

10 Common PCI Myths



1. I'm a small operator, who only takes a handful of cards, so I don't need to comply with PCI.

A common misunderstanding is that small merchants, handling as few as 10 credit card transaction a day are exempt from compliance with the PCI Data Security Standard (PCI DSS). If you are a merchant and you accept credit card payments - then you must comply with PCI.

2. PCI only applies to E-commerce companies

PCI applies to every company that stores, processes or transmits cardholder information. In fact anyone who takes card present transactions that involve POS devices are more at risk than E-Commerce solutions. Quite often these types of transactions involve storage of track data (which is forbidden under PCI). Disclosure of this type of data will bring heavy fines and requests for compensation from the banks involved.

3. You only have to be compliant with the majority of criteria

The pass mark for PCI is 100%, so if you fail even one of the criteria, you fail PCI. Meeting all PCI standards is not a one time event; it is a starting point for an ongoing security program. Failing to achieve even one of the requirements, is failing to meet the standard for protecting cardholder information.

4. I only need to protect my credit card data, not ATM debit card related data

Unfortunately, both are required. Many debit cards are dual-purpose "signature debit," which can be used on debit and credit card networks. As such, they are covered under PCI and must be protected in the same way as credit cards.

5. I can wait until my business grows

Unfortunately, the PCI standard applies to all sizes of business and waiting could be costly. Should you be compromised and not be compliant, the fines and the compensation could be substantial.

6. I can just answer "yes" to all the criteria on the self-assessment

The self-assessment is merely a mechanism for getting the information about the level of your compliance to your merchant bank or the Card Brands. The standard applies at all times. Just saying yes to the questions puts you, the merchant, at great risk. If compromised and it is discovered that you were never actually compliant, the matter would be taken very seriously by the Card Brands and your Acquiring Bank.

10 Common PCI Myths



7. As a merchant I'm not liable if a credit card is compromised

Merchants can be liable not only for the compromise but also for subsequent damages from the issuing banks.

8. I can wait until my bank asks me to be compliant

The dates for Merchants demonstrating compliance are long gone, and the Merchant is responsible for making sure they are in compliance. Waiting until the bank asks you could be very costly.

9. As a Merchant, I did not sign anything, saying I would be compliant; therefore, I do not need to be.

The PCI standard is part of the operating regulations under which Merchants are allowed to maintain merchant accounts. The regulations signed when the Merchant opens an account at the bank state that the card brand's regulations have to be adhered to. Even if you have been in business for decades, PCI still applies, if you store, process or transmit credit card information.

10. As a Merchant, I'm entitled to store any data

Many Merchants believe that they own the customer and have a right to store all the data about that customer in order to help their business. Not only is this incorrect regarding PCI, it may also be a violation of State and Federal legislation regarding privacy. The PCI regulations specifically forbid storing of any of the following:

- Unencrypted credit card number
- CVV or CVV2
- Pin blocks
- PIN numbers
- Track 1 or 2 data

Any of the above found in databases, log files, audit trails, backups etc. can result in serious consequences for the Merchant, especially if a compromise has taken place.

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. Contact Jim with questions by email at jim.fish@coalfiresystems.com; or by calling 206-352-6029, ext. 7501.