

PCI Compliance Frequently Asked Questions

GENERAL INFORMATION.....	2
WHAT ARE THE PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARDS?.....	2
<i>What are the requirements for PCI DSS?.....</i>	2
<i>Is this a one-time requirement?.....</i>	2
<i>Are all merchants and service providers required to comply with the PCI DSS?.....</i>	3
<i>If I use a third-party software developer or Internet payment gateway, do they need to be in compliance with the PCI DSS?.....</i>	3
<i>Who is Trustwave?.....</i>	3
<i>What is a data compromise?.....</i>	3
<i>What is the difference between compliance and validation?.....</i>	3
<i>What are the benefits of being in compliance with the PCI DSS?.....</i>	3
MAGNETIC STRIPE DATA.....	4
<i>What is magnetic stripe data?.....</i>	4
<i>What is the difference between CVV and CVV2?.....</i>	4
<i>What is PIN verification (PVV)?.....</i>	4
<i>Can I store magnetic stripe data? How about CVV, CVV2, or PVV?.....</i>	4
COMPLIANCE VALIDATION.....	5
<i>How is a merchant's compliance classification level determined?.....</i>	5
<i>What is the PCI Self-Assessment Questionnaire (SAQ)?.....</i>	5
NETWORK VULNERABILITY SCAN.....	5
<i>What is a network vulnerability scan?.....</i>	5
<i>Is the network security scan only applicable to e-commerce entities?.....</i>	6
<i>How is an IP-based POS environment defined?.....</i>	6
<i>Is the scan mandatory if my POS does not have IP capabilities / or if I am not connected to the Internet / or have a wireless connection?.....</i>	6
<i>What if I fail the scan?.....</i>	6
OTHER COMPLIANCE QUESTIONS.....	7
<i>Is there a deadline to be compliant?.....</i>	7
<i>How long will this take?.....</i>	7
<i>If I complete the questionnaire and network scan, does this guarantee that I will not get compromised?.....</i>	7
<i>What processing software/applications are currently known to be compliant?.....</i>	8
REPORTING AND PENALTIES.....	9
<i>What are the compliance validation reporting requirements for merchants?.....</i>	9
<i>Can I be considered compliant if I have outstanding non-compliant issues but provide a remediation plan?.....</i>	9
<i>Are there fines if cardholder data is compromised?.....</i>	9
STATE REQUIREMENTS.....	10
MINNESOTA.....	10
OTHER STATES.....	10

General Information ---

What are the Payment Card Industry (PCI) Data Security Standards?

The PCI Data Security Standards are association (Visa®/MasterCard®) and industry mandated requirements for handling of credit card information, classification of merchants, and validation of merchant compliance. As a merchant, you are responsible for the security of cardholder data and must be careful not to store certain types of data on your systems or the systems of your third party service providers. You are also responsible for any damages or liability that may occur as a result of a data security breach or other non-compliance with the PCI Data Security Standards. The information security principles contained within these standards are based on ISO 17799, the internationally recognized standard for information security practices.

What are the requirements for PCI DSS?

There are twelve requirements falling into 6 categories:

- 1) *Build and maintain a secure network:* Install and maintain a firewall and use unique, high-security passwords with special care to replace default passwords.
- 2) *Protect cardholder data:* Whenever possible, do not store cardholder data. If there is a business need, you must protect this data. You must also encrypt any data passed across public networks, including your shopping cart and web-hosting providers.
- 3) *Maintain a vulnerability management program:* Use an anti-virus software program and keep it up date. Develop and maintain secure operating systems and payment applications. Ensure the anti-virus software applications you use are compliant (see www.visa.com/pabp).
- 4) *Implement strong access control measures:* Access, both electronic and physical access, to cardholder data should be on a “need-to-know” basis. Ensure those people with access have a unique ID and password for electronic access. Do not share logon information.
- 5) *Regularly monitor and test networks:* Track and monitor all access to networks and cardholder data. Ensure you have a regular testing schedule for security systems and processes: firewalls, patches, and anti-virus.
- 6) *Maintain an information security policy:* It is critical that your organization has a policy on how data security is handled at your business. Ensure you have an information security policy and that it's disseminated and updated regularly.

Is this a one-time requirement?

No. PCI DSS compliance is an ongoing process. Validation actions vary depending on the actual number of transactions you process. However, the credit card associations require all merchants to comply with PCI DSS at all times. There are two main components of validation:

- 1) Completing the [PCI Self-Assessment Questionnaire \(SAQ\)](#) annually
- 2) Undergoing [network vulnerability scans](#) performed by an approved scanning vendor quarterly



Are all merchants and service providers required to comply with the PCI DSS?

Yes. Any entities (merchants or service providers) that store, process, or transmit cardholder data must comply with the PCI DSS. The requirements apply to all acceptance channels including retail (brick-and-mortar), mail/telephone order (MOTO) and e-commerce. Validation requirements vary depending on the number of transactions an entity processes.

If I use a third-party software developer or Internet payment gateway, do they need to be in compliance with the PCI DSS?

Yes, any third-party software provider or Internet payment gateway that processes, transmits or stores cardholder data must be compliant; however, there are several companies that are not. You must check with your provider to confirm their compliance status. If you use a provider that is not compliant, you should discontinue use of that provider and notify CBMS of your new provider.

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

http://usa.visa.com/download/merchants/cisp_list_of_cisp_compliant_service_providers.pdf

Who is Trustwave?

Trustwave is a qualified security assessor (QSA). A QSA is an auditing company specializing in information security. They use card association developed criteria (the PCI DSS) to validate whether or not a merchant's information security is robust enough to sufficiently protect cardholder data from unauthorized access or malicious parties.

What is a data compromise?

A 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 websites 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. Skimming breaches are actually a hybrid of both a physical and electronic breach as the perpetrator takes possession of the card, steals the magnetic stripe data and returns the card to the cardholder.

What is the difference between compliance and validation?

You are compliant when you are abiding by the new security standards. Compliance is required for merchants on all levels.

Validation is the process confirming that you are 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, MasterCard, Discover, only require merchants on levels 1 through 3 to be validated. However, Level 4 merchants still must be in compliance and are encouraged to validate.

What are the benefits of being in compliance with the PCI DSS?

It is good business practice to adhere to the PCI standards and protect cardholder information. Additionally, Visa, MasterCard and Discover[®] may impose fines on their member banking institutions when merchants do not comply with PCI DSS. You are contractually obligated to indemnify and reimburse us, as your acquirer, for such fines. Please note such fines could be significant (as much as \$500,000), especially if your business is compromised and you have not been validated as compliant.

Magnetic Stripe Data

What is magnetic stripe data?

Magnetic stripe data is also known as “full track data” or “track 1” and “track 2”. The back of a credit card has a magnetic stripe. Every magnetic stripe has three tracks. Track 1 contains:

- The 13 or 16 digit personal account number “PAN”
- Name information (last name, title, suffix, first name, middle initial)
- Expiration date
- Service code
- CVV

Track 2 contains:

- PAN
- Expiration date
- Service code
- PIN verification (PVV)
- CVV

Track 3 is rarely used.

What is the difference between CVV and CVV2?

CVV is three written out digits on the back of the credit card. CVV data is captured through electronic means, whereas CVV2 is used to authenticate Card Not Present Transaction and is captured through the magnetic stripe. It is the same number, but differentiated by the means it is used.

What is PIN verification (PVV)?

The PVV is a cryptographic algorithm value stored in the Track 2 data. When an authentic PIN value is used, the combination of the PIN and the PVV allows a legitimate transaction to be processed.

Can I store magnetic stripe data? How about CVV, CVV2, or PVV?

Full track data (Track 1 and Track 2) cannot be stored past the initial transaction authorization completion. This includes CVV, CVV2, and PVV.

Elements that may be stored after authorization are name, account number, expiration date, and service code. To be PCI compliant, the account number must be encrypted, hashed, or truncated.

Compliance Validation

How is a merchant's compliance classification level determined?

Your compliance classification level is determined by annual transaction volume. The volume calculation is based on the gross number of Visa, MasterCard or Discover transactions processed within your merchant account. However, it will be based on the aggregate transaction volume of a corporation that owns several chains.

Level	Merchant Classification Criteria
1	Visa and MasterCard: Any merchant-regardless of acceptance channel that: <ul style="list-style-type: none"> Processes over 6 million Visa or MasterCard transactions per year Has suffered a hack or an attack that resulted in an account data compromise Visa or MasterCard determines should meet the Level 1 merchant requirements Has been identified by any other payment card brand as Level 1
2	Visa and MasterCard: Any merchant that processes 1 million to 6 million Visa or MasterCard transactions, regardless of acceptance channel
3	Visa and MasterCard: Any merchant that processes 20,000 to 1 million Visa or MasterCard e-commerce transactions
4	Visa and MasterCard: Any merchant that processes fewer than 20,000 Visa or MasterCard e-commerce transactions or processes fewer than 1 million Visa or MasterCard transactions, regardless of acceptance channel

What is the PCI Self-Assessment Questionnaire (SAQ)?

The PCI Self-Assessment Questionnaire is a list of questions used to assess your compliance with the requirements of the PCI DSS. The questionnaire includes questions about your policies, procedures, administrative controls, access controls and physical security measures as they pertain to those systems that store, process or transmit cardholder data.

Network Vulnerability Scan

What is a network vulnerability scan?

A vulnerability scan is an automated, non-intrusive scan that assesses your network and Web applications from the Internet. The scan identifies any vulnerabilities or gaps that could allow an unauthorized or malicious user to gain access to your network and potentially compromise cardholder data. The scans provided by Trustwave do not require you to install any software and no denial-of-service attacks will be performed.

Is the network security scan only applicable to e-commerce entities?

No. The network security scan is applicable to all merchants and service providers with Web addresses that can be accessed from outside the company walls. Even if an entity does not offer Web-based transactions, there are other services that make systems Internet accessible. Even email or employee Internet access makes your network vulnerable. 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 Internet provider web addresses are only required to complete the Report On Compliance (ROC) or the Compliance Questionnaire, as appropriate.

How is an IP-based POS environment defined?

The point of sale (POS) environment is the environment in which a transaction takes place at a merchant location (i.e. retail store, restaurant, hotel property, gas station, supermarket, or other point of sale location). An Internet protocol-based (IP) POS environment is one in which transactions are stored, processed, or transmitted on any system communicating to external systems through email or an Internet web address.

Is the scan mandatory if my POS does not have IP capabilities / or if I am not connected to the Internet / or have a wireless connection?

Any company with communication through the Internet, even email or a simple website with no e-commerce capability needs a scan. Your establishment might not need a scan if there is no external means for an intruder (hacker) to penetrate your systems.

What if I fail the scan?

If you fail the network vulnerability scan in TrustKeeper, this means that the scan discovered areas of your network that could be hacked. TrustKeeper will help guide you to remediate a failed scan and work toward achieving compliance. First, log into TrustKeeper to review the scan results. The report will provide a description of the identified issues and resources to begin fixing the problems. You will need to address each of the problems and then schedule a directed scan to ensure your remediation of the problem meets the PCI DSS.



Other Compliance Questions

Is there a deadline to be compliant?

Yes. However, these deadlines depend on your merchant level. The number and type of payment card transactions you process in a year determine your merchant level. Acquirers may also set their own deadlines for compliance. CBMS will be sending correspondence to our merchants regarding deadlines for compliance in 2008.

Merchant Level	Validation Actions	Validated By	Deadline
1	Annual On-site PCI Data Security Assessment	Qualified Data Security Company or Internal Audit (if signed by Officer of the company)	9/30/04 (Visa's new level 1 merchants have up to one year from identification to validate)
	Quarterly Network Scan	Qualified Independent Scan Vendor	
2	Annual PCI Self-Assessment Questionnaire	Merchant	6/30/05 (Visa's new level 2 merchants have until 9/30/07)
	Quarterly Network Scan	Qualified Independent Scan Vendor	
3	Annual PCI Self-Assessment Questionnaire	Merchant	9/30/07
	Quarterly Network Scan	Qualified Independent Scan Vendor	
4	Annual PCI Self-Assessment Questionnaire	Merchant	Validation requirements and dates are determined by the merchant's acquirer
	Quarterly Network Scan	Qualified Independent Scan Vendor	

Please note that compliance is not a one-time requirement. You should achieve and maintain compliance on an ongoing basis.

How long will this take?

The SAQ takes about 45 minutes to complete. The network scan provider can estimate the time it will take to complete that portion of the process. Once non-compliant issues have been identified, the length of time it takes an organization to implement solutions to resolve the issues impacts the length of the PCI DSS compliance process. The length of time also varies depending on the resolution and the complexity of the environment.

If I complete the questionnaire and network scan, does this guarantee that I will not get compromised?

No. The best practice is not to maintain cardholder data. These are the current standards and are subject to change.



What processing software/applications are currently known to be compliant?

To access the list of card processing software programs, see www.visa.com/pabp. This links to the card processing software programs that Visa has validated to be compliant with the PCI Data Security requirements, including the requirement that after authorization, Security data will be purged from the records and systems when these programs are used.

Security data is certain security information, including the full contents of any track of the magnetic stripe from the back of a card and the CVV (the three or four digit value printed on the signature panel of the card). Copies of these software programs that have version numbers older (those with a lower version number) than those indicated must be upgraded, have a special security patch installed, or be replaced with compliant software. If you are using any software programs not appearing on the list, you must confirm with your software vendor that the version you are using is compliant with current security requirements.

Reporting and Penalties

What are the compliance validation reporting requirements for merchants?

Merchants will provide compliance validation documentation to CBMS. CBMS must follow each card association's respective reporting requirements to ensure that your status is appropriately filed with each.

Can I be considered compliant if I have outstanding non-compliant issues but provide a remediation plan?

No. Lack of full compliance prevents you from being considered compliant. CBMS encourages you to complete the initial review, develop a remediation plan; complete items on the remediation plan, and revalidate compliance of those outstanding items in a timely manner.

Are there fines if cardholder data is compromised?

Yes. If cardholder data that you are responsible for is compromised, you may be subject to the following liabilities and fines associated with non-compliance:

- Potential fines of up to \$500,000 (at the discretion of Visa, MasterCard, Discover or other card associations)
- All fraud losses incurred from the use of the compromised account numbers from the date of compromise forward
- Cost of re-issuing cards associated with the compromise
- Cost of any additional fraud prevention/detection activities required by the card associations (i.e. a forensic audit) or costs incurred by credit card issuers associated with the compromise (i.e. additional monitoring of system for fraudulent activity)



State Requirements

Minnesota

Minnesota passed the Plastic Card Security Act in 2007. This new state law makes certain merchants liable for cost associated with cardholder data theft. Merchants should consult the specifics of the statute.

Other States

State laws concerning security of credit card data change regularly and it is your responsibility to be compliant with the laws of all states in which you do business.

CBMS cannot and does not endorse nor warrant completeness or accuracy of data provided by other websites.