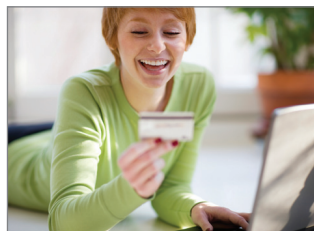# Visa PCI DSS Data Security Compliance Program

Overview

The **Payment Card Industry Data Security Standard (PCI DSS)** is a comprehensive set of international security requirements for protecting cardholder data. The PCI DSS was developed by Visa and the founding payment brands of the PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures on a global basis.

These 12 requirements are the foundation of Visa's data security compliance program known as the *Account Information Security (AIS) Program*. This program was formerly known as the *Cardholder Information Security Program (CISP)* in the U.S.

Payment Card Industry Data Security Standard (PCI DSS)

- **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 cardholder data
    4. Encrypt transmission of cardholder data and sensitive information across open 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

Every piece of cardholder account information that passes through the Visa payment system is vital to our business. Without proper safeguards in place, this information can be vulnerable to internal and external compromise, leading to fraud and loss of consumer confidence. The goal of Visa's security programs is to ensure the highest standard of due diligence to protect sensitive cardholder data from hackers and fraudsters.

About the Program

What is PCI DSS?

The PCI DSS protects Visa cardholder data wherever it resides.

Who Needs to Comply?

All Visa acquirers and issuers must comply, and must also ensure the compliance of their merchants and service providers who store, process, or transmit Visa account numbers. This program applies to all payment channels including card present, mail/telephone order, and e-commerce.

How Does it Work?

To achieve PCI DSS compliance, all Visa acquirers, issuers, merchants and service providers must adhere to the PCI DSS requirements set forth by the PCI Security Standards Council, which offers a single approach to safeguarding sensitive data for all card brands. Businesses may also be required to validate PCI DSS compliance in accordance with payment card brand requirements.

Why is it Important?

By complying with the PCI DSS, entities can protect their business and their customers while building a culture of security that benefits all parties in the payment system.

What To Do If Compromised

In the event of a security incident, Visa acquirers, issuers, merchants, and service providers must take immediate action to investigate the incident, limit the exposure of cardholder data, notify Visa, and report investigation findings. Visa's What To Do If Compromised guide, which can be found online at www.visa.com/cisp, contains step-by-step guidelines to assist clients, merchants, and service providers through a security incident.

For More Information

A detailed description of Visa's payment system security compliance programs including PCI DSS compliance and validation requirements, payment application security mandates, and PIN security and key management requirements can be found at *www.visa.com/CISP*. In addition, Visa publishes data security alerts, bulletins and webinar presentations; all are available for download.

PCI DSS Compliance Validation

Separate from the mandate to comply with PCI DSS is the validation of compliance. Validation identifies vulnerabilities and ensures that appropriate levels of cardholder information security are maintained. Visa has prioritized and defined validation levels based on the volume of transactions and the potential risk and exposure introduced into the Visa system.

Some businesses validate compliance through an *Annual On-Site Security Assessment* and *Quarterly Network Vulnerability Scan;* others complete an *Annual Self-Assessment Questionnaire* and *Quarterly Network Vulnerability Scan.*

Acquirers and Issuers

All Visa acquirers and issuers must comply with the PCI DSS and will be advised by Visa of applicable validation requirements. At minimum, acquirers are responsible for ensuring the compliance and validation of their merchants. Issuers and acquirers must also ensure that their Third Party Agents—and the Third Party Agents used by their merchants—are registered with Visa and are PCI DSS compliant.

Merchants

Merchants who store, process, or transmit Visa cardholder data generally 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 (inclusive of credit, debit and prepaid) from a merchant Doing Business As (DBA).

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.
2	Merchants processing 1 million to 6 million Visa transactions annually (all channels).
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually.
4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually.

Service Providers

Service providers that store, process or transmit Visa cardholder data on behalf of Visa acquirers, issuers, merchants or other service providers fall into one of two service provider levels. Level 2 service providers are not posted on Visa's list of compliant services providers unless they opt to undergo a Level 1 onsite security assessment.

SERVICE PROVIDER LEVEL	DESCRIPTION	POSTED ON VISA'S GLOBAL LIST OF VALIDATED SERVICE PROVIDERS
1	VisaNet® processors or any service provider that stores, processes and/or transmits over 300,000 Visa transactions annually.	Yes
2*	Any service provider that stores, processes and/or transmits less than 300,000 Visa transactions annually.	No*

* Level 2 service providers may choose to validate as a Level 1 service provider in order to be listed on Visa's Global List of Validated Service Providers.

Visa acquirers and issuers must also register all Third Party Agents with Visa. Registration of Third Party Agents can be accomplished through the Visa Membership Management application (VMM), which is accessible through Visa Online (*www.us.visaonline.com*)

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

*Network scanning is applicable to any internet facing system. ** Validation requirements are determined by the merchant's acquirer.

Payment Application Security

The PCI Payment Application Data Security Standard (PA-DSS), developed to create security standards for payment application vendors, mitigates the risk of compromises through vulnerable payment applications, prevents storage of sensitive authentication data (i.e., full magnetic-stripe data, CVV2 and PIN data) and supports overall compliance with the PCI DSS. Visa developed a series of payment application mandates that require acquirers to ensure that their merchants and service providers do not use vulnerable payment applications known to retain sensitive authentication data and also ensure the use of PCI PA-DSS compliant applications. Details on these mandates are available at *www.visa.com/CISP*.