

Branded Stores and PCI Compliance Who is Responsible?

May 18, 2009

2:30 p.m. – 3:30 p.m.

Disclaimer

The opinions of the contributors expressed herein do not necessarily state or reflect those of the National Association of Convenience Stores. Reference herein to any specific commercial products, process, or service by trade name, trademark manufacturer, or otherwise, shall not constitute or imply an endorsement, recommendation, or support by the National Association of Convenience Stores. The National Association of Convenience Stores makes no warranty, express or implied, nor does it assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process described in these materials.

Presenter:



Jim Huguelet
W. Capra Consulting Group
Payment Architect

Retail Representatives:



Kelly Mahoney



Hubert Williams



Charlotte Loomiller



Carolyn Allen



Kenneth Morse

Clearly Understanding PCI Roles

There are five key roles related to PCI that are often confused, leading to confusion about PCI as a whole

- Setting PCI Standards
- **Implementing PCI Standards**
- Validating Implementations of PCI Standards
- Approving Assessors to Validate Implementations of PCI Standards
- Enforcing PCI Standards



This is the Focus of
Today's Session

Who Owns PCI at My Branded Sites?

- Acquirers are contractually obligated to payment brands for PCI Compliance of their merchants/agents
- Acquirers pass this responsibility down the contractual chain, and this is where things get tricky
- PCI Implementation responsibility is clearest in industries with company-owned and operated retail sites
 - Petro/C-Store's channels of trade often involve Jobbers (perhaps multiple levels) & Dealers (often multiple types), ownership versus operation of sites, and other subtleties that blur this tremendously
 - Difficult to provide general direction
- Opinions Vary:
 - One Jobber: "I just provide fuel; I'm simply another vendor to sites"
 - One Site Operator: "My MOC is fully responsible for PCI"
 - One MOC: "Site owners are ultimately responsible for the PCI of their sites"

Who Owns PCI at My Branded Sites?

- Ownership of compliance is almost always shared between brands & marketers
- The key activity for answering this question: **Conduct a Contractual Analysis for Each Component of Your Sites' Payment Solutions** across:
 - Each brand
 - Each channel of trade
 - Both up and down the value chain
- It is critical for everyone (Brands, Jobbers, Dealers, Owners, and Operators) to get absolute clarity and agreement on who owns what aspects of implementing PCI at each site (which might vary by brands, jobbers, dealers, owners, and operators) and what “Points of Demarcation” exist
- A contractual analysis is a challenging, detailed, but ultimately necessary activity
 - Not all contracts are likely same version
 - Many contracts do not have explicit language on PCI responsibilities
 - May need to examine contracts for language on
 - Program Participation
 - Adhering to Legal, Contractual, or Industry Requirements

Key Areas of Site Payment Solutions

- POS System
 - POS Software & Hardware
 - BOS Software & Hardware
 - Payment Switch Software & Hardware
- Telecommunications
- Site LAN
 - Firewall
 - IDP
- Dispensers & Outdoor Payment Terminals
- Indoor PINPads
- Store Operations
 - Receipt/Report Storage
- PCI Services
 - User ID & Access Control (Remote and On-Site)
 - File Integrity Monitoring
 - Remote Access (for Help Desk)
 - Log Monitoring
 - POS/BOS Application Updates
 - POS/BOS O/S Updates (Including Security Patches)

How to Handle Gray Areas

If a contractual analysis does not yield clear answers in a particular area, consider the following key questions to help guide determining responsibility for each area of a particular site payment solution:

- Does the site own it, lease it, or get it?
- Does the site maintain or update it?
- Does the site directly contract for it?
- Does the site directly pay for it?
- Does the site have a choice to use it?

Practical Advice to Site Owners

- Consider having a face to face meeting with all involved parties (both up and down the value chain) to discuss all components in your site payment solution(s)
- If you're the site owner (i.e., you pay taxes on the site's sales) and/or have your own merchant ID with the acquirer, you should act as if you are fully accountable for PCI compliance for all areas of your site payment solutions until you can contractually determine otherwise
- In all future contracts you enter into, include / require explicit language on PCI responsibilities to eliminate gray areas

Questions?

Kelly Mahoney

BP

kelly.mahoney@bp.com



Hubert Williams

Sunoco, Inc.

hcwilliams@sunoco.com

Charlotte Loomiller

Citgo Petroleum Corporation

cloomil@citgo.com

Carolyn Allen

Valero Energy Corporation

carolyn.allen@valero.com

Kenneth Morse

Chevron Corporation

kenneth.morse@chevron.com

Jim Huguelet

W. Capra Consulting Group

jhuguelet@wcapra.com

Thank you!