PCI Compliance

"If you are a merchant that accepts payment cards, you are required to be compliant with the Payment Card Industry Data Security Standard ('PCI DSS')."

Source: www.pcisecuritystandards.org

PCI Compliance consists of 12 steps: *(Click **here** for the Merchant PCI Compliance Quick Reference Guide)*

To comply with these 12- steps of PCI Compliance requirements, there are a few PCI items you should address immediately:

1. **Install and maintain a PCI-compliant managed firewall service**

   Due Date:

   Verifone POS: Installation of Commander/RubyCi POS

   Other POS: Installation of EMV software

   a. CITGO requires use of CITGO Authorized Firewall Managed Service Providers (see list below)

   b. **Firewall requirements**

   CITGO AUTHORIZED FIREWALL MANAGED SERVICE PROVIDERS

2. **Inspect, track and document all terminals and PINPads monthly** to help ensure no tampering or unknown replacements have taken place.

   a. PCI DSS Compliance requirement #9: **www.pcisecuritystandards.org**.

   b. Use this **form** to track and document monthly.

c. Form must be provided to CITGO within 5 (five) business days upon request.

d. Failure to comply could result in a data breach and fines from the Card Brands.

3. **Track and document anti-virus software** on all POS and peripheral equipment such as Point Of Sale and back-office computer.
    a. PCI DSS Compliance requirement #5: **www.pcisecuritystandards.org**.
    b. Use this **form** to track and document monthly.

4. **Change default passwords**
    a. PCI DSS Compliance requirement #5: **www.pcisecuritystandards.org**.
    b. Use complex passwords consisting of upper- and lower-case letters, numbers and special characters (e.g., !, *, @, $ and %)
    c. Change passwords often

Marketers are ultimately responsible for PCI DSS compliance.

Click here for CITGO-required roles and responsibilities. Service providers can sometimes assist with PCI DSS responsibilities.

Ask your service providers for their roles and responsibilities.

Need Help Getting Started?

The ControlScan PCI DSS 1-2-3 Program can help automate the process. It provides:

- An intuitive **Self-Assessment Questionniare** (SAQ)
- **Quarterly External Vulnerability Scans**
- **Unlimited access to a compliance support team** for PCI questions
- **Affordable Security Consulting Services** when needed

Click HERE for more details, then visit www.controlscan.com/petropci to get started.

Payment Card Industry Data Security Standards (PCI DSS) Updates

Source: PCI Security Standards Council, www.pcisecuritystandards.org

According to recent forensic investigations, small merchants remain targets of hackers who are attempting to compromise payment data. As part of an effort to secure the payment system and mitigate the risk of small merchant compromises, Visa is establishing requirements for U.S. and Canada acquirers to ensure that their small merchants take steps to secure their point-of-sale (POS) environment.

Visa Payment Security Compliance Validation Program Requirements for Level 4 Merchants

Using QIR companies provides small merchants some protection against a common vulnerability exploited by criminals. However, this alone will not prevent small merchant compromises. As such, Visa is expanding its PCI DSS validation program to include Level 4 merchants. Effective 31 January 2017, acquirers must ensure their Level 4 merchants validate full PCI DSS compliance annually.

1: Level 4 merchants include owner-operated locations of franchise or corporate organizations. Franchisors or corporate organizations must continue to validate as a merchant or service provider based on their designation and/or level.

Merchants Must Use Qualified Integrators and Reseller (QIR) Professionals

Effective 31 January 2017, acquirers must ensure that all existing Level 4 merchants use PCI-certified QIR professionals from the QIR Companies list at the PCI Security Standards Council (PCI SSC) website for POS application and terminal installation and integration.

PCI Compliance Reference Guides from www.pcisecuritystandards.org

- **File Uploads:**
  - PCI SSC - Getting Started with PCI DSS (.pdf)
  - PCI DSS v3.2 (.pdf)
  - Self-Assessment Questionnaire – C version 3.2 (.doc)
- **More files and information available at www.pcisecuritystandards.org**

Payment Card Industry Resources

- PCI Security Standards Council
- PCI Payment Protection Resources for Small Merchants
- U.S. Chamber of Commerce Internet Security Essentials for Business 2.0

Security Resources

- Connexxus WeCare Program
- Skimming Prevention: Best Practices for Merchants v.2.0

Breaches and Attacks Resources

- Security Blog
- Verizon Data Breach Investigation Report
- Trustwave Global Security Report
- World's Biggest Data Breaches