

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

Many organizations are aware of the Payment Card Industry (PCI) and PCI compliance but are not sure if they're doing everything necessary. This white paper provides an overview of PCI, along with useful information for 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 Qualified Security Assessors (QSAs) and Approved Scanning 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](http://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 for merchants or service providers.** 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 Scanning Vendors (ASVs)
3. Payment Application-Data Security Standard (PA-DSS)
4. PIN Transaction Security (PTS)

**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 Regulations<sup>1</sup> 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 outlined in the Cardholder Information Security Program.”

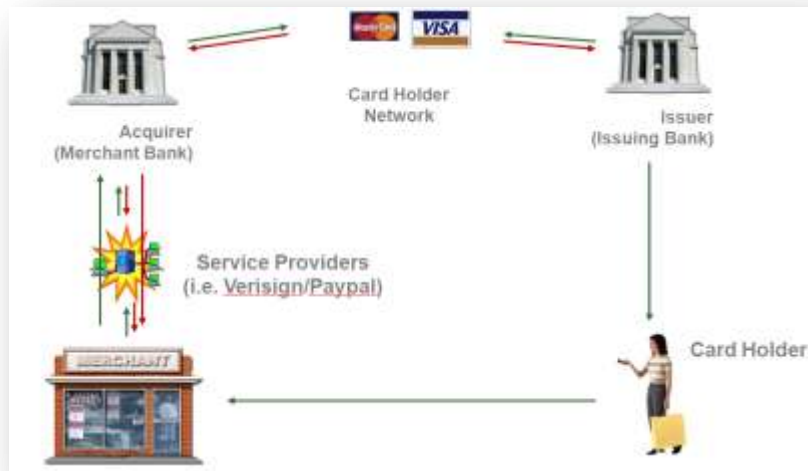
<sup>1</sup> <http://usa.visa.com/download/merchants/visa-usa-operating-regulations.pdf>

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. More information can be found for these programs at the web sites listed in the following table.

Card Brand	Compliance Program	Web site
VISA	CISP (Cardholder Information Security Program)	<a href="http://www.visa.com/cisp">www.visa.com/cisp</a>
MasterCard	SDP (Site Data Protection)	<a href="http://www.mastercard.com/sdp">www.mastercard.com/sdp</a>
American Express	DSOP (Data Security Operating Procedures)	<a href="http://www.americanexpress.com/datasecurity">www.americanexpress.com/datasecurity</a>
Discover	DISC (Discover Information Security and Compliance)	<a href="http://www.discovernetwork.com/DISC">www.discovernetwork.com/DISC</a>
JCB	JCB Data Security Program	<a href="http://www.jcb-global.com/english/pci">www.jcb-global.com/english/pci</a>

**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:



## 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 Scanning 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>

The PCI SSC announced a new Internal Security Assessor (ISA) program and released the “Validation Requirements for Internal Security Assessors” at the end of April 2010. The ISA program states that it is intended to help merchants better prepare for assessments, interface with their QSA, and manage their compliance programs; it is not intended to replace QSA services. However, MasterCard has indicated that this program must be used for Level 1 and 2 Merchants that want to do self assessments after June 2011.

The ISA program is an accreditation program, unlike the standard PCI merchant training. As such, the requirements are much more detailed. The “Validation Requirements for Internal Security Assessors” is written to allow only full-time Internal IT Security Auditors to qualify as an ISA. Details about the program and its requirements are at the link below.

[https://www.pcisecuritystandards.org/education/isa\\_training.shtml](https://www.pcisecuritystandards.org/education/isa_training.shtml)

## 3. How do I know my merchant level?

The card brands have set a tiered system for determining merchant levels. 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. The acquiring bank for each merchant is ultimately responsible for determining merchant levels, so the best approach is to contact your acquirer.

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

Each acquiring bank ultimately determines merchant validation requirements. The card brands each publish their own guidelines, which are summarized in the table below.

Merchant Level	Description	Validation Action	Validated By
1	Merchants processing over 6 million transactions annually (all channels) or global merchants identified as Level 1 by a card brand.  Any merchant that has suffered a hack or that a card brand at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the system	<ul style="list-style-type: none"> <li>• Annual Onsite PCI Data Security Assessment</li> <li>• Quarterly Network Scan</li> </ul>	<ul style="list-style-type: none"> <li>• Qualified Security Assessor or Internal Audit if signed by Officer of the company</li> <li>• Approved Scanning Vendor</li> </ul>
2	Any merchant regardless of acceptance channel processing 1,000,000 to 6,000,000 transactions per year	<ul style="list-style-type: none"> <li>• Annual PCI Self Assessment Questionnaire</li> <li>--- OR ---</li> <li>• Annual Onsite PCI Data Security Audit</li> <li>• Quarterly Network Scan</li> </ul>	<ul style="list-style-type: none"> <li>• Merchant OR QSA</li> <li>➢ Note: Effective 6/30/11, MasterCard requires SAQs to be completed by a PCI-DSS accredited in-house resource. Alternatively, Merchants can do an on-site audit with a QSA</li> <li>• Approved Scanning Vendor</li> </ul>
3	Any merchant processing 20,000 to 1,000,000 commerce transactions per year.	<ul style="list-style-type: none"> <li>• Annual PCI Self Assessment Questionnaire</li> <li>• Quarterly Network Scan</li> </ul>	<ul style="list-style-type: none"> <li>• Merchant</li> <li>• Approved Scanning Vendor</li> </ul>
4	Any merchant processing less than 20,000 e-commerce transactions per year, and all other merchants regardless of acceptance channel processing up to 1,000,000 Visa transactions per year.	<ul style="list-style-type: none"> <li>• Annual PCI Self Assessment Questionnaire</li> <li>• Quarterly Network Scan (if applicable)</li> </ul>	<ul style="list-style-type: none"> <li>• Merchant</li> <li>• Approved Scanning Vendor</li> </ul>

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

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

[http://usa.visa.com/merchants/risk\\_management/cisp\\_service\\_providers.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](http://www.visa.com/cisp)

MasterCard PCI-Compliant Service Providers

[www.mastercard.com/us/sdp/serviceproviders/index.html](http://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](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](https://www209.americanexpress.com/merchant/singlevoice/pdfs/en_US/DSOP_Service_Provider_US.pdf)

## 9. What is the PIN Transaction Security (PTS) 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 information on a set of standards and protocols published by the card brands. PCI SSC maintains the list of all PIN Transaction Security 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. To gain approval by PCI Security Standards Council, PIN transaction security must comply with the requirements and guidelines specified by the PCI SSC.

[https://www.pcisecuritystandards.org/security\\_standards/ped/pedapprovallist.html](https://www.pcisecuritystandards.org/security_standards/ped/pedapprovallist.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 Scanning 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](http://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](https://www.pcisecuritystandards.org/qa_asv/find_one.shtml)