securityMETRICS®

Secure and PCI DSS Compliant E-commerce Payment Card Processing

Introduction

As an e-commerce merchant, to accept payment cards over the Internet and ensure protection against criminals, there are several options you must consider.

Visa endorses the Payment Card Industry Data Security Standard (PCI DSS) as a set of security guidelines for you to follow to ensure secure payment card data processing. Understanding and complying with the PCI DSS requirements is an essential part of your business success; one where only you hold the responsibility. If you carefully read and consider the following information you can make smart, informed decisions to achieve and maintain PCI DSS compliance and protect your business.

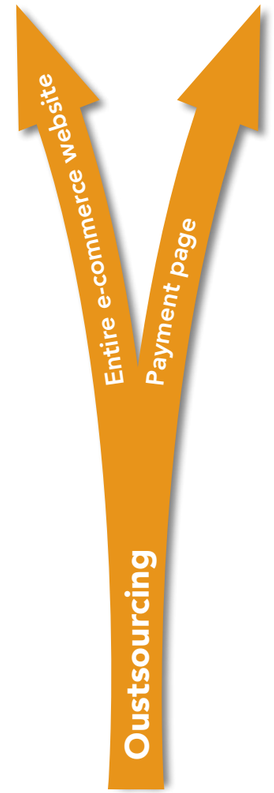
Many e-commerce businesses outsource or contract most technical aspects of e-commerce. Securely building a site that conforms to PCI DSS requirements is quite complex. The way you manage your e-commerce website, either through outsourcing or developing the site yourself, determines your requirements for PCI DSS compliance.

Outsourcing

Two methods of outsourcing apply to e-commerce:

1. Outsource the entire e-commerce website (shopping cart and payment pages) to a single vendor.
2. Outsource the payment page where payment card data is entered and find or write a shopping cart system.

Note: *Shopping cart is assumed not to take or pass any credit card data, only product and price information.*



Outsource the entire e-commerce website

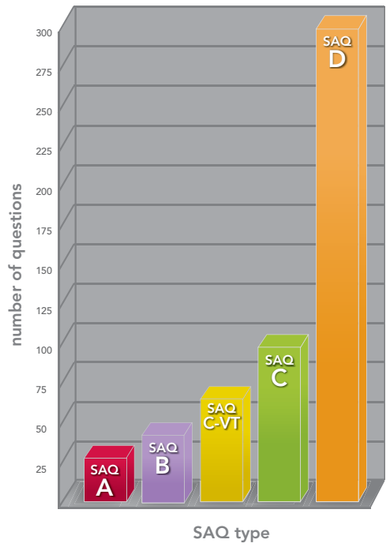
To outsource the entire payment process, you need an e-commerce hosting partner validated as a PCI DSS compliant merchant service provider listed on the Visa approved list of service providers found at www.visa.com. This greatly simplifies PCI compliance for your business. Your PCI DSS compliant e-commerce partner hosts and manages your e-commerce site in a PCI DSS compliant manner as part of their normal service offering.

Because no e-commerce payment card data flows through any of your company systems, you only have to worry about two simple tasks to achieve and maintain PCI DSS compliance.

First, secure all media you may receive that contains payment card data. For example: secure any printed transaction information you may generate by interacting with administration pages of your e-commerce website such as faxes sent to your business, etc. Typically, this media is printed material that must be physically secured if retained and properly destroyed when no longer needed.

Second, maintain documented policies and procedures describing how you manage your e-commerce hosting partner. Periodically check your hosting partner's PCI DSS compliance status on Visa's compliant merchant service provider list and create and maintain a written agreement between your business and your e-commerce partner to protect card data.

If you have these two processes in place, you have all the information needed to validate PCI DSS compliance. Now, you simply need to complete the Self Assessment Questionnaire A (SAQ A) form and submit it to your acquiring bank.



Based on the design of your e-commerce solution you must validate your compliance in one of four ways (A,B,C, or D) to your merchant bank. A is the easiest questionnaire with 14 questions, and D is the most difficult with 250+ questions.

TIP: Be sure not to choose an e-commerce hosting partner that is cheaper, faster, and creates good looking websites, but disregards PCI DSS security requirements. In the end, your business will end up paying fines if compromised. Select an e-commerce hosting partner that is validated and listed as PCI DSS compliant.

Outsource the payment page

When you outsource the payment page(s) to an e-commerce hosting partner involved in accepting and processing payment card data, you need to select an e-commerce hosting partner that has been validated and listed as PCI DSS compliant. If you do, then you can achieve compliance the same way as if you outsource the entire e-commerce website.

Consider your shopping cart

If you outsource the payment page, you will at the very least need a shopping cart. You may choose to develop it yourself, purchase a prebuilt shopping cart, or contract the development of the shopping cart portion of your website.

If your shopping cart website (whether hosted by you or someone else) never stores, processes, or transmits payment card data, PCI DSS security controls do not apply to it.

A common e-commerce pitfall

Some merchants that have an e-commerce presence find very cost-effective "virtual hosting" providers that claim their set up is secure. Virtual hosting provides you with a "slice" of a larger server and includes access to shopping cart software that can be set up to process payment cards. Very easily, you are able to accept e-commerce payment cards. However, this configuration offers no assurance of PCI DSS compliance either of the virtual hosting environment or the shopping cart software. The shopping cart software often operates insecurely. If steps are taken to achieve PCI compliance, hosting providers may become upset if external vulnerability scans (scans required for PCI DSS compliance that check for weaknesses in the web domain) are set up and fail. It means more work for the virtual host as they are required to modify or update servers or applications. Additionally,

Outsourcing Entire E-commerce Site: *Pros and Cons*

Pros	Cons
You do not deal with electronic card data	More expensive
Very simple process to validate compliance with SAQ A	Potential for less flexibility in website design
Low risk to card data when using a PCI DSS validated e-commerce partner	Must interact with 3rd party for page/product changes
	Must find a provider you integrate well with

TIP: Beware of payment pages or shopping cart systems that collect payment card data but don't perform authorization or settlement of the transaction. They may require or have an option for you to download the transaction data so it can be typed manually into your own payment processing system. This process may require more work and processes to validate and maintain PCI DSS compliance.

these providers frequently offer a web control panel that lets you manage your files and e-commerce software without providing a strong and compliant authentication method, making you vulnerable to attack. It is extremely difficult for common virtual hosted environments to achieve PCI DSS compliance.

Note: Virtual hosting is not the same as cloud services that create a virtual server dedicated to the use of a merchant. If using an e-commerce cloud provider, be sure to find one that is PCI DSS validated.

Do it yourself

Developing all pages for e-commerce payment processing is not a simple task. You are responsible for setting up and maintaining e-commerce systems and processes that meet all appropriate PCI DSS requirements. This option can seem very attractive because of perceived lower up-front costs (e.g., affordable virtual web site hosting, an acquaintance who can develop the web site, free shopping cart software), but may quickly become complex and costly when considering the effort required to truly validate and maintain PCI DSS compliance.

Whether you host systems at your office location or data center, you are responsible for creating and maintaining a PCI DSS compliant e-commerce payment system.

Even though you are only required to validate compliance to your PCI DSS validation type, "you must still comply with all applicable PCI DSS requirements in order to be PCI DSS compliant"

-Payment Card Industry Security Standard Council (PCI SSC)

Outsourcing Payment Page Only: *Pros and Cons*

Pros	Cons
Do not deal with electronic card data	Redirect process may hamper customer seamless experience with your shopping cart site
Very simple process to validate compliance with SAQ A	Potentially less flexibility in payment page design
More flexibility in shopping cart options	Must interact with 3rd party for page/product changes
Low risk to card data when using a PCI DSS validated e-commerce partner	Need to find a provider you like

The following is a simplified list of requirements for validating compliance to SAQ C (where payment cards are processed through the Internet and no payment cards are stored. When card data storage is involved, more requirements apply):

- ☐ Install and maintain a strong hardware firewall between your e-commerce web server and the Internet creating a secure DMZ for your web server to reside. This firewall needs to limit network traffic inbound and outbound for your web server to work and be maintained.
- ☐ Have and follow documented procedures for installing new hardware to ensure vendor default settings have been changed (e.g., default accounts, passwords).
- ☐ Have a scheduled process to make sure no sensitive card data is accidentally saved on your e-commerce systems. Use a data discovery software program to do these searches.
- ☐ Ensure your web server is using secure and properly encrypted inbound and outbound messages by carefully maintaining security settings on the web server.
- ☐ Be sure anti-virus software is installed, active, and regularly updated on all e-commerce systems.
- ☐ Keep all e-commerce systems up-to-date and patched, monthly.
- ☐ Ensure strong access control (password and user name) is present on all systems and e-commerce software to ensure only those with the correct job function can manage critical systems.
- ☐ Implement 2-factor authentication for all remote management of e-commerce systems. This means using more than just a username and password (or two passwords). Along with a password you need another unique piece of information that identifies an individual who wants to access the system (fingerprint, individually assigned complex numerical certificate, etc.).
- ☐ Only enable remote vendor accounts that give access to your e-commerce systems during the period of time they need to do the support work.
- ☐ Define processes for handling, transport, and secure storage of any printed credit card numbers (faxes, forms filled out by call center employees, etc.).
- ☐ Conduct quarterly scans to detect rogue wireless devices attached to your e-commerce network.
- ☐ Setup and conduct internal and external vulnerability assessment scans at least quarterly, and fix any issues they uncover. External scans must be run by a PCI Approved Scanning Vendor.
- ☐ Document and distribute security and technology usage policies to employees. Implement a PCI security training program for all relevant employees.

Remember that as a merchant, you must comply with all applicable PCI DSS requirements.

Conclusion

The simplest approach for you to achieve PCI DSS compliance is to outsource all e-commerce functions or at least outsource the functions that accept payment card data to e-commerce hosting partners that are on Visa's list of PCI DSS validated service providers. Taking the full burden of PCI DSS compliance on your shoulders, though possible, is recommended only for merchants with a dedicated internal IT staff, with IT experience.

The intent of this article is to introduce PCI DSS compliance to level 4 e-commerce merchants. A consultation of security steps and procedures with a Qualified Security Assessor (QSA) is recommended to reach accurate PCI DSS compliance.

securityMETRICS®