Data Security Compliance Requirements for Service Providers

Compliance validation requirements for service providers

Issuers, 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 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, or transmit Visa cardholder account or transaction information on behalf of Visa clients, merchants, or other service providers. Service providers are categorized as either Third Party Agents (no direct connection to VisaNet) or VisaNet Processors (directly connected to VisaNet).

Service providers must be registered in the Visa Agent Registration Program prior to inclusion on the Visa Global Registry of Service Providers.

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

- AP/CEMEA: Agents@visa.com
- LAC: AgentRegistrationLAC@visa.com
- NA: AgentRegistration@visa.com

PCI DSS compliance validation requirements

All service providers who have access to cardholder data must comply with the required data security requirements prior to beginning services.

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	Any service provider that stores, processes and/or transmits 300,000 or more Visa accounts/transactions per year
2	Any service provider that stores, processes and/or transmits less than 300,000 Visa accounts/transactions per year

Category	Validation Action	Level 1	Level 2
Third Party Agent	An entity, not defined as a VisaNet Processor, that provides payment-related services, directly or indirectly, to a Visa client and/or stores, transmits, or processes Cardholder data.	Attestation of Compliance (AOC) by a PCI QSA every 12 months. Visa reserves the right to request the full Report on Compliance (ROC).	Attestation of Compliance for Self-Assessment Questionnaire D (AOC SAQ-D) every 12 months
Third Party VNP	Non-Visa client entities that provide issuer and/or acquirer card processing services to Visa clients, merchants,	AOC and full ROC by PCI QSA every 12 months and for new connection requests	

	agents and/or other service providers.		
Visa Client VNP acting as Service Provider	Visa clients that provide issuer and/or acquirer card processing services to other Visa clients, and/or merchants of other Visa clients.	AOC and full ROC by PCI QSA every 12 months and for new connection requests	
Visa Client Acquiring VNP	Visa acquirers that process transactions for their merchants, or provides cash disbursement to a cardholder. This group includes any sponsored (associate) clients and entities with the same parent company.	AOC and full ROC by PCI QSA for new connection requests. AOC and full ROC by PCI QSA or PCI Internal Security Assessor (ISA) every 12 months.	AOC and full ROC by PCI QSA for new connection requests. AOC SAQ-D every 12 months.
Visa Client Issuing VNP	Visa clients that only store, process, and/or transmit their own cardholder data. This group includes any sponsored (associate) clients and entities with the same parent company.	For new connection requests and upon request by Visa, one of the following: •AOC and full ROC by PCI QSA •AOC and full ROC by PCI ISA •SAQ-D by senior executive (e.g. CISO, Head of IT or Risk)	

PCI DSS compliance document submission

Clients, VisaNet Processors and Third Party Agents may submit the fully executed AOC and ROC, if applicable, directly to Visa, or may designate their Qualified Security Assessors (QSAs) to submit on their behalf. ROCs must be sent securely via PGP encryption or other secure methods (for AP/CEMEA). For document submission or any inquiries, please contact:

- NA/LAC: pcirocs@visa.com
- AP/CEMEA: pciagents@visa.com

PCI DSS compliance and the Registry

For any 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 service provider from the Registry at its discretion. Visa Clients engaging any service providers that are not compliant to PCI DSS may be liable for non-compliance assessments starting at $10,000 USD per service provider.

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
TPA Registration Program FAQs
PCI Security Standards Council Site