Visa USA Cardholder Information Security Program (CISP)

Overview

*The **Payment Card Industry (PCI) Data Security Standard** is a result of a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. These 12 requirements are the foundation of Visa's CISP.*

PCI Data Security Standard

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

For More Information

*A detailed description of the Visa CISP compliance validation procedures for merchants and service providers can be found at **www.visa.com/CISP**.*

Every piece of cardholder account information that passes through the Visa payment system is vital to our business operation. However, without proper safeguards in place, this information can be extremely vulnerable to internal and external compromise(s), which can often lead to fraud and identity theft. Visa's *Cardholder Information Security Program (CISP)* ensures the highest standard of due care to help keep sensitive cardholder data safe from hackers and fraudsters.

About the Program

WHAT

Visa's CISP is a critical component to minimize risk and maximize protection. Mandated since June 2001, this robust program is intended to protect Visa cardholder data—wherever it resides.

WHO

All Members must be CISP-compliant and are responsible for ensuring the compliance of their merchants and service providers. The program applies to all payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce.

HOW

To achieve CISP compliance, all Members, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard, which offers a single approach to safeguarding sensitive data for all card brands.

CISP compliance validation identifies and corrects vulnerabilities by ensuring appropriate levels of cardholder data security are maintained.

WHY

By complying with CISP requirements, Visa Members, merchants, and service providers not only meet their obligations to the Visa payment system, but also build a culture of security that benefits all parties.

Everyone	■ Limited risk ■ More confidence in the payment industry
Member	■ Protected reputation
Merchant & Service Provider	■ Competitive edge gained ■ Increased revenue and improved bottom line ■ Positive image maintained ■ Customers are protected
Industry	■ "Good security neighbors" encouraged ■ Information is safeguarded
Consumer	■ Identity theft prevention

Visa USA Cardholder Information Security Program (CISP)

Compliance and Validation

CISP Compliance Validation

Separate and distinct from the mandate to comply with CISP requirements is the validation of compliance. It is a critical function that identifies and corrects vulnerabilities by ensuring 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 Security Audit* and *Quarterly Network Scan*, while others complete an *Annual Self-Assessment Questionnaire* and the scan. Issuers and Acquirers must also identify and review the list of all third-party service providers that they use or that are used by their merchants and ensure they are CISP-compliant.

FOR MERCHANTS...

There are four levels of merchant CISP compliance validation.

MERCHANT LEVEL	DESCRIPTION
1	■ 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 150,000 to 6,000,000 Visa e-commerce transactions per year.
3	Any merchant processing 20,000 to 150,000 Visa e-commerce transactions per year.
4	All other merchants not in Levels 1, 2, or 3, regardless of acceptance channel.

FOR SERVICE PROVIDERS...

For service providers that process, store, or transmit Visa cardholder data on behalf of Visa Members, merchants, or other service providers, there are three levels of compliance validation.

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 responsibilities, a service provider must also be registered as an Agent with a sponsoring Visa Member.

		COMPLIANCE ACTIONS	VALIDATION ACTIONS		
Group	**Level**	**Comply with PCI Data Security Standards**	**On-Site 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 Annually
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, contains step-by-step guidelines to assist Members, merchants, and service providers through a security incident.