

frequently asked questions

Payment Card Industry (PCI) Data Security Standard (DSS)

Many merchants have been hearing a lot about PCI compliancy and wonder what it is and why they have to participate and take time from their busy schedule and business. We hope we can help you get a better understanding by providing you some basic information.

Outlined below are some Questions and Answers that may help.

■ What is PCI and DSS?

In response to the overwhelming occurrences of cardholder fraud and identity theft, the Payment Card Industry (PCI) Data Security Standard (DSS) was created by major credit card companies to safeguard customer information. Visa, MasterCard, American Express, and other credit card associations mandate that merchants and service providers meet certain minimum standards of security when they store, process and transmit cardholder data. Unfortunately, the process of demystifying the rules and obtaining PCI compliance is often confusing.

■ Why is TriSource implementing this program?

The Card brands have mandated that by December 31st of 2008, all merchants must be PCI compliant. Beginning in October 2008, all NEW merchants boarded must be utilizing PCI compliant hardware and software. The only way to ensure merchants are compliant is by performing system scans and in depth Self Assessment Questionnaires.

Additionally, the risk of data breaches continues to increase, with fines resulting in over \$100,000 on some merchants for these breaches.

■ What happens if I am using dial terminals?

Merchants using dial terminals are not part of this managed PCI program. Dial terminal merchants must simply complete the Self Assessment Questionnaire (SAQ)

■ What if I don't complete a Self Assessment Questionnaire (SAQ)?

The Card brands have mandated December, 2008 as the date for compliance. Failure to comply with the PCI standards by that date may result in an inability of merchants to process beyond that date.

■ My business uses a PCI compliant gateway for eCommerce. Why do we need to have scans and complete the Self Assessment Questionnaires?

Using a compliant gateway is only one component of a transaction. The entire *system and environment* must be PCI compliant. The main risk to an eCommerce merchant is the handoff from the merchant website to the eCommerce gateway. This point is vulnerable to viruses, malware and other programs that mask the information making it seem like the consumer is on the merchant's payment site.

Completion of the Self Assessment Questionnaire (SAQ) takes care of PCI compliance in the *environment*, while the scan takes care of PCI within the *system*. If as a merchant your are using a virtual terminal, whether with a swipe or simply key entered, the *environment* must be PCI compliant, and in some cases, the *system*, may also need scans to ensure compliance.



■ Am I 100% secure from breaches if I become PCI DSS compliant?

Self Assessment Questionnaires and scans are only a portion of making sure your business is protected. Think of it this way. If your building has passed all the fire codes it doesn't mean your building won't burn down. If you become compliant with the questionnaires and scanning it doesn't mean you cannot get breached, it merely means that you are complying with the standards as they are written. It is up to you to ensure that your employees continue to follow the standards and that your systems and service providers adhere to the latest requirements.

You may need to take other precautions as well. Some of these precautions are to ensure you have good up to date firewalls, data loss prevention standards, encryption, anti-virus software, solid honest employees.

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.

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.

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.

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.

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.

I can just answer "yes" to all the criteria on the self-assessment. The Self-Assessment Questionnaire 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.

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.

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.

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:

- Un-encrypted 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.