

PCI Compliance Frequently Asked Questions

Who does PCI Compliance apply to?

PCI is an industry-mandated requirement for *all* companies, organizations and merchants that accept, transmit or store credit card data for the purpose of commercial transactions, regardless of company size, number of transactions or type of business. Specifically it applies to any merchant who accepts cards bearing the Visa, MasterCard, American Express, Discover or JCB logo.

The following are some of the more common misconceptions regarding PCI Compliance:

If I only take a handful of cards, does it apply to me?

If you are a merchant and are set up to take credit cards by any mechanism, you need to be compliant. The payment brands have collectively adopted PCI DSS as the requirement for any organization that processes, stores or transmits cardholder data.

I only accept phone orders. Does PCI still apply to me?

Yes. All businesses that accept credit cards, regardless of the method or process, must be PCI compliant.

I run my business from my home. Do I need to comply?

Yes. Home users may be the most vulnerable because typically they're not well protected. They often have 'always on' broadband connections and use things like chat, which makes them prime targets for hackers looking for the path of least resistance.

Don't most breaches involve large retailers?

If you look at media reports, it would seem that way. The reality is smaller merchants are prime targets for hackers since most have less sophisticated technology and security measures. Jennifer Fischer, Visa's senior business leader for payment system security compliance, confirms: "Visa continues to see small merchants most frequently targeted by hackers." Plus, hackers are only part of the problem—35% of reported breaches are due to human error such as lost laptops, inadvertent posting of confidential data, and files mistakenly tossed in an open dumpster. The cost of a data breach for a typical merchant averages \$36,000 and can be as high as \$50,000 or more.

Definitions

Acquirer

Bancard association member that initiates and maintains relationships with merchants that accept payment cards.

AES (Advanced Encryption Standard)

Block cipher adopted by NIST in November 2001. Algorithm is specified in FIPS PUB 197.

ASV (Approved Scanning Vendor)

A vendor that has been approved by the PCI SSC. The PCI SSC administers all ASV contracts, plus trains and certifies ASVs.

Cardholder Data

Any personally identifiable data associated with a cardholder, or Primary Account Number (PAN). This may include service code, expiration date and cardholder name.

Card Validation Value or Code

Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alternation or counterfeiting. The following is the term for each card brand:

- JCB—CAV Card Authentication Value
- MasterCard—CVC Card Validation Code
- Visa and Discover—CVV Card Verification Value
- American Express—CSC Card Security Code

The second type of card validation value or code is the three-digit value printed to the right of the card number in the signature panel on the back. For American Express, the code is a four-digit unembossed number printed above the card number on the face. This code is uniquely associated with each individual piece of plastic. Here are the details for each brand:

- American Express and Discover---CID Card Identification Number
- JCB—CAV2 Card Authentication Value 2
- MasterCard—CVC2 Card Validation Code 2
- Visa—CVV2 Card Verification Value 2

Cryptography

Discipline of mathematics and computer science concerned with information security and related issues, particularly encryption and authentication and such applications as access control.

DES (Data Encryption Standard)

Block cipher elected as the official Federal Information Processing Standard (FIPS) for the U.S. in 1976. Successor is the Advanced Encryption Standard (AES).

DMZ (Demilitarized Zone)

Network added between a private and public network to provide additional layer of security.

Encryption

Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.

Externally-facing IP Address

Your externally-facing IP address is the one assigned to your gateway (usually router or modem) which is connected to the Internet. You can look it up at: <http://whatismyip.com>.

Firewall

Part of a computer network designed to block unauthorized access. This can be done using either hardware or software.

IP Address

IP stands for Internet Protocol. Your IP address is a unique number (expressed as a series of numbers i.e. 72.11.111.11) used by technology devices such as printers, modems, et al to communicate with one another on a network. If you have an Internet Service Provider (ISP), they will assign you one. Think of it like your home address that others need to send your mail to the

right place. There are two types: *static* is fixed and never changes; *dynamic* changes every time you connect to the Internet.

IP-based POS

Transactions are transmitted, processed or stored on IP-based systems, or systems communicating via TCP/IP.

Magnetic Stripe Data (Track Data)

Data encoded in the magnetic stripe used for authorization during transactions when the card is presented. Entities must not retain full magnetic stripe data subsequent to transaction authorization. Subsequent to authorization, service codes, discretionary data/Card Validation Value/Code, and proprietary reserved values must be purged; however, account number, expiration date, name and service code may be extracted and retained if needed for business.

Merchant

Any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (Visa, MasterCard, American Express, Discover and JCB) as payment for goods and/or services.

Network Security Scan

Scans are done using an automated tool that remotely checks networks, systems and applications. The purpose is to identify vulnerabilities in operating systems, services and devices that hackers could use to target the company's private network. Compliance requires that scans (if applicable) be performed through an Approved Scanning Vendor (ASV) on a quarterly basis.

PAN (Primary Account Number)

Payment card number (credit or debit) that identifies the issuer and particular cardholder account. Also called account number.

Payment Application

This has very broad meaning. Basically, any piece of software designed to touch card data would qualify. In other words, anything that transmits, processes, or stores cardholder data electronically including anything from a Point-of-Sale systems in a restaurant to a web site e-commerce shopping cart.

PCI SSC (Payment Card Industry Security Standards Council)

An organization formed in September 2006 by the major card brands (Visa, MasterCard, American Express, Discover and JCB) to manage the on-going definition and evolution of a common standard designed to proactively protect customer account data throughout the transaction process. The intent was for this consortium to combine the individual data security programs of each card brand into one common standard to make it easier for merchants and service providers to comply.

PCI DSS (Payment Card Industry Data Security Standard)

A set of requirements designed to ensure ALL companies, regardless of size that accept, transmit, process, or store credit card info maintain a secure environment. This includes debit, credit, and pre-paid cards branded with one of the following five brand logos: Visa, MasterCard, American Express, Discover and JCB. It's origin began in 1999 when Visa USA created it's own data security program. By early 2003, each major card brand had its own version. The intent of the PCI DSS is to create a common, industry-wide standard to make it easier to comply. Compliance is mandated and enforced by the card brands. The PCI SSC manages the standard itself (development, enhancement, dissemination, implementation, etc).

Point-of-Sale

A transaction that takes place at a merchant location (i.e. retail store, restaurant, hotel, gas station, etc.)

PVV (Pin Verification Value)

Encoded in magnetic stripe of payment card.

Service Code

Three- or four-digit number on the magnetic-stripe that specifies acceptance requirements and limitations for a magnetic-stripe read transaction.

Service Provider

Any company that transmits, processes or stores cardholder data on behalf of another entity.

Meeting the requirements***What requirements are included in the PCI DSS?***

1. Install and maintain a firewall to protect cardholder data
2. Do not use vendor-supplied defaults for systems passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software and programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for employees and contractors

What do I need to do to get compliant?

The major card brands categorize merchants into four levels based on volume of transactions. The actions required to be compliant differ based on your level. GMS will identify your level and the steps required for you to achieve and maintain compliance.

The two main required actions include completing an annual Self-Assessment Questionnaire (SAQ) and performing quarterly scans. All merchants, regardless of level, need to complete a questionnaire. There are four different versions—GMS will identify the one that applies to you. Whether or not scans are required depends on how data is managed and connectivity to the Internet. GMS will identify if scans are required, manage the process, and even perform the scans.

Once the required actions have been successfully completed, GMS will submit the proper reports to the card brands on your behalf to document that you have met the requirements. To ensure you stay compliant, GMS will send you reminders when your next questionnaire and scan (if applicable) are due.

What if vulnerabilities are found in the scan?

If vulnerabilities are found, GMS will provide guidance regarding how to resolve them. Timely response and action is required in order to meet the compliance reporting deadlines. If the proper actions are not taken in a timely fashion, and the reporting deadline is not met, you will be charged \$19.95 per month for every month you are non-compliant.

I have multiple locations. Is each one required to validate PCI Compliance?

Any location with a *unique* merchant ID that accepts, transmits, or stores cardholder data must validate compliance as a separate entity. For example, a salon with two locations that share the same merchant ID can complete one questionnaire that covers both locations, however, individual scans may still be required (if applicable). If each location has a unique merchant ID, each would need to complete its own questionnaire and scan (if applicable).

Am I compliant if I have an SSL (Secure Sockets Layer) certificate?

No. SSL certificates make it safer to transmit data through encryption, but don't secure a Web server from malicious attacks or intrusions. They provide the first tier of security, but there are other steps to achieve compliance.

What about changes in my processing environment?

You must notify GMS of any changes to your processing environment including ISPs (Internet Service Providers), phone changes, IP address changes, changes in hardware (computers, servers), and new web sites. Any of these changes requires an additional scan to be performed.

Consequences of non-compliance

What if I comply with some, but not all, of the requirements?

The standards define a basic level of security, not something to work towards, so 100% compliance is required to avoid fines and other negative consequences.

What are the penalties for noncompliance?

First, you'll pay \$19.95 per month for every month you don't comply. If fined, the bank will likely terminate your relationship or increase transaction fees. Plus, there's the potential cost should you have a data breach—for a typical merchant it averages \$36,000 and can be as high as \$50,000 or more. Brand and reputation damage are difficult to measure but can devastate a small business. Suffice it to say, the penalties can be catastrophic. GMS has put together this program specifically to help you achieve and maintain compliance, easily and affordably.