



PSC

Payment and Security Experts

10 Myths About PCI Compliance

10 Myths about PCI Compliance

1. I'm a small merchant, who only takes a handful of cards, so I don't need PCI

A common misunderstanding with the standard is that small merchants, handling a few 10's of credit cards a day are exempt from compliance. If you are a merchant and you are set up to take credit cards, by any mechanism - then you need to be compliant.

2. PCI only applies to E-commerce companies

No, 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. The standard is not really meant to be something to strive for; it is really a floor, a basis for further security measures. Failing to achieve even one of the requirements, is failing to meet a basic standard for handling cardholder information. All companies that routinely handle this type of data should be aiming to exceed the standard.

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 sort by the banks (it costs between \$50 and \$90 to replace one card) 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 to Visa. The standard applies at all times. Just saying yes to the questions puts the merchant at great risk. If a compromise took place and it was obvious that the merchant was not and has never been compliant, the matter would be taken very seriously by VISA. The merchant would be risking the whole business by answering "yes" to the questions, when there is no basis in fact for that answer.

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

Merchants are liable and not just for the credit card compromise, there are basically 4 scenarios where credit card data is compromised:

Discovery	Merchant PCI Compliant?	Reported by?	Possible Result
Merchant discovers the compromise	Yes, and subsequent forensic team confirm this	By the merchant to VISA using the approved process	VISA and the Merchant track the compromise and correct any errors in the process. Unlikely any fines are levied and the problem is not made public
VISA discovers the compromise	Yes, and subsequent forensic team confirm this	By VISA	VISA and the Merchant track the compromise and correct any errors in the process. Merchant may be required to improve certain aspects of their security structure. Unlikely any fines are levied and the problem is not made public
Merchant discovers the compromise	No, or was complaint, but forensic team discovered compliance lapsed	By the merchant to VISA using the approved process	VISA and the Merchant track the compromise and correct any errors in the process. Merchant is required to have full annual onsite audit Merchant is required to correct any areas out of compliance and demonstrate compliance at a date set by VISA Fines or damages may be levied
VISA	No, or was complaint, but forensic team discovered compliance lapsed	By VISA	VISA and the Merchant track the compromise and correct any errors in the process. Merchant is required to have full annual onsite audit Merchant will be fined by VISA via the bank and will have to pay restitution to all issuing banks affected; the total of these fines may be \$50 to \$90 per card compromised.

In all the above, you can see that it is not a pleasant experience for the Merchant. 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 indeed.

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

The PCI standard forms part of the operating regulations that are the rules under which Merchants are allowed to operate merchant accounts. The regulations signed when the Merchant opens an account at the bank state that the VISA 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 cards.

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 at a Merchant can result in serious consequences for the Merchant, especially if a compromise has taken place.