What is PCI Compliance?

Dated: February 9, 2009

The PCI Security Standards Council (SSC) has formed global requirements to protect cardholder data, an issue which is complex and ever evolving. The PCI Data Security Standard (DSS) details security requirements for members, merchants, and service providers that store, process, or transmit cardholder data. The Credit Card Industry has established these policies and procedures in an effort to secure transactions and protect this cardholder data. PCI is critical in protecting consumers from identity theft.

The latest version of PCI DSS (Version 1.2) consists of common sense steps that mirror best security practices. The PCI SSC has declared twelve requirements grouped into six objectives. These requirements are applicable if a primary account number is stored, processed, or transmitted. A copy of these requirements may be obtained by accessing the following website: www.pcisecuritystandards.org. Or, you may contact me directly.

Compliance is a continuous process and there are three ongoing steps to adhering to the PCI DSS that must be followed:

1. First, ***assess*** – identify cardholder data, taking an inventory of your IT assets and business processes for payment card processing, and analyze them for vulnerabilities that could expose the cardholder data;
2. Secondly, ***remediate*** – fix any vulnerable systems that could expose cardholder data. Do not store cardholder data unless needed;
3. And lastly, ***report*** – compile and submit required records.

As a marketer, it is *your responsibility* to comply with PCI DSS. As of this past **October 10, 2008**, all level 3 and level 4 merchants must comply with PCI DSS or use Payment Application Best Practices (PABP)-compliant applications. It is imperative that all of your software is up-to-date in order to help with this compliance process. Please contact your current processor to confirm that you are using the latest versions of software available. Starting **January 1, 2009**, all newly-installed fuel dispensers that accept debit cards must have PCI-compliant encrypted pin pads and dispenser manufacturers must incorporate key pads capable of compliance with the Triple Data Encryption Standard (TDES). All vulnerable payment applications will be de-certified by **October 10, 2009**. **June 30, 2010**, marks the deadline which requires all fuel dispensers to be capable of encrypting PINs in the TDES. The final deadline is **July 1, 2010**. By this time, dispensers that process debit transactions must comply with PCI encrypted pin pad (EPP) standards; all attended point-of-sale (POS) payment terminals with PIN entry devices (PEDs) must be certified as PCI-compliant; TDES will be required for all debit transactions; and VisaNet Processors (VNPs), agents, and merchants must use only PABP-compliant applications.

Merchant Level	Description
Level 1	More than 6 million transactions per year.
Level 2	Between 1 and 6 million transactions per year.
Level 3	Between 20,000 and 1 million transactions per year.
Level 4	Less than 20,000 transactions per year.

Here are some helpful recommendations gathered from several different sources to assist in the compliance process:

- Install and maintain a computer firewall to protect cardholder data. Marketers are responsible for networks at their own back office locations.
- Stop using vendor-supplied defaults for passwords. This is applicable for routers, firewalls, network switches or bridges, and any computer where card data is stored or passes through.
- Segment your network and protect every segment that stores, processes, or transmits data.
- Protect stored data. As a marketer, you should only be storing that portion of the customer's account information needed for your business purposes. This is to include the name and account number or expiration date. This information should be locked in a secure area and access should be given to only authorized personnel. Materials to safeguard are receipts, manual tickets, journal tapes, batch reports and back-up disks, or other electronic media. This material should be kept for a minimum of 6 months and a maximum of 9 months. At this point, the information should be shredded.
    - Batch reports may still be printed. This will not put you as a marketer in non-compliance. Marketers should print out the information and reconcile it daily with POS credit totals. This is the only way to catch any problems and ensure reimbursement for missing batches or transactions.
    - While these reports contain sensitive data, you will not be in violation if the data is stored and disposed of properly.
- No system should store card security codes or debit PINs for any longer than it takes to complete a current transaction.
- Encrypt transmission of cardholder data across open, public networks.
- Use and regularly update anti-virus software.
- Limit access to POS terminals to authorized employees only. Each employee should have their own, unique computer identification.
    - Do not allow employees to bring laptop computers or other electronic equipment to your site.
    - Do not connect or disconnect any equipment to either the network switch or the satellite inside unit or modem.
    - The PCI Council must certify any third-party hardware or software. A certified technician must perform the installation work.
- Track and monitor all access to network resources and cardholder data.
- Maintain a policy that addresses information security. A yearly "self-assessment" form must be completed to ensure compliance. (A copy of the Self-Assessment Questionnaire (SAQ) may also be found on the PCI Security Standards website.)

Fuel retailers in general face more security challenges than their counterparts. That being said, it is vital to educate your store employees and managers; perform walk around checks during store startup and shift changes; do not block the clerk's view of the pumping stations; use security cameras both inside and outside the store; and restrict service access to pumps during routine maintenance. Please remember that compliance is not a one-time event – it is an ongoing state which must be validated yearly. **The financial penalties for a non-compliance breach are real.**