

## PCI & Credit Card Security: Background

Restaurant owners and their customers have enjoyed the convenience of accepting and using credit and debit cards for many years. However, given the skyrocketing cost and frequency of credit fraud, the major card brands (Visa, MasterCard, American Express, Discover and JCB) have taken steps to protect all stakeholders.

The mag stripe on credit cards was invented by IBM in 1968 and became the industry standard. Given that the track data on the mag stripe is easy to read and duplicate, the card brands, through the Payment Card Industry Security Standards Council, has built a set of standards to secure cardholder data, beginning with the directive: **'Don't store track data.'**

## PCI Standards

The PCI Security Standards Council has taken a three-pronged approach to protecting consumers, banks and merchants/restaurateurs:

1. **PCI DSS (Payment Card Industry Data Security Standard)** - covers all **entities** that store, process, or transmit cardholder data (Merchants, restaurateurs, service providers, processors, etc.)

**Deadline for Compliance:** January 2007 (deadlines are long passed)

**What this Means** – All restaurateurs (regardless of size) must complete and submit a PCI Self-Assessment Questionnaire annually to their Acquiring Bank.

2. **PA-DSS (Payment Application Data Security Standard)** - covers all **applications** used to store, process, or transmit cardholder data as part of authorization or settlement. (Point-of-Sales (POS) application developers)

**Deadlines for Compliance:**

**Oct. 1, 2008** - Payment processors, agents and merchants must use software that is compliant with the new payment application security standards.

**Oct. 1, 2009** - All merchants will be required to start terminating the use of any noncompliant payment applications that they might still have in their environments.

**July 1, 2010** - Mandates the use of only those payment applications that support the new standards.

**What this Means** – If, after the deadline, a merchant/restaurateur is not running a PA DSS-validated application, they will automatically fail their PCI assessment and could lose their ability to accept credit cards.

3. **Pin Entry Devices (PED) Standard** – covers all **PEDs** and is aimed at ensuring that the cardholder's PIN, and any sensitive information such as resident keys, are protected consistently at a PIN acceptance device.

***Deadline for Compliance:***

**Jan. 1, 2004** - All newly purchased Point-of-Sale (POS) PIN Entry Devices must have passed testing by a Visa recognized laboratory and been approved by Visa..

**July 1, 2010** - Mandates that all deployed POS PEDs must have passed testing by a PCI recognized laboratory and been approved by the PCI SSC.

**What this Means** - Merchants/restaurateurs have 2 years to replace older, un-approved PEDs.

## PCI Dos

- Do routine vulnerability scans of your systems.
- Do security awareness training for all of your staff.
- Do audits of system access.
- Do monitor your system activity logs.
- Do remove access privileges of separated employees.
- Do install software patches.
- Do take any threats seriously - have an incident response plan in place.

## PCI Don'ts

- Don't store or archive whole credit card numbers.
- Don't transmit credit card information unencrypted.

PCI is not simply about proving you are compliant with the standards – it's about protecting your customers and your business.

## How PCI Affects Restaurateurs

Given consumers' expectation of ubiquitous acceptance of credit and debit cards, a restaurateur's validation that they are protecting their customer's personal information is good for business:

**Reputation / Image** – in a competitive business – an operator does not want to be named in the media as the place where card data was stolen

**Protects Ability to Accept Credit / Debit Card Payments** - non-compliance and/or a breach can jeopardize a restaurateur's ability to accept credit/debit payments. In many cases, credit/debit payments account for 80% to 90% of transactions. Losing the ability to accept credit cards = reduced traffic/customers.

## Impact of State Privacy Laws

A breach that discloses personal credit card information in one of the 40+ States with privacy laws may have a double impact on a restaurateur. Being off-side with PCI may result in fines and litigation costs. Being off-side with State Privacy Laws is a felony with potentially more serious consequences.

## Compliance / Security Strategy

1. Ensure you are using a PA-DSS or PABP validated POS system
2. Ensure you are using an approved PED
3. Have regular security awareness training for your staff - particularly supervisors
4. Do background checks on anyone with administrative access to your system
5. Have staff sign a 'Confidentiality Agreement'
6. Carefully and accurately complete the PCI Self Assessment Questionnaire (SAQ) – if you are not sure – ask
7. If gaps in PCI compliance are identified, develop a realistic plan to remediate them
8. Maintain mature controls to sustain compliance
  - Access controls
    - Dual factor for system and device management
    - Strong passwords and secure PW storage
  - Monitoring to detect attack and record evidence
  - Control wireless access points
  - Maintain secure configuration
  - Segment networks
9. Maintain an Incident Response Plan and Test It
10. Test and audit the cardholder environment like your business depended on it

This can be a daunting task the first go around but when the above are in place, ongoing PCI compliance is not an expensive undertaking. It is good business practice to protect the sensitive information that your customers entrust with you.

## Questions?

Jim Fish is Vice-President, Partnerships and Channels for Coalfire Systems, Inc. Coalfire is a Colorado based IT Governance and Compliance consultancy with offices in California, Washington, New York and Canada. If you have questions, contact Jim by email at [jim.fish@coalfiresystems.com](mailto:jim.fish@coalfiresystems.com); or by calling 206-352-6029, ext. 7501.