VISA DATA SECURITY PROGRAM
KEEPING CARDHOLDER DATA SAFE

12 STEPS TO KEEP YOUR BUSINESS SAFE

Providing customers with a safe, reliable transactions network is a priority your business shares with the entire global payments industry. The threat of data piracy is real, and simple procedures can and must be taken to anticipate it — and to spot crimes quickly when thieves momentarily succeed.

To help, Visa joined with other founding members of the PCS Security Standards Council to create the Payment Card Industry Data Security Standard, an industry standard for companies worldwide. All Visa acquirers and issuers must comply with the Standard, and also ensure that their merchants and service providers — everyone storing, processing, or transmitting Visa account numbers — do the same.

Following these 12 steps will ensure transactions are conducted with confidence and ease, worldwide.

IF YOUR SYSTEM IS COMPROMISED

Act swiftly if a security breach occurs. Notify Visa, investigate, and report what you learn. Our online guide can assist clients, merchants, and service providers through every step of the process. Go to www.visa.com/cisp to learn more.

FOR MORE INFORMATION

More detailed information on Visa's security compliance program is available at www.visa.com/cisp. Learn about complying with the Standard, validation requirements, PIN security and key management, and more. Plus, stay current with data security by accessing alerts, bulletins, and webinars.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

Commit to these steps in order to ensure compliance with the industry's recommended practices.

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

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.

VALIDATING YOUR COMPLIANCE

Validation with PCI DSS is highly important. It certifies that cardholder data is being safely handled at your location and reveals any weaknesses to be addressed.

Visa has created four validation levels tied to transaction volume and the level of risk posed, each requiring different steps. Level 1 is the highest.

Businesses validate their compliance either through an Annual On-Site Security Assessment or an Annual Self-Assessment Questionnaire. Both also require a Network Vulnerability Scan to be conducted once every quarter, if it is applicable.

Effective 1 October 2012, Visa's Technology Innovation Program (TIP) rewards U.S. merchants that have invested in EMV technology by eliminating the PCI DSS validation requirement for any year in which at least 75 percent of the eligible merchant's Visa transactions originate from dual-interface EMV chip-enabled terminals. Learn more at visa.com/cisp.

FOR ACQUIRERS AND ISSUERS

At a minimum, acquirers are responsible for ensuring that their merchants comply with PCI DSS, and receive appropriate validation. Issuers need to join with them to make sure that Third Party Agents — as well as those used by their merchants — are registered with Visa and complying with the Standard.

FOR MERCHANTS

The number of steps necessary for validation is determined by a merchant's total transaction volume over a 12-month period. Use this chart to determine your level.

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.

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).

		COMPLIANCE ACTIONS	VALIDATION ACTIONS		
GROUP	LEVEL	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 Annually	Required Quarterly
Service Providers	1	Required	Required Annually		Required Quarterly
	2	Required		Required Annually	Required Quarterly

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

FOR SERVICE PROVIDERS

Service providers that store, process, or transmit cardholder data on behalf of acquirers, issuers, and merchants are categorized into one of two levels, defined by their number of annual Visa transactions. Those grouped in Level 1 — signifying 300,000 or more such transactions — are listed on Visa's Global Registry of Service Providers. Level 2 providers can join the list by undergoing a Level 1 Annual Onsite Security Assessment.

SERVICE PROVIDER LEVEL	DESCRIPTION	POSTED ON VISA'S GLOBAL REGISTRY OF 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 Registry of Service Providers.

ANOTHER WAY TO KEEP DATA SAFE

The PCI Payment Application Data Security Standard (PA-DSS) applies to payment application vendors. It is intended to lessen the risk of security breaches in payment applications, prevent storage of sensitive authentication data (i.e., full magnetic-stripe data, CVV2, and PIN data), and support overall compliance with PCI DSS.

Visa's policies are intended to support these standards by ensuring our merchants and service providers do not use payment applications that retain data, thereby making it easier to steal. For those doing business with Visa, that means using applications found to comply with this important data standard. To learn more about what is required, go to www.visa.com/cisp.

Secure technologies such as point-to-point encryption and tokenization, when implemented in accordance with the PCI DSS, may help simplify PCI DSS compliance. Go to www.pcissc.org for guidelines on these technologies.