PCI 101: Transaction Volumes and Validation Requirements

By Chip Ross
January 4, 2019

Regarding PCI compliance, all entities that store, process or transmit cardholder data are subject to the requirements of the PCI Data Security Standard (PCI DSS). Merchant or Service Provider Level, and how cardholder data is handled normally determine how an entity is required to validate compliance.

At the most basic level, any entity that interacts with cardholder data (CHD) is either a Merchant, or a Service Provider. At a high level, a Merchant is an entity that accepts CHD as payment for goods or services, and a Service Provider is an entity that stores, processes or transmits CHD on behalf of another entity, or provides some service that can affect the security of another entity's CHD. It is possible for an entity to be both a Merchant and a Service Provider.

Merchant Level is determined by:

1. The annual volume of transactions
    a. This is a count of individual transactions, for each card brand, not dollar amounts
2. What any card brand demands, if there has been a breach, or for any other reason
3. What any acquiring bank demands, if there has been a breach, or for any other reason

Service Provider Level is determined by:

1. The annual volume of transactions
    a. This is a count of individual transactions, for each card brand, not dollar amounts
2. What any card brand demands, if there has been a breach, or for any other reason

It is important to note that if a Merchant or Service Provider meets the annual transaction volumes for a particular level by one brand, the other brands usually consider them the same level. Additionally, the brands or banks can raise a Merchant or Service Provider Level at any time, for any reason, although this is very rarely done.

An entity may be required to validate their PCI compliance in a number of ways, including a Self-Assessment Questionnaire (SAQ) or by having an on-site assessment conducted by a QSA or an ISA (Internal Security Assessor – a certification that can be obtained through the PCI SSC) who produces a formal Report on Compliance (RoC). An Attestation of Compliance (AOC), a form which summarizes the assessment, is available for the RoC, and for each SAQ. Additionally, quarterly ASV scans (External vulnerability scans performed by a PCI Security Standards Council (PCI SSC) Approved Scanning Vendor) are normally required.

Below is a summary of the annual transaction volumes (a count of individual transactions, not dollar amounts) and corresponding levels and reporting requirements normally used for each card brand.

Merchants

Annual Transaction Volumes (a total of individual transactions, not a dollar amount)

Level	Visa	Amex	MasterCard	Discover	JCB
1	Over 6 million	Over 2.5 million	Over 6 million	Over 6 million	Over 1 million
2	1 – 6 million	50K – 2.5 million	1 – 6 million	1 – 6 million	Less than 1 million
3	20K – 1 million	Less than 50K	20K – 1 million	20K – 1 million	N/A
4	Under 20K	N/A	All others	All others	N/A

Annual Validation Requirements

Level	Visa	Amex	MasterCard	Discover	JCB
1	• RoC by QSA or company internal audit if signed by company officer • Quarterly ASV scans • AOC	• RoC by QSA or company internal audit if signed by either CEO, CFO, CISO, or principal • Quarterly ASV scans	• RoC by QSA or company internal ISA • Quarterly ASV scans	• RoC by QSA or company internal audit • Quarterly ASV scans	• RoC by QSA • Quarterly ASV scans
2	• SAQ • Quarterly ASV scans • AOC	• SAQ signed by either CEO, CFO, CISO, or principal • Quarterly ASV scans	• Optional RoC by QSA • SAQ by QSA or ISA • Quarterly ASV scans	• SAQ • Quarterly ASV scans	• SAQ • Quarterly ASV scans
3	• SAQ • Quarterly ASV scans • AOC	• SAQ* • Quarterly ASV scans*	• SAQ • Quarterly ASV scans	• SAQ • Quarterly ASV scans	N/A
4	Validation requirements set by acquiring bank • SAQ recommended • Quarterly ASV if applicable **VISA Europe Ecommerce:** • Use PCI compliant	N/A	Validation requirements set by acquiring bank	**Discover Merchants:** • SAQ **Acquired Merchants:** • Validation requirements set by acquiring bank Recommended: • SAQ • Quarterly ASV scans	N/A

	service provider OR • SAQ **VISA Europe** **Non e-commerce:** • SAQ • Quarterly ASV scans • AOC				

*Strongly recommended

Service Providers

Annual Transaction volumes (a total of individual transactions, not a dollar amount)

Level	Visa	Amex	MasterCard	Discover	JCB
1	Over 300K***	Over 2.5 million Any Service Provider AMEX deems a Level 1	All TPPs* All DSEs** over 300K All compromised TPPs and DSEs	Over 300K Any Service Provider Discover deems a Level 1	All TPPs*
2	Under 300K	50K – 2.5 million	All DSEs** under 300K	Under 300K	
3	N/A	Less than 50K	N/A	N/A	

*Third Party Processor – MasterCard and JCB have many different types of TPPs, depending on the provided services. More information is available at https://www.mastercard.com/us/sdp/assets/doc/PCI%20Action%20Plan%20-%20V2.0.doc and https://www.global.jcb/en/products/security/data-security-program/index.html
**Data Storage Entity – More information is available at https://globalrisk.mastercard.com/wp-content/uploads/2018/06/Service-Provider-Categories-and-PCI.pdf
***VISA Europe has some specific requirements for Visa System processors. More information is available at https://www.visaeurope.com/about-us/policy-and-regulation/veor

Annual Validation requirements

Level	Visa	Amex	MasterCard	Discover	JCB
1	• RoC by QSA** • Quarterly ASV scans • AOC • Included in Global Registry of Service Providers	• RoC by QSA or company internal audit if signed by either CEO, CFO, CISO, or principal • Quarterly ASV scans	• RoC by QSA • Quarterly ASV scans	• RoC by QSA • Quarterly ASV scans	• RoC by QSA • Quarterly ASV scans
2	• SAQ** • Quarterly ASV scans • Attestation of Compliance form •Not Included in Global Registry of Service Providers	• SAQ signed by either CEO, CFO, CISO, or principal • Quarterly ASV scans	• SAQ • Quarterly ASV scans • Non-compliant must submit a completed MasterCard Action plan	• SAQ • Quarterly ASV scans • Non-compliant must submit a completed Discover Action plan	
3	N/A	• SAQ* • Quarterly ASV scans*	N/A	N/A	

*Strongly recommended
**There are additional requirements for VISA Europe

As is shown above, Level 1 Merchants and Service Providers (and others as the brands or banks deem it so) are required to obtain a full Report on Compliance (RoC), completed by a QSA, ISA, or internal audit, depending on the card brand.

If an entity is not required to obtain a RoC, they may use a Self-Assessment Questionnaire (SAQ). How an entity handles CHD determines which SAQ is applicable. SAQ-A is very simple, with only 22 requirements, and SAQ-D is extensive, with 322 requirements. The others in between vary in number of requirements, but generally increase as they move from A to D. Please note that the only SAQ available for Service Providers is the SAQ-D.

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order), that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Not applicable to face-to-face channels.
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of cardholder data on merchant's systems or premises. *Applicable only to e-commerce channels.*
B	Merchants using only: • Imprint machines with no electronic cardholder data storage, and/or • Standalone, dial-out terminals with no electronic cardholder data storage. Not applicable to e-commerce channels.
B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor with no electronic cardholder data storage. Not applicable to e-commerce channels.
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based, virtual payment terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. Not applicable to e-commerce channels.
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. Not applicable to e-commerce channels.
P2PE	Merchants using only hardware payment terminals included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. Not applicable to e-commerce merchants.
D Merchants	SAQ D for Merchants: All merchants not included in descriptions for the above SAQ types.
D Service Providers	SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete an SAQ.