

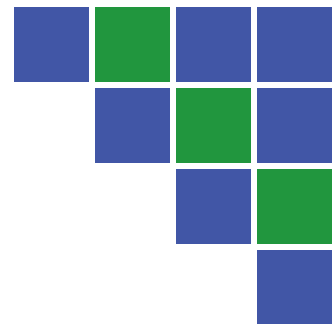


**PANOPTIC SECURITY**

Your PCI Compliance Partner



## Most frequently asked Questions & Responses about PCI Compliance



MEMBER FDIC



Panoptic Security has determined the following questions as those most frequently asked by merchants while working through their SAQ. These questions come in various shapes and forms, and are crucial to the merchants understanding and successful conclusion of the PCI compliance process.

## **ACRONYM    DEFINITION**

ExpertPCI™	Panoptic Security online web application
IP	Internet Protocol
IP Address	Merchant's computer address, similar to a telephone number
PAN	Primary Account Number
PA DSS	Payment Application Data Security Standard
PA-DSS POS	Payment Application Data Security Standard Point of Sale
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
SAQ	Self Assessment Questionnaire

### **1. What is PCI?**

PCI stands for "Payment Card Industry", but it usually means one or the other of the following:

- 1) The Payment Card Industry Security Standards Council. This is an industry body made up of organizations like Visa, MasterCard, American Express, Discover, etc. The Council is how these companies cooperate to agree upon a single, common security standard that they insist merchants meet.

- 2) The actual security standard put together by the Council is described in the first definition above. The name for this standard is the Payment Card Industry Data Security Standard (PCI DSS). Merchants must meet this set of security requirements if their business accepts, transmits, or processes customer payment cards, such as credit or debit cards.

### **2. What is PCI DSS?**

PCI DSS stands for 'Payment Card Industry Data Security Standard'. This is a technical and broad-ranging set of security requirements created by the Payment Card Industry requiring what merchants need to do to protect customer payment information. The PCI Council requires that merchants meet a set of security requirements if their business accepts, transmits, or processes customer payment cards, credit or debit cards. Merchants that do not comply with these requirements can be penalized in a number of ways, up to and including having their card processing privileges revoked, leaving them unable to accept customer payment cards.

### **3. To whom does PCI apply?**

PCI applies to all organizations or merchants, regardless of size, that accept, transmit, or store any payment card information. In other words, if any customer of that organization or merchant pays using a credit or debit card, then the PCI DSS requirements apply.



#### **4. What if a merchant refuses to cooperate?**

Merchants that do not comply with PCI DSS are not necessarily breaking any law, but they are probably violating their Terms of Service or contract with their acquiring bank and the credit card associations. This means that the merchant might be penalized or sued, or these companies might refuse to work with the merchant. This would mean that the merchant would be unable to process credit or debit cards. If a merchant experiences a data breach of their customers credit card information and is not PCI compliant or is not working on becoming compliant, fines and fees of approximately \$100,000 per incident, can be imposed. However, if the merchant has made a good faith effort to become PCI compliant, the fines will be less. Also, many acquirers are imposing a non-compliance fee for any merchant that has not completed the PCI process.

#### **5. Why am I doing this?**

PCI was created and is enforced by the Payment Brands (Visa, MasterCard, Discover, American Express, etc) and also enforced by acquirers in conjunction with the Payment Brands. These service providers are actively working to make the process simpler and easier for you.

#### **6. I don't understand any of these questions, what do I do?**

Answer 'No' to any question that you do not understand or when you are not sure. When you are done answering the questions, the ExpertPCI™ Wizard will give you guidance on how to fix those answers. You will be able to update your answers later, or mark them fixed as part of the Remediation phase.

#### **7. What if I don't understand a Security Question?**

Make sure to read any assistance text provided on the page including any mouse-over explanations (words in green and double underlined) or technical terms, the help text given beneath the question, and the text that can sometimes be found beside the available answer buttons.

#### **8. What is key management?**

If you store credit card data within your payment application, the application requires a 'key' to unlock the credit card data so the data can be used. This 'key' must be protected by policies and procedures within your organization. Usually the software that does the encryption manages its own 'keys' (maybe on a smart card), and you must take extra steps to protect the 'keys'.

#### **9. What is a firewall?**

A firewall is a security product that controls network traffic, allowing 'good' traffic in and blocking 'bad' or unknown traffic. They are often separate devices that sit on your computer network, but can also be software that sits on another computer (laptop, DSL or cable modem).



### **10. What is access control?**

Access control is how you control who has access to credit card information. This includes how individuals are identified to the system i.e. passwords, fingerprints, etc. Access control needs to be updated when an employee leaves the company, changes roles within the company, etc. Passwords MUST be changed every 90 days.

### **11. Why do I need to change my password?**

PCI DSS requires that passwords be changed every 90 days. This limits the amount of information that could be compromised if a hacker obtains your password.

### **12. What is my IP address?**

To obtain your IP address for your payment application, go to <http://www.find-ip-address.org>. Your IP address is on the line of text beginning with 'IP Address Lookup – IP Finder for MY IP (WAN IP)'. Your IP address is a series of numbers separated by 'dots'. i.e. 000.000.0.000

### **13. What is meant by 'Compliance'?**

Compliance means meeting all of the requirements laid out in the Payment Card Industry Data Security Standard. The requirements of compliance are the same for ALL merchants, large or small. However, smaller merchants typically avoid many of the compliance problems that larger organizations face, because their systems and networks are usually simpler.

### **14. What is meant by 'Validation'?**

Validation means a merchant's ability to show, via standard documents and/or tests, that they are meeting the PCI DSS requirements. Different types of merchants face different levels of validation depending on which of four levels they fall into.

### **15. What is meant by 'Remediation'?**

Remediation means the process of fixing any compliance failures. A merchant, who constructs an appropriate remediation program and completes it, will be by definition in compliance with the PCI DSS requirements.

### **16. How do I schedule a scan?**

Log into ExpertPCI™. Click on 'Manage PCI Scanning', and then click on 'Go To Scanning Website', which will take you to the ComplyGuard website. Click on 'Schedule a Test', then click on 'Run a Test Now', and click on 'Submit'. It is a good idea at this time to schedule scans every 90 days, as required. Click on 'Run Future Test' and choose 'Every 90 Days'. You will receive an email from ComplyGuard as to when your scan is scheduled to run and another email with the pass/fail results of the scan.



### **17. How do I get my scan results?**

Log into ExpertPCI™. Click on 'Manage PCI Scanning', which takes you to the PCI Scan Status page. Click on the 'Go To Scanning Website'. You can obtain your scanning results by clicking on 'View Test Results' and click on the most current scan report.

### **18. I failed scanning, how do I fix it?**

Log into ExpertPCI™. Click on 'Manage PCI Scanning', and then click on 'Go To Scanning Website', click on 'View Test Results', click on the 'Failed' report, and then click on the 'Technical Report Tab'. This report will provide a detail of what failed and suggestions on how to fix the failures. If you still have questions, click on the 'Live Help' icon, which will connect you with the scanning support team.

### **19. Do I have to update my SAQ answers when I fix something?**

You are expected to update your SAQ when you fix a problem. The ExpertPCI™ Wizard will do that for you if you use the Remediation Plan to track and manage your progress.

### **20. I have a PA-DSS POS, why do I need to do anything else?**

Using a PA-DSS certified Point of Sale device is a good idea, but it does NOT make you compliant, it just means that you've avoided one way of failing. You still need to complete an SAQ and fix any other problems identified through the SAQ.



If you have any questions please email us at:  
[support@panopticsecurity.com](mailto:support@panopticsecurity.com)

