PCI DSS Compliance Frequently Asked Questions

1. **What is the Payment Card Industry Data Security Standard, or PCI DSS?**

The Payment Card Industry Data Security Standard (PCI DSS) is a set of industry standards designed to protect payment card data. Intended to create an additional level of protection for consumers and reduce the risk of data breaches involving personal cardholder data, the standards are comprised of 12 broad requirements and collectively, more than 200 line item requirements. The 12 broad requirements can be grouped into six key areas: **building and maintaining a secure network; protecting cardholder data; maintaining a vulnerability management program; implementing strong access control measures; regularly monitor and testing networks;** and **maintaining an information security policy.**

Any organization that transmits, stores or processes primary account numbers (PAN) is required to comply with the PCI DSS. In addition, where other cardholder data is stored, processed or transmitted with PAN it must also be protected. Cardholder data includes Primary Account Numbers (PAN), Cardholder name, Expiration Date and Service Codes. Another type of data, known as Sensitive Authentication Data (SAD), is also covered by PCI DSS, but generally the storage of SAD is prohibited. Compliance with the DSS requirements is mandatory, regardless of the size of the merchant or the number of card transactions they process each year. You may be required to complete PCI reporting documentation even if outsourcing your payment card processing to a third party.

2. **What is the role of the PCI Security Standards Council?**

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Founded in 2006 by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., the Council has more than 600 participating organizations that represent merchants, banks, processors and vendors worldwide. It is responsible for the development, management, education, and awareness of the PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements.

Enforcement of compliance with the PCI standards and determination of non-compliance penalties are carried out by the individual payment card brands.

3. **Where can I find the list of PCI DSS requirements?**

For more information on the PCI DSS requirements and updates, visit the PCI Council website. This website has useful information about the PCI Security Standards Council, the complete PCI DSS requirements for merchants, vendors and security consulting companies, and the Council's certification and merchant support services. It also has regular updates on changes to the PCI requirements and upcoming PCI Council events.

4. **Are there any benefits to PCI DSS compliance?**

By properly implementing the PCI DSS and achieving and maintaining compliance, merchants can improve their overall security posture and avoid costly fines and data breaches. They can be better prepared to prevent and detect a host of attacks against their information assets, both at the network and physical level. PCI compliance can improve operational efficiency by ensuring that policies are defined and procedures are documented so that employees know what they should be doing and how to do it. Controls, policies and procedures developed for PCI can be rolled out across the organization to spread the security benefits and reap the greatest return on investment from a PCI compliance project. While compliance does not equal security, the PCI standards can serve as a starting point and framework for organizations that wish to create a more secure environment and better protect their customers.

5. **What kinds of organizations may be impacted by PCI DSS compliance standards?**

Any organization that transmits, processes or stores payment card data - debit and credit cards included - must comply with the PCI standards. This includes **financial institutions**, such as banks, insurance companies, lending agencies and brokerage firms. It also includes all kinds of **merchants**, from medical and dental offices to pharmacies, hospitals, schools and universities, clothing stores, government agencies, cafes, restaurants, and ecommerce companies. It even affects individuals that accept payment cards for purchases, such as those at a farmer's market, food truck or crafts fair.

It also includes **service providers** such as transaction processors, payment gateways, customer call centers, web hosting providers and data centers, among others.

In addition to the requirements laid out in the PCI Data Security Standard (PCI DSS), the PCI Council has created programs specifically for **software developers** as well as **hardware** and **device manufacturers**, including the Payment Application Data Security Standard (PA-DSS) and the PIN Transaction Security (PTS) program.

6. **Who enforces the PCI DSS requirements?**

Although the PCI DSS requirements are developed and maintained by an industry standards body called the PCI Security Standards Council (SSC), the standards are enforced by the five payment card brands: Visa, MasterCard, American Express, JCB International and Discover. Each brand provides its own compliance guidelines, reporting and validation requirements, deadlines, brand-specific definitions and penalties for noncompliance. Please contact your merchant bank for its specific validation requirements and deadlines. Service providers should seek advice directly from the individual card brands.

7. **Why is PCI DSS compliance important?**

PCI DSS compliance is important for many reasons. Failure to comply with PCI requirements can lead to steep fines and penalties levied by the card brands, revocation of credit card payment services or even suspension of accounts. Security oversights can also leave merchants vulnerable to costly and damaging data breaches. Besides making headline news, data breaches can lead to lawsuits, remediation costs and irreparable damage to a merchant's reputation.

In addition to making headline news and increasing the risk of identity theft, data breaches and non-compliance can lead to significant fines and penalties. Fines can range from $2,000 to more than $100,000 per month for PCI compliance violations, plus additional fines for repeat violations, depending on the merchant's acquiring bank. The banks typically pass such fines on to merchants.

If cardholder data is compromised, merchants may also be subject to fraud losses incurred from the use of the compromised account numbers, the cost of re-issuing cards associated with the compromise, and the cost of any additional fraud prevention or detection activities required by the card associations (i.e., a forensic audit) or costs incurred by credit card issuers associated with the compromise (i.e., additional monitoring of system for fraudulent activity). Although fines and penalties are not widely publicized, they can be catastrophic to a small business and cause a great deal of inconvenience and expense to larger organizations. Fines are usually based on number of card records stolen, and may vary depending on payment card brand. In short, if you suffer a breach, you won't like the consequences.

A payment processor that is liable for fines may choose to pass those on to their customers through a similar mechanism, such as higher transaction fees or service charges.

8. **Do the PCI DSS compliance requirements apply to merchants outside the U.S.?**

Yes, the PCI DSS requirements apply to all merchants, even those outside the U.S. The difference is that historically enforcement has been stricter in the U.S. As enforcement rates in the UK and Europe increase, and stricter laws around customer notification of data breaches are enacted by many countries, global PCI compliance rates are expected to increase accordingly. As part of the open standards development process, the PCI Council solicits input on the standards from its global stakeholders through a variety of avenues, including a formal feedback period.

9. **Do the PCI DSS requirements apply to just large organizations?**

No, the PCI requirements apply to all organizations that transmit, process or store data, including those that have a limited number of transactions. Although outsourcing some or all of your payment processes may simplify them and reduce what is in scope for PCI compliance, you cannot ignore it. You need to have policies and procedures in place to protect cardholder data when you get it, as well as when you process charge backs and refunds. Your payment card issuer may also require you to ensure that providers' applications and card payment terminals are PCI compliant. While the payment card issuers initially focused enforcement efforts on Level 1 merchants, they have increased enforcement for Level 2 through 4 merchants in the past few years.

10. What happens to a small business when they don't know enough about PCI DSS and suffer a breach?

It is important for small businesses to understand PCI compliance, not just to protect their customers, but to protect their business. Although many small businesses don't have security expertise or dedicated in-house resources, they must still comply with PCI standards. When a small business is compromised, it may immediately be treated as a Level 1 merchant by the payment card brands and thus subject to greater levels of examination and assessments, including hiring a QSA to conduct a PCI assessment and issuing a Report on Compliance (ROC). It may face increased fines from the payment brands or their acquirer, be required to submit to a detailed forensics investigation, and lose customer trust, any of which may put it out of business. Whether it is commercially sensitive information or intellectual property designs that criminals are after, any size of organization can be targeted. Smaller firms may also be targeted as a means to get to partners, such as larger companies that have a bigger store of financial details.

11. What are the PCI DSS compliance validation requirements for different merchant levels?

In addition to meeting the security requirements of PCI DSS, merchants and service providers must also validate their compliance each year, as outlined in the table below. All merchants and service providers, regardless of where they are based, must submit a passing vulnerability scan performed by an Approved Scanning Vendor (ASV) regardless of their size or the number of credit card transactions they process each year.

Level 1 merchants (greater than 6 million transactions per year) and Level 1 service providers (greater than 300,000 transactions per year) must also undergo an annual onsite audit performed by a Qualified Security Assessor (QSA) or by an employee of the company who has gone through the PCI Internal Security Assessment Training Program.

Level 2, 3 and 4 merchants and service providers must complete a PCI Self-Assessment Questionnaire (SAQ) along with an Attestation of Compliance. Once completed, validation results and documented compliance controls must be submitted to the merchant's acquiring bank. It is important to note that requirements may vary depending on the payment card. For example, Level 2 merchants that accept MasterCard must have more rigor than just the SAQ self-assessment that applies to Levels 3 - 4. MasterCard specifies that as of June 30, 2012, Level 2 merchants that choose to complete an annual SAQ questionnaire must ensure that staff engaged in the self-assessment attend PCI SSC ISA Training, and must pass the associated accreditation program annually in order to continue the option of self-assessment for compliance validation. Alternatively, Level 2 merchants may, at their own discretion, complete an annual onsite assessment conducted by an approved QSA rather than complete an annual self-assessment questionnaire.

It is also important to note that if a Level 2 - 4 merchant suffers a breach that results in a data compromise, they may be escalated to a Level 1 validation level. [Note: also see Visa's definition of merchant levels, which is largely determined by transaction volume. The MasterCard and American Express definitions of merchant levels are similar to Visa's.]

Table 1: Merchant and Service Provider Levels and Validation Requirements

	Levels	Criteria	Annual QSA Audit	Annual SAQ	Quarterly ASV Scan
Merchants	1	6,000,000+ transactions per year or compromised in the past year	✓		✓
	2	1 million to 6 million transactions per year		✓	✓
	3	20,000 to 1 million e-commerce transactions per year		✓	✓
	4	Less than 20,000 e-commerce transactions per year and all other merchants processing up to 1 million transactions per year		✓	✓
Service Providers	1	All VisaNet processors (member and nonmember), and all payment gateways	✓		
	2	Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 Visa accounts/transactions annually	✓		
	3	Any service provider that is not in Level 1 and stores, processes, or transmits less than 1,000,000 Visa accounts/transactions annually		✓	✓

12. How often is PCI DSS validation required?

Merchants must demonstrate compliance annually via a Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC). Validation requirements vary depending on the number of transactions processed annually and the payment card brand. As with other regulations and guidelines, PCI DSS compliance cannot be achieved through technology alone. Compliance requires establishing and maintaining a PCI program that incorporates appropriate business policies, procedures and technologies to ensure ongoing compliance through continuous protection of payment card data.

13. If I use a third-party to process payments, or an ecommerce platform, do I still need to worry about PCI compliance?

Yes, you do. Although outsourcing some or all of your payment processes may reduce your risk of breach or what is in scope for PCI compliance, you cannot ignore it.

14. What kind of vulnerability scanning is required to validate compliance?

Merchants and Service Providers (and any other entity that requires PCI compliance) must perform quarterly internal and external vulnerability scanning. External vulnerability scans must be conducted by an Approved Scanning Vendor (ASV) and result in the production of a passing scan report showing no vulnerabilities are present. Internal scanning can be conducted by the entity themselves, but again, there must be a process to document at least quarterly that a scan has been conducted and any issues remediated, with re-scanning resulting in a "passing" internal scan. Internal and external scan reports will need to be retained as evidence for presentation to a QSA or other external assessment entity such as acquiring banks, card brands or forensic investigation teams.

15. Why engage Dell SecureWorks to assist with PCI compliance?

Merchants typically find that working with Dell SecureWorks helps them cut down on their overall costs and resources, and that they can complete a compliance assessment faster. We also help merchants make the most of what they already have in their security environment and existing PCI processes. For example, if you have a combination of firewalls and security devices from different vendors, we can help monitor and manage them, as well as help you make them more secure with modifications as needed. Our team of compliance professionals and consultants has an average of more than 10 years' experience in their areas of expertise. Not only are they expert in the complex regulatory requirements of various industries, but they are adept in helping organizations create short-term and long-term remediation plans to meet compliance requirements. They can also help reduce the overall costs of meeting compliance requirements. As a Managed Security Services customer, your organization will also enjoy unmetered guidance and support from our team of certified Security Analysts.

16. What kinds of services does Dell SecureWorks offer for mid-size or smaller merchants?

Dell SecureWorks offers services for merchants at almost all levels. Although we work with a number of enterprise and Level 1 merchants, we also work with regional retailers and other smaller merchants to help them address PCI DSS requirements. For example, there are some companies that only want a quarterly PCI network scan from an Approved Scanning Vendor (ASV), which we offer. Or they need help with monitoring and managing their firewalls. Sometimes customers wish to conduct their self-assessment questionnaire (SAQ) in house, but then realize they need help with remediation or guidance on how to reduce the scope of what's in consideration for PCI compliance, and we can assist with that as well.

17. What kinds of consulting services does Dell SecureWorks offer for PCI compliance?

Dell SecureWorks offers a full suite of consulting solutions to help merchants address PCI compliance. Each service builds on the work accomplished in the previous stage. These include Readiness Reviews, Gap Analyses, Mock Audits and Reports on Compliance (ROC) or assistance with Self-Assessment Questionnaires (SAQ).

18. What other products and services does Dell offer to help merchants with PCI compliance? How do Dell SecureWorks services complement them?

Dell offers a full suite of hardware, appliances and software to help address all 12 aspects of PCI compliance, including SonicWALL firewalls, KACE appliances, endpoint solutions and others. Dell SecureWorks complements these products by providing merchants with expert advice to help them develop a strategy for achieving compliance, as well as vendor-neutral managed services to help monitor and manage firewalls, IDS/IPS, log management systems, SIEM systems, quarterly PCI scanning, and all of the other controls mandated by PCI DSS.

19. Does Dell SecureWorks provide PCI compliance services for PCI service providers?

Many of our Managed Security Services, such as log monitoring, firewall management and web application firewall management, may help service providers address PCI compliance concerns. We also offer Security & Risk Consulting to assist with PCI compliance Readiness Reviews, penetration testing and other security and compliance services. Please contact us for more details.

20. What are some of the practical challenges companies face when trying to maintain PCI compliance?

Organizations often assemble a team of people as a task force to meet initial compliance requirements, or pass a ROC or SAQ, but then disband it after certification. Dell SecureWorks recommends ongoing attention and a standing team to review policies, procedures and everything else related to PCI compliance on a regular basis, not just once a year.

Another challenge is that companies may purchase new equipment or devices to meet certain PCI compliance requirements, but fail to monitor or manage them after they are set up, which effectively renders them useless against threats. Or organizations may create an employee policy document and never update it, even though there is frequent staff turnover. In other instances, organizations may get initial management buy-in to become compliant, but lack ongoing funding and budgets to properly maintain compliance.

21. **What are some of the technical challenges companies face when trying to maintain PCI compliance?**

Some of the most common technical challenges include network segmentation, data encryption, patch management and wireless networking security. Others include 24x7 log monitoring, firewall management and web application firewall management.

22. **Is an annual ROC or SAQ all that is required to be PCI compliant? How can companies better maintain PCI compliance?**

Although an annual Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ) requires a significant investment of time and resources, it is merely a snapshot of a moment in time. It is not the same as ongoing compliance, which requires dedicated people, processes and technology. Any changes to the merchant environment can lead to non-compliance. There are several steps merchants can take to better meet their compliance obligations and ensure they have effective security controls. Dell SecureWorks recommends embedding security controls into everyday processes, performing regular PCI health checks, and preparing for assessments with an organized plan.

23. **If my organization is certified as PCI compliant, does it mean it is secure?**

No, as many high-profile data breach cases have shown, companies that are certified as PCI compliant can still suffer data breaches and financial losses. PCI compliance alone won't protect corporate data and systems from costly, time-consuming data breaches and advanced threats. PCI compliance should be viewed as the baseline, not the end goal, for any organization. Annual validation of compliance means nothing without continual efforts to maintain that compliant state. A well-defined security program can help organizations not only meet and maintain PCI compliance, but also address new and emerging threats as well as innovations such as mobile, virtualization and other technology. Only by designing, implementing and maintaining effective security controls to meet PCI requirements can organizations gain security alongside compliance.

24. **What do I need to consider regarding mobile devices and tablets for employees in a store environment, as it relates to PCI compliance?**

One of the key things is to determine what the devices are going to be used for and whether or not they'll be used to process transactions or have any payment card data processed through them or stored on them. If so, they will fall into scope for PCI compliance. Even being on the same network as systems that store, process or transmit payment card data will bring these devices into scope. While the PCI guidelines might not have specific requirements yet for every aspect of mobile applications and devices, they are clear around keeping cardholder data protected, wherever it may be.

This is such a new area for many merchants that they aren't properly addressing security issues or updating their employee guidelines or policies to deal with them adequately. You can't take it for granted that employees will know what to do in a given situation or think about the ramifications of bringing their own devices into store or medical environments. Make them aware of the need for compliance and why it's important to customers and to the business.

25. **I am new to PCI and have no idea where to start. What do you suggest?**

If you're just getting started with PCI compliance, you can find a wealth of information on the PCI Council website. For more information, download the PCI Council's **Getting Started Guide** and **Quick Reference Guide**. To learn what your specific compliance requirements are, the PCI Council recommends you check with your card brand:

- American Express
- Discover Financial Services
- JCB International
- MasterCard Worldwide
- Visa Inc.
- Visa Europe

In addition, you may wish to join any number of PCI compliance-related discussion groups on LinkedIn or through other industry forums. We also suggest you take advantage of complimentary webcasts and other educational tools offered by Dell SecureWorks.

Within your organization, we recommend that you form an internal PCI compliance team if there isn't one already, and begin organizing your PCI compliance efforts around the guidelines and processes published by the PCI Council. Dell SecureWorks can also assist you via a Gap Analysis or other PCI consulting engagement.

26. What is PCI PFI?

The PCI Forensic Investigator (PFI) program was created to establish a standardized process for the forensic investigation and reporting of information security incidents involving cardholder information.

For more information, visit http://www.secureworks.com.

Email info@secureworks.com or phone 877-838-7947 to speak to a Dell SecureWorks Security Specialist.