

Chase Paymentech ALERT

What Every Merchant Needs to Know About Consumer Card Data Security

Your customers want assurance that their credit card account information is safe. But offering them a safe and secure way to pay is more than just a good business practice – it's a requirement. Every merchant who handles credit card account information is responsible for safeguarding that information and can be held liable for security compromises. Non-compliance fines can cost thousands of dollars. The Payment Card Industry Data Security Standard (PCI DSS) is intended to protect cardholder data – wherever it resides – ensuring that banks, merchants and service providers maintain the highest information security levels.

PCI DSS applies to all Members (financial institutions), merchants and service providers (a third party who provides payment-related services to merchants) that store, process or transmit cardholder data. These security requirements apply to all "system components," which are defined as any network component, server or application included in, or connected to, the cardholder environment. Network components include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances and other security appliances. Servers include, but are not limited to, Web, database, authentication, DNS, mail, proxy and NTP. Applications include all purchased and custom applications, including internal and external (Web) applications.

Does this apply to me?

If your business stores, processes, or transmits cardholder data, PCI DSS applies to you.

Why do I have to go through the compliance process?

The simple answer is to avoid potential fines that the card brands may levy. The more important reason is to protect your customers' confidential information and to safeguard your valuable business reputation. The card brands have set fine schedules for companies that are not compliant with the security programs. Fines cost up to \$50,000 per month and/or egregious fines of up to \$500,000.

In addition, you could have your processing privileges restricted or terminated for non-compliance. Even more important, in the long run, non-compliance puts your customers' trust and loyalty at risk. Many consumers are becoming more and more aware of security relating to their personal information. Your compliance demonstrates that you are protecting your customers' personal data. A breach in security may cause irreparable damage to the relationships you have built with your customers and ultimately have a negative impact to your bottom line. Is that a risk you are willing to take?

How do I ensure my company is compliant?

To learn more about the card brands' PCI data security requirements, visit Chase Paymentech's Card Brand Data Security information page at: www.chasepaymentech.ca, under "Merchant Support;" "PCI Data Security Standards." For more information about a specific payment brand, visit the brand's Web site.

How do I ensure my equipment and payment applications are compliant?

Merchants are strongly encouraged to use compliant equipment and/or compliant payment applications. For a list of compliant payment applications, visit the PCI Security Standards Council web site: www.pcisecuritystandards.org, click on "Security Standards" and review the documents listed under "PCI DSS," "PTS," and "PA-DSS." As a Service Provider, Chase Paymentech only provides validated hardware to merchants.

How do I ensure my Service Providers are compliant?

Any Service Provider with whom you share or exchange cardholder data is required to be compliant with the PCI DSS. All Service Providers must also be registered with Visa and MasterCard. For a list of compliant service providers, for both Visa and MasterCard, visit:

Visa: <http://www.visa.ca/en/merchant/fraud-prevention/account-information-security/index.jsp>

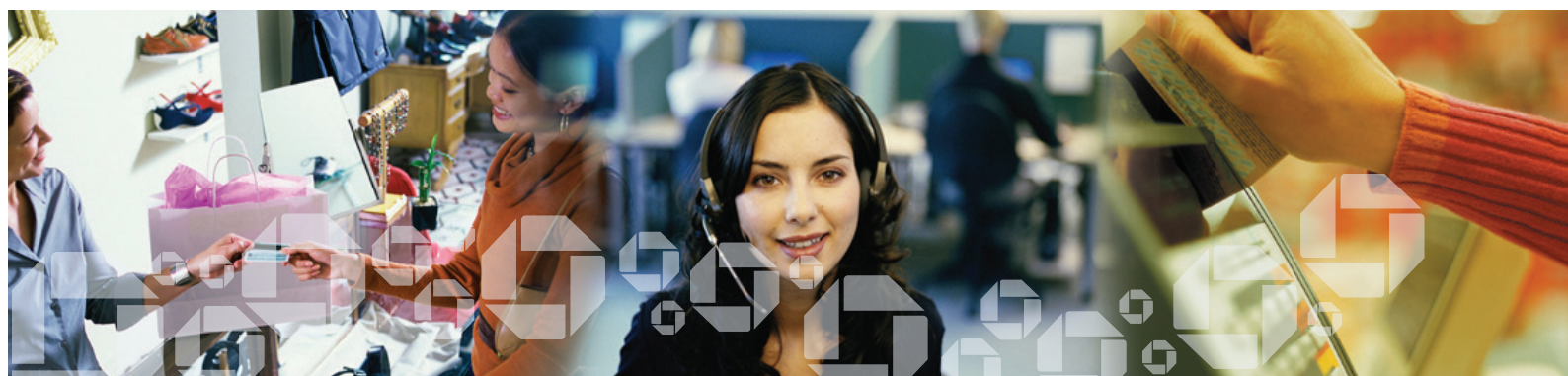
MasterCard: http://www.mastercard.com/us/sdp/serviceproviders/compliant_serviceprovider.html

Is Chase Paymentech compliant?

Yes. PCI DSS compliance is a top priority for Chase Paymentech. Since its inception in 2007, Chase Paymentech has served on the PCI Security Standard Council (PCI SSC) Board of Advisors. The Board of Advisors plays a key role in driving Council strategy and helping to craft the security standard as it goes forward.

Once I become compliant, how long am I considered compliant?

All merchants are required to maintain compliance at all times. Submission of your compliance validation is required annually if you are a Level 1, 2 or 3 merchant.



What are the compliance deadlines?

Compliance validation deadlines vary by card brand and the number of credit card transactions your business processes.

Note: Visa and MasterCard designate U.S. merchant levels 1-4, based on the number of transactions your business processes. Visa Europe, other Visa regions, American Express and other payment brands have different criteria to determine merchant levels and deadlines

Please reference the table below for U.S. and Canadian merchants processing Visa and MasterCard:

VISA Inc./MasterCard International	Validation Actions		
	Merchant Level Criteria	On Site Security Assessment	Self-Assessment Questionnaire
Level 1¹ 6+ million transactions annually across all acceptance channels within one card brand.	Report on Compliance (ROC) (submitted to Acquirer Annually)	Not Applicable	Required Quarterly
Level 2² 1 million to 6 million transactions annually across all acceptance channels within one card brand.	Not Applicable	Submitted to Acquirer Annually	Required Quarterly
Level 3 20,000 to 1 million e-commerce transactions annually within one card brand.	Not Applicable	Submitted to Acquirer Annually	Required Quarterly
Level 4 Less than 20,000 e-commerce and less than 1 million total transactions annually across all acceptance channels within one card brand.	Not Applicable	Required Annually (submission to acquirer not mandatory)	Required Quarterly (submission to acquirer not mandatory)

¹For MasterCard: Effective June 30, 2011, Level 1 merchants that choose to conduct an annual onsite assessment using an internal auditor must ensure that primary internal auditor staff engaged in validating PCI DSS compliance attend PCI SSC-offered ISA training and pass the PCI SSC ISA accreditation program annually in order to continue to use internal auditors.

²For MasterCard: Effective June 30, 2011, Level 2 merchants that choose to complete an annual self-assessment questionnaire must ensure that staff engaged in the self-assessment attend PCI SSC-offered ISA training and pass the PCI SSC ISA accreditation program annually in order to continue the option of self-assessment for compliance validation. Alternatively, Level 2 merchants may, at their own discretion, complete an annual onsite assessment conducted by a PCI SSC approved QSA rather than complete an annual self-assessment questionnaire.



Understanding PCI Data Security Standard

PCI DSS contains 12 requirement categories that are grouped under six general headings. The complete list of standards is available for download from the PCI Security Standards Council's Web sites (www.pcisecuritystandards.org); however the six general headings and 12 requirements are:

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect data.

Requirement 2: Do not use vendor-supplied defaults for system passwords and security parameters.

Protect Cardholder Data

Requirement 3: Protect stored data.

Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks.

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software.

Requirement 6: Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

Requirement 7: Restrict access to data by business need-to-know.

Requirement 8: Assign a unique ID to each person with computer access.

Requirement 9: Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

Requirement 11: Regularly test security systems and processes.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security.

PCI SSC also provides a "Prioritized Approach" guide and worksheet to assist merchants in identifying and prioritizing their PCI DSS implementation efforts to help expedite the process in an effort to reduce risk to card holder data as quickly as possible. The tool groups together the requirements of PCI DSS 1.2 into six key milestones for merchants to consider in their card data security strategy. These documents can be found on the PCI SSC Web site by visiting:

<https://www.pcisecuritystandards.org/education/prioritized.shtml>

Validating Your Compliance

As your partner, Chase Paymentech is here to help ensure that you are fully informed about the data security requirements and actions you are required to take for compliance. We are prepared to offer support while you work toward completing your requirements as quickly and easily as possible; however, we recognize that navigating the compliance process can be challenging. To help you manage the process of becoming compliant, we have arranged preferential pricing with Trustwave (www.trustwave.com), a firm that specializes in data security and compliance services for Chase Paymentech merchants. In partnership with Chase Paymentech, Trustwave is offering our merchants a reduced rate for data security compliance services.

Trustwave's compliance solution is a simple, cost-effective method for validating compliance with the PCI DSS for all the major card companies' security programs, including:

- American Express Data Security Operating Policy (DSOP)
- Discover Information Security and Compliance (DISC)
- MasterCard Site Data Protection (SDP)
- Visa Canada Account Information (AIS)
- Visa USA Cardholder Information Security Program (CISP)

Your steps to becoming compliant through Chase Paymentech's program with Trustwave may include an online self-assessment, vulnerability scanning and remediation (if necessary), as well as ongoing compliance maintenance. If you would like to take advantage of this special opportunity from Chase Paymentech and Trustwave, simply go to <http://chasecanada.riskprofiler.net>, and enter CHASECANADA08TKR in the enrollment code field under "Are you at risk?"

Helpful Terms and Definitions

Acquirer

Entity, such as Chase Paymentech, that contracts with merchants to facilitate customer payment transactions with multiple payment brands like Visa® and MasterCard®.

AIS

Visa Canada's Cardholder Information Security Program which specifies data security requirements for safeguarding personal cardholder information.

Cardholder

The customer to whom a payment card has been issued, or the individual authorized to use the card.

Cardholder Data

All personally-identifiable data about the cardholder and relationship to the Merchant (i.e., account number, expiration date, data provided by the merchant, other electronic data gathered by the merchant/agent, customer address, telephone number, etc.).

CISP

Visa's Cardholder Information Security Program which specifies data security requirements for safeguarding personal cardholder information.

Compliance

Operating within the requirements of the relevant card company standards.

Compromise

An intrusion into a computer system or theft of data where unauthorized disclosure, modification or destruction of cardholder data may have occurred.

Encryption

Conversion of information into a form unintelligible to anyone except holders of a specific cryptographic key.

FTC Tutorial

"Protecting Personal Information: A Guide for Business," from the Federal Trade Commission, alerts businesses and other organizations to practical, and low- or no-cost ways to keep data secure.

Magnetic Stripe Data (Full Track Data)

Data encoded in the magnetic stripe used for authorization during a card present transaction. Entities may not retain full magnetic stripe data subsequent to transaction authorization. Specifically, subsequent to authorization, service codes, discretionary data/CVV and Visa reserved values must be purged; however, account number, expiration date and name may be extracted and retained.

Payment Application Data Security Standard (PA-DSS)

Formerly requirements under Visa's Payment Applications Best Practices (PABP) for developing secure payment applications. This program is administered by the PCI Security Standards Council (PCI-SSC) to provide uniform guidance to developers ensuring PCI DSS compliant features are being incorporated into payment applications.

Helpful Terms and Definitions

PABP

Visa developed the "Payment Application Best Practices" program to assist software vendors in creating secure payment applications that foster merchant compliance with the PCI Data Security Standard.

Payment Card Industry Data Security Standard (PCI-DSS)

Multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures which are required by the card brands' cardholder data security programs (i.e., CISP, SDP, etc.). The complete standards are available for download from the Payment Card Industry Data Security Standards Council Web site.

PCI Self-Assessment Questionnaire (SAQ)

Questionnaires used to assess PCI DSS compliance status. There are four questionnaire versions, allowing you to choose the one that is right for your business. All Level 2 and Level 3 Merchants are required to complete and submit a questionnaire to their Acquirer annually. Level 4 merchants are required to complete the questionnaire annually, but do not have to submit it to their Acquirer.

Perimeter Scan

A non-intrusive test that involves probing external-facing systems and reporting on the services available to the external network (i.e., the Internet).

ROC

A required annual Report on Compliance that Level 1 Merchants must submit to their acquirer to provide evidence of compliance validation with PCI DSS.

SDP

MasterCard's Site Data Protection program that specifies requirements for data security.

Truncation

Removal of a data segment (i.e., commonly involves deleting the first 12 digits of a card number, leaving only the last four visible on a receipt or report).

Vulnerability Scan

An automated tool that checks a merchant or service provider's systems for vulnerabilities, identifying those that could be used by hackers to target the company's private network.

More Online Help

<http://www.chasepaymentech.com/datasecurity>

<http://www.trustwave.com>

<http://www.mastercardsecurity.com>

http://usa.visa.com/merchants/risk_management/cisp.html

<http://www.pcisecuritystandards.org>

<http://www.privacyrights.org/ar/ChronDataBreaches.htm>

<http://www.ftc.gov/infosecurity>

http://www.usa.visa.com/merchants/risk_management/cisp_payment_applications.html

<http://www.visa.ca/en/merchant/fraud-prevention/account-information-security/index.jsp>

