SITE SECURITY ESSENTIALS

One of the most important tasks for site operators is to help make certain that credit card data is safe and secure. Training your personnel about how to defend your site against thieves looking to install skimmers or steal fuel is imperative!

Stay sharp, stay informed, & stay ahead of the criminals.

1 Protecting Credit Card Data

Credit card breaches can be damaging to any business.

Follow these tips to protect credit card data at your sites:

- Any material containing **cardholder information should be kept in a secure, locked area**. Don't forget printed batch reports!
- Only keep material with cardholder information as long as required for your business or legal purposes – and **always cross-cut shred the material when discarding it**
- **Restrict access** to areas with sensitive cardholder data to authorized personnel only
- Be sure **each employee** with access to Point of Sale, EPS, PIN pads and network equipment **has a unique login ID** and has received training on site security
- Do not allow site personnel to bring a laptop or other electronic equipment to your sites

{NOTE TO SELF}

Remember to change all passwords frequently. If an employee is terminated, revoke their access to secure systems and collect any keys or access cards immediately.

Use the BP Dispenser Security Program!

Install Tubar unique locks & keys from CompX

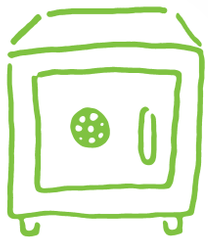
Use security seals on all fuel dispensers

Tamper evident security seals are placed near the credit/debit transaction area and show a "void" message when lifted. This provides a visual alert to store employees during their daily inspection. Stickers clearly indicate that they are to prevent tampering so consumers are confident their credit card data is secure.

For more information about the program:

Log into bpconnection.com and go to Programs>PCI Compliance & Card Security>BP Dispenser Security Program.

2 Safeguarding Payment Card Acceptance Devices



PCI Standard 3.1 requires sites to protect payment card acceptance devices from tampering and substitution.

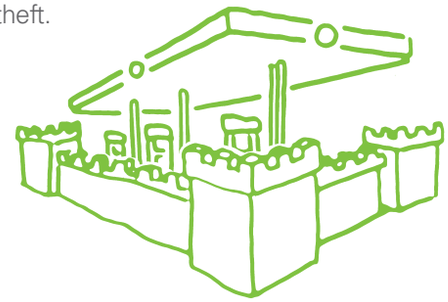
Sure, PCI compliance is a requirement. But it helps protect your sites, too.

Each site is required to:

- Maintain a list of equipment with serial numbers
- **Inspect equipment regularly**, especially PIN pads, to prevent substitution and ensure no unauthorized payment processing equipment has been connected
- Train personnel to **be aware of and report suspicious behavior, equipment tampering, or device replacement**
- **Keep a technician log** – verify identity and require sign in and sign out when technicians work on your payment processing equipment
- Ensure that any third party POS applications are Payment Application Data Security Standard (PA-DSS) approved
- **Install anti-virus and security patches** on your POS and back office applications

3 Defending the Forecourt

Site employee diligence is your best weapon against skimming and fuel theft.



Keep these suggestions in mind:

- Constantly **monitor fuel dispenser activity**, especially at dispensers that are hardest to see from inside the store
- Look for a high incidence of **bad card reads** or problems accepting cards at a specific fueling position/dispenser
- **Be aware of "dispenser offline"** messages displayed on the POS. This could mean the dispenser is disabled to install a skimmer or steal fuel
- Be suspicious of vehicles parked on the forecourt for extended periods of time or blocking the view of some dispensers
- Be alert for anyone posing as a technician that tries to perform unauthorized work on dispensers
- Inspect dispensers regularly for any evidence of tampering – **use the inspection checklist** available from BP Parts
- **Keep an eye out for skimming devices** attached to indoor or outdoor payment terminals. Refer to Section 1 of the BP Payment Guide to find out what to do in the event your site experiences a security breach such as finding a skimming device

PREVENTING FUEL THEFT

Some dispensers allow anyone with a remote, wired or wireless, to put the dispenser in "stand-by" mode to freely dispense fuel.

For Wayne Ovation dispensers, remove the remote activating jumper to prevent remote access to the dispenser controls.

Be aware of any complaints of a strong smell of gasoline on the forecourt.

Employees should never confront a thief!

Contact local law enforcement any time suspicious activity is observed.

Experiencing problems? Have questions? Need help?

Call 1-888-BP-HELP-U (1-888-274-3578)

Log into bpconnection.com and go to

Programs>PCI Compliance & Card Security>BP Dispenser Security Program

This information was developed in conjunction with the Technology Committee of the BPAMA.