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

Merchants

Merchants

Compliance validation details for merchants

Acquirers are responsible for ensuring that all of their merchants comply with the PCI Data Security Standard (DSS) requirements; however, merchant compliance validation has been prioritized based on the volume of transactions, the potential risk, and exposure introduced into the payment system.

PCI Compliance Acceleration Program

Visa developed the PCI Compliance Acceleration Program to provide financial incentives and establish enforcement provisions for acquirers to ensure their merchants validate PCI DSS compliance. In accordance with the PCI Compliance Acceleration Program, acquirers must additionally ensure that all Level 1 and 2 merchants validate that prohibited data is not retained by submitting a completed Prohibited Data Retention Attestation form ***OR*** Confirmation of Report Accuracy form to their acquirer.

The Merchant PCI DSS Compliance Update highlights compliance progress for level 1, 2 and 3 merchants.

On this page

Merchant levels defined

All merchants will fall into one of the four merchant levels based on Visa transaction volume over a 12-month period. Transaction volume is based on the aggregate number of Visa transactions (inclusive of credit, debit and prepaid) from a merchant Doing Business As ("DBA"). In cases where a merchant corporation has more than one DBA, Visa acquirers must consider the aggregate volume of transactions stored, processed or transmitted by the corporate entity to determine the validation level. If data is not aggregated, such that the corporate entity does not store, process or transmit cardholder data on behalf of multiple DBAs, acquirers will continue to consider the DBA's individual transaction volume to determine the validation level. Merchant levels are defined as:

Merchant Level*	Description
1	Merchants processing over 6 million Visa transactions annually (all channels) or global merchants identified as Level 1 by any Visa region** Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.
2	Any merchant-regardless of acceptance channel-processing 1,000,000 to 6,000,000 Visa transactions per year.
3	Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants-regardless of acceptance channel-processing up to 1,000,000 Visa transactions per year.

* Any merchant that has suffered a hack that resulted in an account data compromise may be escalated to a higher validation level.

** A merchant meeting Level 1 criteria in any Visa country/region that operates in more than one country/region is considered a global Level 1 merchant. Exceptions may apply to global merchants if no common infrastructure exists or if Visa data is not aggregated across borders; in such cases the merchant validates according to regional levels.

Back to top

Compliance validation basics

In addition to adhering to the PCI Data Security Standard, compliance validation is required for Level 1, Level 2, and Level 3 merchants, and may be required for Level 4 merchants.

Level	Validation Action	Validated By	Due Date
1	Annual On-site PCI Data Security Assessment • and Quarterly Network Scan	Qualified Security Assessor or Internal Audit if signed by Officer of the company Approved Scanning Vendor	9/30/04 New level 1 merchants have up to one year from identification to validate.
2	Annual PCI Self-Assessment Questionnaire • and Quarterly Network Scan	Merchant Approved Scanning Vendor	New level 2 merchants: 9/30/2007
3	Annual PCI Self-Assessment Questionnaire • and Quarterly Network Scan	Merchant Approved Scanning Vendor	6/30/05
4*	Annual PCI Self-Assessment Questionnaire • and Quarterly Network Scan (if applicable)	Merchant Approved Scanning Vendor	Validation requirements and dates are determined by the merchant's acquirer

*The PCI DSS requires that all merchants with externally-facing IP addresses perform external network scanning to achieve compliance. Acquirers may require submission of scan reports and/or questionnaires by level 4 merchants.

Back to top

Validation procedures and documentation

Acquirers must ensure that their merchants validate at the appropriate level and obtain the required compliance validation documentation from their merchants. Acquirers must submit monthly status reports to Visa and all compliance validation documentation must be made available to Visa upon request. Acquirers and merchants should also verify the compliance reporting requirements of other payment card brands which may require proof of compliance validation.

Compliance validation takes place at the merchant's expense, as follows:

- **Level 1 Merchants**

The ***Annual On-Site PCI Data Security Assessment*** must be completed for Level 1 merchants according to the **PCI Security Audit Procedures** document. This document is also to be used as the template for the **Report on Compliance**.

Level 1 merchants should engage a **Qualified Security Assessor** to complete the **Report on Compliance** and provide the report to their acquirer. Alternatively, acquirers may elect to accept the **Report on Compliance** from a Level 1 merchant, provided that a letter signed by a merchant officer accompanies the report. Level 1 merchants must also submit the **Confirmation of Report Accuracy** form completed by their assessor to their acquirers.

Acquirers must submit the **Confirmation of Report Accuracy** form and a letter accepting the merchant’s full compliance validation to Visa upon receipt and acceptance of the merchant’s validation documentation.

Download the PCI Security Audit Procedures.

Download the merchant Confirmation of Report Accuracy.

- **Level 2/Level 3 Merchants**

The ***Annual PCI Self-Assessment Questionnaire*** must be completed by Level 2 and 3 merchants. Level 4 merchants may be required to complete the PCI Self-Assessment Questionnaire as specified by their acquirer.

Download the PCI Self-Assessment Questionnaire.

Level 1/Level 2/Level 3 Merchants
The ***Quarterly Network Security Scan*** is an automated tool that checks systems for vulnerabilities. It conducts a non-intrusive scan to remotely review networks and Web applications based in the externally-facing Internet Protocol (IP) address provided by the merchant. Acquirers are responsible for ensuring that the quarterly network security scans required of their levels 1, 2, and 3 merchants are performed by an Approved Scanning Vendor. The ***Quarterly Network Security Scan*** is applicable to merchants with externally-facing IP addresses.

Download the PCI Security Scanning Procedures.

Back to top

For more information
To learn more about the Visa's compliance programs, contact Visa via email at AskVisaUSA@Visa.com.

- Printable page

Top Downloads

- Visa's Business Guide to Data Security
- PCI Data Security Standard
- Qualified Security Assessor List
- List of PCI DSS-Compliant Service Providers PDF | 180k
- View all CISP downloads
- Get Acrobat Reader from Adobe.com

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