Data Security Briefing

Protecting Payment Card Data at Your Dispensers

Developed by the PCATS Data Security Committee

The following guide was created with the cooperation and assistance of Dresser Wayne, Gilbarco Veeder-Root and concerned retailers. 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.

The National Association of Convenience Stores, PCATS, participating vendors and retailers make no warranty, express or implied, nor do they assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process described in these materials.

Ver. 1.0 May, 2010

PCATS Data Security Group and Dispenser Provider Best Practices

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.

LOW COST STEPS

- Monitor your dispensers for any high levels of bad card reads or problems accepting cards.
- Create a reference sheet of what your cashiers should look for and post by your POS, 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
    - Be alert to any unit off-line message at the POS. Investigate the reason for any offline message.
- Train your store personnel to perform daily site-level dispenser security checks:
    - Use access security strips to aid store personnel in visual inspection and to assist in the detection of tampering at the dispenser.
    - Daily inspection of dispensers to examine locks and panels for tampering (scratching, cuts)
    - Periodic inspection 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 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 dispensers to aid in observing any suspicious activity on the forecourt.

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 and encrypt payment card magnetic stripe data.
- Consider installing dispenser access security kit upgrades for high risk locations (interstates, high volume).
- Use video surveillance equipment to discourage unauthorized access to your dispensers. 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.