

Visa USA Cardholder Information Security Program (CISP)

Compliance and Validation



CISP Compliance Validation

Separate from the mandate to comply with the CISP requirements is the **validation** of compliance. Validation identifies vulnerabilities and ensures that appropriate levels of cardholder information security are maintained. Visa has prioritized and defined levels of CISP compliance validation based on the volume of transactions, the potential risk, and exposure introduced into the Visa system by merchants and service providers.

Some merchants and service providers validate compliance through an *Annual On-Site PCI Security Audit* and *Quarterly Network Scan*, while others complete an *Annual Self-Assessment Questionnaire* and *Quarterly Network Scan*. Issuers and acquirers must also ensure that all of their third-party service providers are CISP-compliant, as well as those used by their merchants.

For Merchants . . .

Merchants who store, process, or transmit Visa cardholder data will fall into one of four merchant levels based on Visa transaction volume over a 12-month period. Transaction volume is based on the aggregate number of Visa transactions from a merchant Doing Business As (DBA).

MERCHANT LEVEL	DESCRIPTION
1	<ul style="list-style-type: none"> Any merchant, regardless of acceptance channel, processing over 6,000,000 Visa transactions per year. Any merchant that has suffered a breach that resulted in an account data compromise. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system. Any merchant identified by any other payment card brand as Level 1.
2	Any merchant 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 less than 20,000 Visa e-commerce transactions per year, and all other merchants processing up to 1,000,000 Visa transactions per year.

For Service Providers . . .

Service providers that process, store, or transmit Visa cardholder data on behalf of Visa members, merchants, or other service providers will fall into one of three service provider levels.

SERVICE PROVIDER LEVEL	DESCRIPTION
1	All VisaNet® processors (member and nonmember) and all payment gateways.
2	Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 Visa accounts/transactions annually.
3	Any service provider that is not in Level 1 and stores, processes, or transmits less than 1,000,000 Visa accounts/transactions annually.

In addition to their CISP compliance validation, a service provider must also be registered as a member bank with Visa.

Group	Level	COMPLIANCE ACTIONS	VALIDATION ACTIONS		
		Comply with PCI Data Security Standards	On-Site PCI Security Audit	Self-Assessment Questionnaire	Network Scan
Merchant	1	Required	Required Annually		Required Quarterly
	2 & 3	Required		Required Annually	Required Quarterly
	4	Required		Recommended Annually	Recommended Quarterly
Service Provider	1	Required	Required Annually		Required Quarterly
	2	Required	Required Annually		Required Quarterly
	3	Required		Required Annually	Required Quarterly

What To Do If Compromised

In the event of a security incident, members, merchants, and service providers must take immediate action to investigate the incident, limit the exposure of cardholder data, notify Visa, and report investigation findings. The *CISP What To Do If Compromised* guide, which can be found on the CISP web site at www.visa.com/cisp, contains step-by-step guidelines to assist members, merchants, and service providers through a security incident.