PCI DSS Information for Merchants and Service Providers

Maintaining payment security is required for all entities that store, process or transmit cardholder data.

	Level	Criteria	Attestation of Compliance - AOC Onsite assessment	Self-Assessment Questionnaire SAQ	Annual Report on Compliance - ROC (by QSA)	ASV Network Scan (for e-Commerce only)	Validate 3rd Party Payment Application
MERCHANT	1	• Any merchant, regardless of acceptance channel, processing **more than 6 million transactions per year.** • Any merchant that suffered a security breach, resulting in an account compromise.	Required Annually		Required Annually	Required Quarterly	Required*
	2	• Any merchant processing between 1 to 6 million transactions per year.		Required Annually		Required Quarterly	Required*
	3	• Any merchant processing between 20,000 to 1 million transactions per year.		Required Annually		Required Quarterly	Required*
	4	• **All other merchants** not in Levels 1, 2, or 3, regardless of acceptance channel.		Required Annually		Required Quarterly	Required*
SERVICE PROVIDER	1	• All processors and all payment gateways.	Required Annually		Required Annually	Required Quarterly	Required*
	2	• Any service provider that is Level 1 and stores, processes or transmits **more** than 300,000 transactions annually (across all their Acquirers).	Required Annually		Required Annually	Required Quarterly	Required*
	3	• Any service provider that is Level 2 and stores, processes or transmits **less** than 300,000 transactions annually (across all their Acquirers).		Required Annually		Required Quarterly	Required*

****Any merchant or service provider using third party payment applications are required to validate compliance or use an approved PCI DSS payment application - https://www.pcisecuritystandards.org/security_standards/vpa/***

** See page 2 for SAQ requirements

The PCI DSS self-assessment questionnaires (SAQs)

**The PCI DSS self-assessment questionnaires (SAQs) are validation tools intended to assist merchants report the results of their PCI DSS self-assessment. The different SAQ types are shown in the table below to help you identify which SAQ best applies to your organization. Detailed descriptions for each SAQ are provided within the applicable SAQ.

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS validated 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 any cardholder data on the 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 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.*
PSPE-HW	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
D	**SAQ D for Merchants**: All merchants not included in descriptions for the above SAQ types.
	SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete a SAQ.

Any merchant or service provider using third party payment applications are required to validate compliance or use an approved PCI DSS payment application - https://www.pcisecuritystandards.org/security_standards/vpa/

*** See page 2 for SAQ requirements*