Data Security Compliance Requirements for Service Providers

Compliance validation requirements for service providers

Both issuers and acquirers, and merchants must use service providers that are compliant with industry data security standards such as the Payment Card Industry Data Security Standard (PCI DSS), PCI PIN, Payment Application DSS (PA DSS) as well as any country specific security requirements. Although there may not be a direct contractual relationship between merchant service providers and merchant acquiring banks, Visa issuing and acquiring banks are responsible for any liability that may occur as a result of non-compliance.

To locate a validated service provider, visit the Visa Global Registry of Service Providers (the Registry).

Service provider registration

Service providers are organizations that store, process, transmit, or have access to Visa cardholder account or transaction information on behalf of Visa clients, merchants, or other service providers.

Service providers, or third party agents (TPA), must be registered in the Visa Third Party Agent Registration Program prior to inclusion on the Visa Global Registry of Service Providers.

All third party agents must be PCI compliant prior to beginning services in which they would have access to cardholder data.

For Third Party Agent registration requirements, please click here. For specific questions not covered in the TPA FAQ, email AgentRegistration@Visa.com.

PCI DSS compliance validation requirements

PCI DSS compliance validation is required every 12 months for all Level 1 and Level 2 service providers.

Service provider levels are defined as follows:

Level	Description
1	VisaNet processors or any service provider (TPA) that stores, processes and/or transmits over 300,000 Visa transactions per year
2*	Any service provider (TPA) that stores, processes and/or transmits less than 300,000 Visa transactions per year

In addition to adhering to the PCI DSS, compliance validation is required for all service providers.

Level	Validation Action	Validated By
1	Annual On-Site PCI Data Security Assessment Quarterly Network Scan	Qualified Security Assessor Approved Scanning Vendor
2	Annual PCI Self-Assessment Questionnaire (PCI DSS SAQ-D) Quarterly Network Scan	Service Provider Approved Scanning Vendor

Service Providers must demonstrate PCI DSS compliance and provide their compliance validation to Visa every 12 months.

Third Party Agents: Level 1 Service Providers not directly connected to Visa are required to complete the Annual On-Site PCI Data Security Assessment and submit an executed Attestation of Compliance (AOC), signed by both the Service Provider and the Qualified Security Assessor (QSA) to Visa. Visa reserves the right to request the full Report on Compliance (ROC). Level 2 Service Providers must

submit a signed Self-Assessment Questionnaire (SAQ-D) form or an AOC including QSA signature for revalidation.

* Visa will not review the contents of the SAQ-D as issuers and acquirers are responsible for reviewing the accuracy of the SAQ-D.

Visa Clients, VisaNet Processors (VNP): Client banks and processors directly connected to Visa must validate compliance by submitting the full ROC and the AOC signed by both parties. ROCs must be sent securely via PGP encryption. If PGP is not available, please contact Visa at pcirocs@visa.com to discuss an alternative submission method.

Qualified Security Assessors (QSAs) and service providers must submit only fully executed AOC forms, properly signed by the QSA and the third party agent confirming compliance with the PCI DSS. All materials must be sent to pcirocs@visa.com.

PCI DSS compliance and the Registry

For Level 1 service providers published on the Registry, if Visa does not receive the appropriate revalidation documents:

- Within 1 – 60 days upon expiry of the validation documents, the entity will be highlighted in Yellow on the Registry.
- Within 61 – 90 days upon expiry of the validation documents, the entity will be highlighted in Red on the Registry.
- After 90 days, the entity will be removed from the Registry.

Please note that Visa reserves the rights to remove any third party agent from the Registry at its discretion. Non-Compliance Assessments starts at $10,000 USD per TPA assessed to the Visa client.

For more information about the registration and PCI DSS compliance validation process, review TPA Registration Program FAQs or click here. For specific questions not covered in the FAQs, contact Visa via email at AgentRegistration@Visa.com.

Merchant Servicer (MS) PCI DSS compliance validation requirements

Merchant Servicer agents must submit PCI DSS compliance validation materials through the Merchant Servicer Self-Identification Program (MSSIP).

Additional Resources

PCI Data Security Standard

PCI DSS Qualified Security Assessor list

Visa PIN, AVP and ACS Security Assessor list

Visa's Global Registry of Service Providers

Third Party Agent Registration Program

Merchant Servicer Self-Identification Program

View all data security downloads

TPA Registration Program FAQs

PCI Security Standards Council Site

PCI Data Security Standard