

Payment Card Industry Data Security Standard (PCI DSS) Q & A

November 6, 2008

What is the PCI DSS? And what do the acronyms CISP, SDP, DSOP and DISC stand for?

The PCI DSS is a set of comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council (American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International), to help facilitate the adoption of consistent data security measures globally. The PCI DSS includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures intended to proactively protect customer account data.

The card brands each have their own programs that help merchants enforce compliance with the PCI DSS. The PCI Security Standards Council was founded in 2006 to oversee the standard itself, but each of the card brands issues fines and fees and schedules deadlines through their own enforcement programs.

Visa's Cardholder Information Security Program (CISP)

<http://www.visa.com/cisp>

MasterCard's Site Data Protection (SDP) program

<https://sdp.mastercardintl.com/index.shtml>

Discover's Discover Information Security and Compliance (DISC) program

http://www.discovernetwork.com/merchant/resources/data/data_security.html

American Express Data Security Operating Policy (DSOP)

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

PCI Security Standards Council

<http://pcisecuritystandard.org>

Are all Merchants and Service Providers required to comply with the PCI DSS?

Yes. All 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.

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 Compliance Questionnaire annually
2. Undergoing Vulnerability Scans performed by an Approved Scanning Vendor quarterly

What are the Requirements for PCI DSS?

There are twelve requirements that fall 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 anti-virus and keep it up date. Develop and maintain secure operating systems and payment applications. Ensure the applications your 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. 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’s critical that your organization has a resource for how data security is handled at your business. Ensure you have a policy and that it’s disseminated and updated regularly.

What is the Visa deadline for compliance for newly-boarded merchants?

To promote payment application security awareness and increase merchant adoption of secure payment applications, Visa instituted a number of payment application security mandates in October of 2007.

Effective October 1, 2008, newly boarded merchants that qualify as Level 3 or 4 must either validate their compliance with the Payment Card Industry Data Security Standard (PCI DSS) or use payment applications that comply with Visa’s Payment Application Best Practices (PABP). Thus, any merchant that is accepting payment cards for the first time will be required by their acquiring bank/processor/ISO to either validate their compliance with the PCI DSS or use a payment application that is PABP-compliant. In the U.S. this includes merchants that are switching from one acquiring bank to another.

How is “cardholder data” defined?

Cardholder data is the full magnetic stripe or the PAN plus any of the following:

- Cardholder name
- Expiration date
- Service Code

The PCI DSS applies to any of this cardholder data that is stored, processed, or transmitted.

Can I store magnetic stripe data? How about the CVV2 and CVC?

It is never acceptable to store magnetic stripe data after authorization of the transaction.

It is also never acceptable to retain CVV2 and CVC, (the last three digits printed on the signature panel) after transaction authorization.

Compliance Validation

Can a merchant’s internal staff validate compliance?

No. Elavon requires that a merchant use a Qualified Security Assessor for annual compliance and an Approved Scanning Vendor to perform the quarterly vulnerability scans. A list of approved Qualified Data Security Companies can be found on the Visa website at www.visa.com/cisp.

Does Elavon recommend a specific Security Assessor or Scanning Vendor to assist merchants with their data security assessment?

Elavon has teamed with Trustwave – a Visa® and MasterCard® accredited Qualified Security Assessor – to assist you with your data security assessment. Trustwave’s TrustKeeper® service will help you understand this important requirement for your business, provide you with an analysis of your PCI DSS status, and assist you with your required compliance efforts. Specifics regarding Compliance validation in this document will discuss the capabilities using this assessor.

Who is Trustwave?

Trustwave is the leading provider of on-demand data security and payment card industry compliance management solutions to Fortune 2000 businesses and the public sector. Our flagship product, TrustKeeper®, provides data security and compliance validation services to approximately 30,000 businesses throughout the world to achieve compliance with the PCI DSS and other regulatory requirements. Trustwave is an Approved Scanning Vendor (ASV) and a Qualified Security Assessor (QSA) for the card associations.

What is the PCI Self-Assessment Questionnaire?

The PCI Self-Assessment Questionnaire is a list of questions used to assess your compliance with the requirements of the PCI DSS. In February of 2008, the PCI Security Standards Council released four versions of the questionnaire to account for different merchant environments.

1. **SAQ A:** Addresses requirements applicable to merchants who have outsourced all cardholder data storage, processing and transmission.
2. **SAQ B:** Created to address requirements pertinent to merchants who process cardholder data via imprint machines or standalone dial-up terminals only.
3. **SAQ C:** Constructed to focus on requirements applicable to merchants whose payment applications systems are connected to the Internet.
4. **SAQ D:** Designed to address requirements relevant to all service providers defined by a payment brand as eligible to complete an SAQ and those merchants who do not fall under the types addressed by SAQ A, B or C.

For more information on the questionnaire, and to determine which one is right for your business, please visit: <https://www.pcisecuritystandards.org/tech/saq.htm>

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 (on the external-facing IPs). The scan will identify any vulnerabilities or gaps that may allow an unauthorized or malicious user to gain access to your network and potentially compromise cardholder data. The scans provided by Trustwave will not require you to install any software on their systems, and no denial-of-service attacks will be performed.

What if I fail the scan?

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

What is a Directed Scan?

Many times a vulnerability scan will discover vulnerabilities that need to be resolved in order to maintain compliance. Once you resolve these vulnerabilities, a directed scan can be run upon your request to verify that you have resolved any compliance issues. You may also run a directed scan after you have made changes to your network to ensure that the changes have not affected your compliance status. These are additional scans above and beyond the regular quarterly scans.

What are the penalties and fines associated with a security breach?

Per the card associations, the penalties and fines for failure to comply with requirements or to rectify a security issue can be severe. These fines range from \$10,000 to \$500,000 per incident.. If a security breach occurs in

your environment, you will be liable for the cost of the required forensic investigations, fraudulent purchases, and the cost of re-issuing cards. Please note that you may also lose your credit card acceptance privileges.

Is there a deadline to be compliant?

Yes. However, these deadlines depend on your merchant level. Your merchant level is determined by the number and type of payment card transactions you process in a year. Acquirers may also set their own deadlines for compliance. Please note that compliance is not a one-time requirement. You should achieve and maintain compliance on an ongoing basis.

Visa publishes the following deadlines for PCI DSS compliance:

Merchant Level	Validation Actions	Validated By	Deadline
2	Annual PCI Self-Assessment Questionnaire	Merchant	6/30/05 (Visa's new level 2 merchants have until 9/30/07)
	Quarterly Network Scan	Approved Scanning Vendor	
3	Annual PCI Self-Assessment Questionnaire	Merchant	6/30/05
	Quarterly Network Scan	Approved Scanning Vendor	
4	Annual PCI Self-Assessment Questionnaire	Merchant	Validation requirements and dates are determined by the merchant's acquirer
	Quarterly Network Scan	Approved Scanning Vendor	

How are the merchant levels defined?

Visa and MasterCard define merchant levels as follows:

Level	Merchant Classification Criteria
1	<p><u>Visa & MasterCard</u>: Any merchant-regardless of acceptance channel-that:</p> <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	<p><u>Visa & MasterCard</u>: Any merchant that processes 1 million to 6 million Visa or MasterCard transactions, regardless of acceptance channel</p>
3	<p><u>Visa & MasterCard</u>: Any merchant that processes 20,000 to 1 million Visa or MasterCard e-commerce transactions</p>
4	<p><u>Visa & MasterCard</u>: 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</p>

What if my business does not go through this compliance procedure?

If you do not comply with the security requirements of the card associations, you put your organization at risk of payment card compromise. Your acquirer may also pass fines levied by the card associations for non-compliance on to you.

Do I get anything to prove I am compliant, if so, will it be automatically sent to Visa or MasterCard?

Once you have successfully completed the compliance program, Trustwave will issue you a Certificate of Compliance. Any reporting to your acquirer will be facilitated by TrustKeeper. If you complete the compliance program with any other approved Qualified Data Security Company, you will be required to provide current documentation to Elavon annually showing your compliance status.

We don't have time for this. How long will this take?

The length of the process varies. Once non-compliance issues have been identified, the length of time it takes an organization to implement solutions to resolve the issues will affect the length of the PCI DSS compliance process. The length of time also varies depending on the resolution and the complexity of the environment.

MSP Channel Specifics

How will my merchants be notified of these requirements?

On November 21, 2008 Elavon will be mailing a letter to all Level 4 merchants who use a software program to process credit and debit card payments. This includes merchants on the Elavon network and all Foreign Networks. This letter will advise the affected merchants of a \$135 annual fee beginning December, 2008 as well as a monthly fee of \$20 to be assessed to those merchants who have not validated PCI DSS compliance before March 1, 2009. There will also be notification posted to Merchant Connect advising of Elavon's partnership with TrustWave and to provide instructions on how to become registered with Trustwave. A list of your merchants receiving this notification will be provided by your Relationship Manager.

What if a merchant receives a letter from Elavon but has already certified PCI DSS compliance?

The letters will instruct the merchants to contact customer service to provide appropriate documentation. Elavon does not require that a merchant use Trustwave for their annual assessment and scanning obligations but we do require that they use a certified assessor. A list of approved Qualified Data Security Companies can be found on the Visa website at www.visa.com/cisp.

If the merchant uses an assessor other than TrustWave, will they have to pay the annual fee?

All merchants not currently certified with Trustwave will receive notification of PCI Validation requirements and related fees and they will be billed the annual fee beginning December 2008. If they are certified through another assessor, they can provide appropriate documentation to Customer Service and the fee will be refunded. If this information is not received by March, 2009, they will be billed the \$20 monthly fee until documentation is provided.

How will these requirements affect new merchants?

The annual fee for merchants without documentation supporting PCI DSS Compliance is being added to existing merchants as of October 1, 2008. Elavon will be responsible for implementing all fees associated with PCI DSS compliance validation, the MSP does not need to add this fee to new merchants on the merchant application.

Also, in compliance with PA-DSS requirements, all new merchants must utilize Visa Validated Payment Applications or Compliant Service Providers. Effective October 1, 2008, this was a requirement on new applications and effective November 9, 2008 enhancements have been made to MSP Fast to better accommodate these requirements. More information on these updates can be found on the MSP Info Center.

Where can I find more information on PCI DSS or PA DSS?

The MSP Info Center will continually be updated as more information is made available. Information on these mandates can be found by searching on keywords: PCI DSS or PA DSS.

And as always, please feel free to call your MSP Relationship Manager at 800-819-6019 with additional questions you may have.