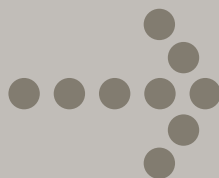




# PCI Data Security Standards Quick Reference Guide



# Table of Contents



- 1 The History of PCI
- 2 Overview of PCI Standards
- 3 Merchant Levels
- 4 BP's Role
- 5 BP Branded Marketer's Role
- 6 Your PCI Checklist
- 7 Consequences to Consider
- 8 PCI Information Resources



# PCI Data Security Standards Quick Reference Guide

Payment Card Industry (PCI) Data Security Standards are real and have been mandated to protect you, your business, and your customers. We have developed this Quick Reference Guide as a tool to help you understand these standards and how they will affect your business.

## 1 The History of PCI

The **Payment Card Industry Security Standards Council** ("the Council") was founded by Discover, JCB, MasterCard, American Express, and Visa. Effective September 7, 2006, this Council now owns and maintains the Payment Card Industry Data Security Standards ("PCI DSS"). PCI evolved from mounting card issuer concerns over the growing frequency of payment card compromises at merchant locations.

## 2 Overview of PCI Standards

**PCI DSS** is a set of clearly defined standards setting forth a merchant's duties to secure sensitive cardholder data. The Standards apply to all entities that store, process or transmit cardholder data, including the entire cardholder's account number, expiration date, cardholder name, and the service code describing whether a sale was made inside/outside. PCI DSS generally:

- Set standards for handling card transaction data
- Govern the encryption standards for the Personal Identification Number (PIN) for debit transactions

These goals of PCI DSS, and requirements to meet these goals are:

### Goal #1 – Build and Maintain a Secure Network

*Requirement 1:* Install and maintain a firewall configuration to protect cardholder data

*Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters

### Goal #2 – Protect Cardholder Data

*Requirement 3:* Protect stored cardholder data

*Requirement 4:* Encrypt transmission of cardholder data across open, public networks

### Goal #3 – Maintain a Vulnerability Management Program

*Requirement 5:* Use and regularly update anti-virus software

*Requirement 6:* Develop and maintain secure systems and applications

### Goal #4 – Implement Strong Access Control Measures

*Requirement 7:* Restrict access to cardholder data by business need-to-know

*Requirement 8:* Assign a unique ID to each person with computer access

*Requirement 9:* Restrict physical access to cardholder data

### Goal #5 – Regularly Monitor and Test Networks

*Requirement 10:* Track and monitor all access to network resources and cardholder data

*Requirement 11:* Regularly test security systems and processes

### Goal #6 – Maintain an Information Security Policy

*Requirement 12:* Maintain a policy that addresses information security

## 3 Merchant Levels

**PCI DSS became an official standard in September 2006.** Your merchant level, which is based on your annual Visa *or* MasterCard transaction levels, determines your PCI requirements when you are required to validate your compliance with PCI DSS.

BP is a Level 1 merchant. Most BP branded marketers are Level 4 merchants. You can confirm your Merchant Level by confirming your annual Visa *or* MasterCard transaction levels.

(See chart next page)

Merchant Level	Description
1	Any merchant, regardless of acceptance channel, processing over 6,000,000 Visa <i>or</i> MasterCard transactions per year.  Any merchant that Visa <i>or</i> MasterCard, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa <i>or</i> MasterCard system.
2	Any merchant, regardless of acceptance channel, processing 1,000,000 to 6,000,000 Visa <i>or</i> MasterCard transactions per year.
3	Any merchant processing 20,000 to 1,000,000 Visa <i>or</i> MasterCard e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 Visa <i>or</i> MasterCard e-commerce transactions per year, and all other merchants, regardless of acceptance channel, processing up to 1,000,000 Visa <i>or</i> MasterCard transactions per year.

## 4 BP's Role

BP is required to validate compliance on the PIN pads, EPS (V900 CommLinx device), and everything that flows through our back office systems out through the network provider (Hughes) and the payment processor First Data. In addition, BP continues to work with hardware vendors to ensure that branded marketers have many choices for compliant hardware at their locations. BP is also a Participating Organization in the PCI Security Standards Council and uses that platform to speak on behalf of ourselves and our customers.

## 5 BP Branded Marketer's Role

It is your responsibility to comply with the PCI DSS. The PCI DSS will affect your location in the following ways: hardware, site operations, company back office and compliance validation.

### What do I need to do to prepare my sites to become PCI Compliant?

- Train and re-train your site staff on the importance of protecting and properly destroying paper documents that may contain sensitive cardholder data (reports, receipts, journal tapes, etc.). Refer to section 12.0 in the BP Payment Guide for more information.
- Restrict access to any systems that may contain sensitive data (i.e., back office systems, accounting systems, etc.).
- Ensure all systems that may contain sensitive cardholder data are encrypted. Confirm with your POS vendor that your POS device is PABP/PADSS certified.
- Encrypt sensitive cardholder data during transmission on public/open networks (i.e. from site to headquarters). Data transmitted via the point-of-sale to BP's host (Paypoint) is currently encrypting properly.
- Provide validation of your company's compliance status annually via a self-assessment questionnaire.
- **For Wide Area Network Option A (Connecting into branded marketer's WAN) Customers Only:** You are responsible for ensuring that your network is PCI Compliant. In addition, you must perform a quarterly scan on your network via a certified scanning vendor and complete a self-assessment questionnaire.

### What are the key dates for PCI Compliance?

- **1/1/2008** – Any new INSIDE PIN pads purchased as of 1/1/2008 must be Triple Data Encryption Standard (TDES) capable and PCI PED certified.
- **1/1/2009** – Starting 1/1/2009 all new dispenser installs must have PIN pads that are TDES capable and PCI Encrypted PIN pad (EPP) certified.
- **7/1/2010** – All POS devices must be certified as Payment Applications Best Practice (PABP) or, once the new standard is in place, as Payment Application Data Security Standard (PADSS) by 7/1/2010.
- **7/1/2010** – All existing INSIDE PIN pads must be using TDES by 7/1/2010.
- **7/1/2010** – All existing dispenser PIN pads must be using TDES and EPP by 7/1/2010\*.

\*A TDES upgrade is only required at the dispenser PIN pad for sites accepting debit at the pump.

## 6 Your PCI Checklist

Use the following checklist to help you prepare for PCI compliance over the next two years.

### Suggested 2008 Activities:

- Register with Trustwave or another certified QSA.
- Begin educating yourself and your employees.
- Create a budget for 2009 activities.

### Suggested 2009 Activities:

- Register with Trustwave or another certified QSA.
- Become educated about PCI. There are many free webinar events and workshops on the topic. BP will post them on [bpconnection.com](http://bpconnection.com) for your convenience.
- Determine if you will complete the self assessment form yourself (available at [pcisecuritystandards.com](http://pcisecuritystandards.com)) or if you will pay a nominal fee and hire an auditing company to help you through the process.
- Identify where key investment will be required – hardware, operations, etc.
  - If you want to continue to accept debit at your dispensers, contact your hardware vendor for cost information. Upgrades are due by 7/1/2010.
- Complete the Self Assessment Questionnaire by 12/2009.
  - Identify any gaps to remediate.
- Begin remediation work.

### Suggested 2010 Activities:

- Continue PCI education/awareness.
  - Dates may change so make sure you're ahead of the curve!
- Begin remediation work.
- Complete any remediation activities required from 2009 assessment.
  - Keep the deadlines for hardware upgrades in mind!
- Complete the Self Assessment Questionnaire by 12/2010.
  - Identify any gaps and begin remediation.
- Validate yourself as PCI DSS compliant.

## 7 Consequences to Consider

Compliance is not a one time event - it's an ongoing state that you must validate once a year.

**The financial penalties for a compliance breach are real.** It is estimated that for every card stolen, it will cost your business \$202\*. For the average site with 6,000 card transactions a month, that could result in up to \$1.2m for just one month's worth of data!

Protecting the BP brand is one of the reasons we all participate in BPAMA - we believe in the value of the BP brand. The type of press coverage a breach would receive, whether at a BP corporate level or because of a single branded marketer breach, would be damaging to the investment we've all made in the BP brand.

\*According to Ponemon Institute

## 8 PCI Information Resources

### PCI & Standards

[www.visa.com/cisp](http://www.visa.com/cisp)

[www.visa.com/pin](http://www.visa.com/pin)

[www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

### Card Brand Websites

[www.visa.com/cisp](http://www.visa.com/cisp)

[www.mastercard.com/sdp](http://www.mastercard.com/sdp)

[www.discovernetwork.com/resources/data/data\\_security.html](http://www.discovernetwork.com/resources/data/data_security.html)

### Other Sources

[www.pcianswers.com](http://www.pcianswers.com)

[www.askaboutpci.com](http://www.askaboutpci.com)

[www.bpconnection.com](http://www.bpconnection.com)

