

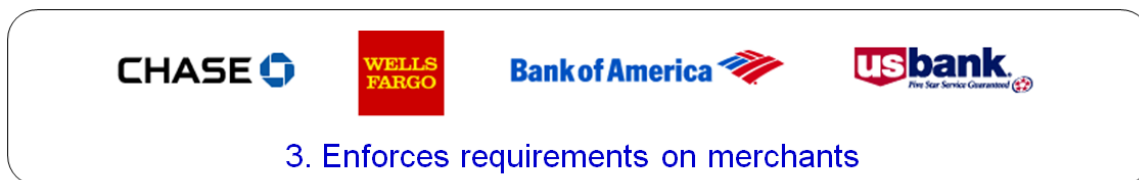
The Top 10 Compliance Issues for the Payment Card Industry (PCI)

By Rick Dakin, President, Coalfire Systems

Many organizations are aware of the Payment Card Industry (PCI) and PCI compliance but are unsure if they're doing everything necessary. These are some common questions from merchants, service providers, and other organizations that must meet PCI requirements.

1. What is PCI?

PCI is a general term for the Payment Card Industry. This industry encompasses all organizations that store, process and transmit cardholder data. The major stakeholders in PCI are merchants, service providers, banks, card brands, the PCI Security Standards Council (PCI SSC), and PCI assessors (QSAs) and Approved Scan Vendors (ASVs). There are three main tiers of players: the PCI SSC, card brands, and member banks.



PCI SSC - The PCI Security Standards Council (www.pcisecuritystandards.org) is an independent organization founded in 2006. The PCI SSC is responsible for the development, management, education, and awareness of the PCI Security Standards. The **PCI SSC does NOT enforce or manage PCI compliance.** The PCI SSC publishes standards, maintains authorized assessors, educates and certifies assessors, and maintains lists of approved assessors and applications.

There are four major compliance programs that the PCI SSC is responsible for:

1. Data Security Standard (DSS)
2. Approved Scan Vendor (ASV)
3. Payment Application Data Security Standard (PA-DSS)
4. Pin-Entry Device (PED)

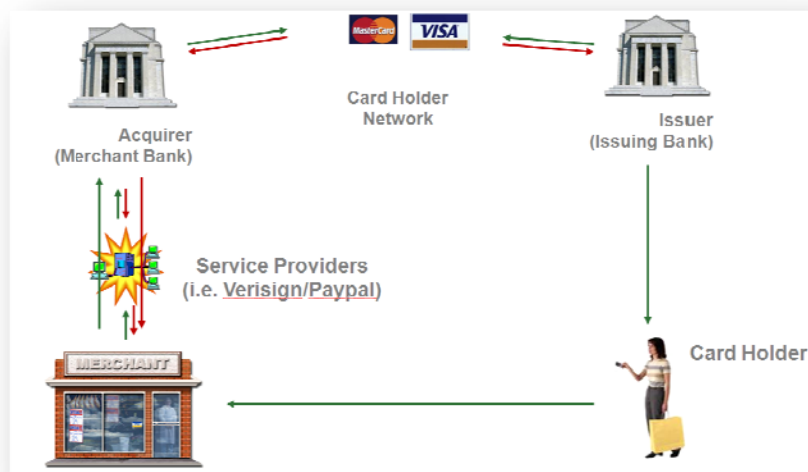
Card Brands – The major card brands (American Express, Discover, JCB, MasterCard, and Visa) maintain their own compliance programs. While there are differences in the operational regulations for each brand and their respective validation requirements, all card brands require their merchants, service providers, and member banks to be PCI-compliant at all times. For example, page 72 of Visa USA’s Operating Regulations¹ states “A Member must comply, and ensure that its Merchants and Agents comply, with the Payment Card Industry Data Security Standard and the validation and reporting requirements as outlines in the Cardholder Information Security Program.”

Each card brand has similar statements. They require their member banks to be compliant with their specific card brand requirements, and also to meet the requirements of the PCI DSS. The banks are responsible for ensuring that their merchants are compliant. (**Note:** American Express is not a member association and, therefore does not utilize member banks.) More information can be found for these programs at:

Card Brand	Compliance Program	Website
VISA	CISP (Cardholder Information Security Program)	www.visa.com/cisp
MasterCard	SDP (Site Data Protection)	www.mastercard.com/sdp
American Express	DSOP (Data Security Operating Procedures)	www.americanexpress.com/datasecurity
Discover	DISC (Discover Information Security and Compliance)	www.discovernetwork.com/DISC
JCB	JCB Data Security Program	www.jcb-global.com/english/pci

Member Banks are banks that connect to the card brands and accept credit card transactions. Card brands can act as intermediaries for the settlement and reconciliation of credit card transactions through their networks (i.e. Visa and MasterCard), or they can act as the banks themselves (American Express).

The following illustration provides a high-level overview:



¹ <http://usa.visa.com/download/merchants/visa-usa-operating-regulations.pdf>

2. What do merchants have to do to be PCI-compliant?

Merchants must meet the requirements of the PCI DSS at all times. Compliance is, however, different from validation. Although merchants must be *compliant* at all times, they *validate* their compliance by providing two items to their banks upon request:

1. Report on Compliance (ROC) or Self Assessment Questionnaire (SAQ)
2. Quarterly Network scans.

ROCs are independent assessments conducted by companies that are trained and authorized by the PCI SSC. These companies are Qualified Security Assessors (QSAs) and complete their assessments according to the PCI Assessment Procedures. ROCs are required for large merchants (Level 1 and Level 2 merchants).

SAQs follow a similar format to the ROC, but are not performed by QSAs. Instead, they are self-attestations provided by a company officer of an organization.

Quarterly Network Scans are technical tests conducted by Approved Scan Vendors (ASVs). ASVs run external scans on all public-facing IP addresses of an organization and rank the findings based on guidance from the PCI SSC.

The Prioritized Approach provides guidance that will help merchants identify how to reduce risk to cardholder data as early as possible in their compliance journey. The tool groups together the requirements of PCI DSS 1.2 into six key milestones for merchants to consider in their card data security strategy.

For merchants who are new to the PCI-compliance program, the PCI SSC has published a “Prioritized Approach” that offers guidance on how to focus PCI DSS implementation efforts in a way that expedites the security of cardholder data.

<https://www.pcisecuritystandards.org/education/prioritized.shtml>

3. How do I know my merchant level?

The acquiring bank for each merchant is ultimately responsible for determining how that merchant will attest to their PCI-compliance status. The card brands have set a tiered system for determining validation. Most merchants have their level determined by the number of transactions per card type in a year. This is based on volume and not the transaction dollar amount.

Level	American Express	MasterCard	Visa
1	Merchants processing over 2.5 million AMEX card transactions annually or any merchant that AMEX otherwise deems a Level 1.	Merchants processing over 6 million MasterCard transactions (all channels) annually or compromised merchants.	Merchants processing over 6 million Visa Transactions annually, identified by another payment card brand as level 1 , or merchants compromised last year.
2	Merchants processing 50,000 to 2.5 million AMEX transactions annually, or any merchant that AMEX otherwise deems a Level 2.	Merchants processing 1 million to 6 million MasterCard transactions annually or any merchant considered Level 2 by another card brand.	Merchants processing 1 million to 6 million Visa transactions annually.
3	Merchants processing less than 50,000 AMEX transactions annually.	Merchants processing over 20,000 MasterCard e-commerce transactions annually.	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually.
4	N/A	All other MasterCard merchants.	Merchants processing less than 20,000 Visa e-commerce transactions annually, and all other merchants processing up to 1 million Visa transactions annually.

4. What determines if a merchant requires a ROC or a SAQ?

Each acquiring bank ultimately decides whether they will accept a SAQ or ROC from a merchant. In general, if a merchant is accepting more than 6 million transactions for any card brand, the acquiring bank will require an onsite assessment (ROC).

On June 15, 2009, however, MasterCard Worldwide announced that **Level 2** merchants must validate PCI compliance through an on-site review (ROC) conducted by a PCI Qualified Security Assessor (QSA) and issued no later than December 31, 2010.

Level	American Express	MasterCard	Visa
1	<ul style="list-style-type: none"> Onsite Review by a QSA. Quarterly Network Scan by ASV. 	<ul style="list-style-type: none"> Onsite Review by a QSA. Quarterly Network Scan by ASV. 	<ul style="list-style-type: none"> Onsite Review by a QSA. Quarterly Network Scan by ASV.
2	<ul style="list-style-type: none"> Quarterly Network Scan by ASV. 	<ul style="list-style-type: none"> Onsite Review by a QSA. Quarterly Network Scan by ASV. 	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Quarterly Network Scan by ASV.
3	<ul style="list-style-type: none"> Quarterly Network Scan by ASV. 	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Quarterly Network Scan by ASV. 	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Quarterly Network Scan by ASV.
4	N/A	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Quarterly Network Scan by ASV. 	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Quarterly Network Scan by ASV.

5. What is a service provider?

The PCI has different requirements for service providers than merchants. Service providers are organizations that process, store, or transmit cardholder data on behalf of client, merchants, or other service providers.

Visa classifies service providers as Third Party Agents (TPA). A TPA is an entity, not connected to VisaNet, that provides payment-related services, directly or indirectly, to a Visa client and/or stores, processes or transmits Visa account numbers. TPAs include organizations such as Independent Sales Organizations (ISOs), Third Party Servicers (TPSs), Encryption and Support Organizations (ESOs) and Merchant Servicers (MSs). **Agent registration is required for all entities performing solicitation activities and/or storing, processing or transmitting Visa account numbers for Visa clients (or on behalf of their merchants).**

http://usa.visa.com/download/merchants/Agent_FAQ.pdf

6. How do service providers determine their level and compliance requirements?

Unlike merchant levels, there are only two levels of service providers. Service providers are organizations that process, store or transmit cardholder data on behalf of clients, merchants or other service providers. Service providers is a collective term for Third Party Processors (TPPs) and Data Storage Entities (DSE) in the MasterCard program. Service provider levels are defined as:

Level	MasterCard	Visa
1	All Third Party Processors and all Data Storage Entities that store, transmit, or process greater than 300,000 total combined MasterCard and Maestro transactions annually	All VisaNet processors (member and nonmember) and any service provider that stores, processes, or transmits more than 300,000 Visa accounts / transactions annually.
2	Includes all Data Storage Entities that store, transmit, or process less than 300,000 total combined MasterCard and Maestro transactions annually	Any service provider that stores, processes, or transmits fewer than 300,000 Visa accounts / transactions annually.

<http://www.mastercard.com/us/sdp/serviceproviders/index.html>

http://usa.visa.com/merchants/risk_management/cisp_service_providers.html

All Level-1 service providers must have an annual onsite review (Report on Compliance--ROC) conducted by a QSA. Compliant service providers are listed by MasterCard and Visa on their respective websites. If an organization is sharing cardholder data with a service provider who does more than 300,000 transactions annually, they should ensure that this service provider is PCI compliant. Both Visa and MasterCard maintain a list of PCI-compliant service providers.

Visa PCI-Compliant Service Providers

www.visa.com/cisp

MasterCard PCI-Compliant Service Providers

www.mastercard.com/us/sdp/serviceproviders/index.html

7. What is the PA-DSS?

The Payment Application Data Security Standard (PA-DSS) is a separate program from the DSS. The DSS applies to merchants and service providers that store, process, or transmit cardholder data. However, there are many applications (such as shopping carts, point of sale systems, registration programs) that are sold as software, and are not managed by

service providers. If an organization is buying payment software from a third party, they should ensure the software is certified to meet PA-DSS.

Validated payment applications are listed by the PCI SSC. Only the specific build on the list is approved (i.e. older and newer versions not listed are not validated as compliant).

https://www.pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html

There is also a list of known vulnerable payment applications. This list is not made available to the public. Contact Coalfire if you think you may have a vulnerable payment application.

8. What are the penalties for non-compliance?

PCI is enforced by member banks, so each bank may issue its own penalties to encourage compliance. If there is a breach of cardholder data, an organization will generally be required to pay the costs for the damages of the lost credit card numbers. In addition, each card brand can enforce penalties that are passed to the service providers or member banks and onto the compromised entity. American Express has published fines in excess of \$200,000 per month of non-compliance status. In general, we have seen banks enforce fines of \$25,000 per month for non-compliant Level 1 and 2 merchants, and \$10,000 per month for non-compliant Level 3 and 4 merchants.

https://www209.americanexpress.com/merchant/singlevoice/pdfs/en_US/DSOP_Service_Provider_US.pdf

9. What is the PIN Entry Device (PED) program?

When PINs are used for credit card transactions, they are entered into devices that consist of hardware and software that encrypt the PIN based on a set of standards and protocols published by the card brands. PCI SSC maintains the list of all PED-compliant devices. If an organization is using a device that accepts PINs, they should ensure that the device is approved. Only the specific build, version, and firmware listed are approved.

https://www.pcisecuritystandards.org/security_standards/ped/pedapprovalist.html

10. Where can I find a list of PCI-approved assessors?

Coalfire was one of the first companies authorized to conduct assessments to meet all requirements for merchants and service providers. Coalfire is approved for all three PCI programs:

- QSA Qualified Security Assessor
- ASV Approved Scan Vendor
- PA-QSA Payment Application Qualified Security Assessor

Coalfire was also one of the first companies to pass the PCI SSC Quality Assurance review, so our work has been reviewed and accepted by the PCI SSC. For more information on Coalfire, please visit our website at www.coalfiresystems.com.

The authorized list of companies that are allowed to conduct onsite assessments can be found at the link below. This list includes those companies in “Remediation” that did not meet standards during a quality assurance review conducted by the PCI SSC review. This link includes a listing of all authorized QSAs, PA-QSAs, ASVs, and individual QSA employees:

https://www.pcisecuritystandards.org/qa_asv/find_one.shtml