

Payment Card Industry Data Security Standards (PCI DSS)

DO I HAVE TO COMPLY WITH PCI (PREVIOUSLY KNOWN AS CISP AND SDP)?

Yes, this program is mandatory for all merchants that store, process or transmit through Visa® and MasterCard®.

WHAT HAPPENS IF I DON'T COMPLY WITH THESE STANDARDS?

You could face fines ranging from \$2,000 to \$500,000 and be financially responsible for all fraud transactions that take place on cards compromised at your location.

WHAT IS THE DIFFERENCE BETWEEN COMPLIANCE AND VALIDATION?

Merchants are compliant when they are abiding by the new security standards. Compliance is required for merchants of all 4 levels. Validation is the process confirming that a merchant is abiding by the new security standards. To become validated, you must complete a Self Assessment Questionnaire and perform a Quarterly Network Scan on your system to detect potential vulnerabilities. Currently, Visa and MasterCard only require merchants in Levels 1 - 3 to be validated. However, Level 4 merchants still must be in compliance and are encouraged to validate.

WHAT IS A DATA COMPROMISE?

Data compromise is an incident involving the electronic or physical breach of cardholder data through the communication and/or information processing of the merchant/third party. Electronic breaches include data vulnerability in transit and storage, attacks via web sites or servers, private key mismanagement, access related to user ID or password, and administrative network performance problems. Physical breaches include theft of documents or equipment such as receipts, files, PCs, or POS terminals.

HOW DO VISA® AND MASTERCARD® DEFINE CARDHOLDER DATA?

Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, etc. The account number is the critical component that makes PCI applicable. All personally identifiable information associated with the cardholder that is stored, processed, or transmitted is also considered cardholder data. However, PCI applies even if the only data stored, processed, or transmitted is account numbers.

WHEN IS IT ACCEPTABLE TO STORE MAGNETIC STRIPE DATA?

It is never acceptable for [acquirers](#), merchants, or service providers to retain magnetic stripe data subsequent to transaction authorization. The Visa & MasterCard Operating Regulations prohibit storage of the contents of the magnetic stripe as a unit. Cardholder name, account number, and expiration date may be retained subsequent to transaction authorization, however the data must be encrypted.

WHEN IS IT ACCEPTABLE TO STORE [CVV2](#) & [CVC2](#)?

It is never acceptable for acquirers, merchants, or service providers to retain CVV2 & CVC2, which consists of the last three digits printed on the signature panel of all Visa & MasterCard cards, subsequent to transaction authorization. The Visa & MasterCard Operating Regulations prohibit such storage, whether encrypted or unencrypted.

WHERE CAN I FIND THE SELF-ASSESSMENT QUESTIONNAIRE?

The Self-Assessment Questionnaire is available on www.visa.com/cisp. Many of the qualified security assessors offer merchants and service providers the option to complete the Compliance Questionnaire on the security assessor's Web site.

WHAT IS A NETWORK SECURITY SCAN?

A network security scan involves an automated tool that checks a merchant or service provider's systems for vulnerabilities. The tool conducts a non-intrusive scan to remotely review networks and Web applications based on the external-facing Internet protocol (IP) addresses provided by the merchant or service provider. The scan will identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network. As provided by qualified security assessors, the tool will not require the merchant or service provider to install any software on their systems, and no denial-of-service attacks will be performed.

IS THE NETWORK SECURITY SCAN ONLY APPLICABLE TO E-COMMERCE ENTITIES?

No. The system perimeter scan is applicable to all merchants and service providers with external-facing IP addresses. Even if an entity does not offer Web-based transactions, there are other services that make systems Internet accessible. Basic functions such as email and employee Internet access will result in the Internet-accessibility of a company's network. These seemingly insignificant paths to and from the Internet can provide unprotected pathways into merchant and service provider systems if not properly controlled. Merchants and service providers without any external-facing IP addresses are only required to complete the Report On Compliance (ROC) or the Compliance Questionnaire, as appropriate.

WHAT ARE THE COMPLIANCE VALIDATION REPORTING REQUIREMENTS FOR MERCHANTS?

Merchants will provide compliance validation documentation to their acquirer(s). Though the compliance validation process is aligned for merchants, acquirers must follow each payment card company's respective reporting requirements to ensure that a merchant's status is appropriately filed with each.

HOW IS THE TRANSACTION VOLUME THAT DETERMINES A MERCHANT'S COMPLIANCE LEVEL MEASURED?

The number of transactions will be determined based on the gross number of Visa transactions processed by a DBA or a chain store—not of a corporation that owns several chains. For all levels, if a merchant meets the compliance validation criteria based on Visa OR MasterCard transaction volume, they must comply with the Payment Card Industry Data Security Standards (PCI DSS) requirements.

WHAT IS AN IP-BASED POS ENVIRONMENT?

The point-of-sale (POS) environment is the environment in which a transaction takes place at a merchant location (e.g. retail store, restaurant, hotel property, gas station, supermarket, or other point-of-sale location). An IP-based POS environment is one in which transactions are stored, processed, or transmitted on IP-based systems, or systems communicating via TCP/IP.

DO MERCHANTS NEED TO INCLUDE THEIR SERVICE PROVIDERS IN THE SCOPE OF THEIR PCI REVIEW?

No. Service providers are responsible for validating their own compliance with PCI independent of their customers. Visa and MasterCard will work with service providers to validate their compliance with PCI.