Data Security Briefing

Protecting Payment Card Data at Your Dispensers

Developed by the Conexxus Data Security Committee

The following guide was created with the assistance of Wayne Fueling Systems, Gilbarco Veeder-Root, NACS and concerned Conexxus retail members. This guide is intended to provide informed suggestions to the petroleum retailer on how to enhance the payment card security of unattended payment terminals at fuel dispensers.

Protecting payment card data at your dispensers

Your 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. No single solution will completely prevent attacks, but careful procedures can significantly reduce the opportunity.

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

LOW COST STEPS

- Monitor your dispensers for any high levels of bad card reads 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 — especially on outside islands;
    - 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 access security strips 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;

***NACS has serialized access stickers available**

under the "We Care" Program*

    - Perform daily inspection of dispensers to examine locks and panels for tampering (scratching, cuts); and
    - Conduct periodic inspections of interior of dispenser payment terminal by qualified service provider for evidence of tampering or skimming.
- Stay current on security standards, as well as fraud and theft vulnerabilities in the convenience and petroleum retailing industry.
- Work with your equipment service provider(s) to create acceptable standards for technician visits and identification. Train your store personnel to ask for identification and confirm scheduled work before any work is done on your POS or dispensers.
- 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.

Protecting payment card data at your dispensers

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 adding card readers that provide increased physical protection.
- Consider using local and/or point-to-point encryption to protect payment card magnetic stripe data.
- Consider utilizing and/or offering mobile payments that adhere to the Conexxus Mobile Payment Standard.
- Consider installing dispenser access security kit upgrades for high risk locations (e.g., on interstates, for high volume sites). Check with your manufacturer for a security kit.
- 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

- 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.

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.