection until present; and
- Notify your brand or corporate office (if applicable) or payment processor/ acquirer to ensure all mandated notification requirements are met.

Do not wait until you discover a skimmer to determine how you will respond. It is important to have a detailed incident response plan of action should your location fall victim to a skimming attack.

Only reopen the dispenser once authorities have deemed it clear.