PCI Compliance Requirements Guide

What Is PCI Compliance?

The Payment Card Industry Data Security Standard (PCI DSS) was created to ensure that both merchants and consumers are safe from data compromise. For business owners, PCI compliance means completing the PCI DSS Self-Assessment Questionnaire (SAQ) annually and paying the annual fee of $99 every July. If you do not complete the annual PCI DSS Self-Assessment Questionnaire (SAQ), you will incur a penalty fee of $19.95 monthly until it is completed each year. However, the cost of time to do the questionnaire far outweighs the consequences you will face if you are not PCI compliant and are victim of a data breach.

The question is, would you rather endure what might be a bit of frustrating filling out the questionnaire annually, or would you rather cough up $20,000+ to clean up a security breach and the liabilities that can come along with it? This includes financial audits and fines! Worse than the money it takes to recover from a data breach is the loss of trust in your company from loyal customers. To put it simply: a data breach can cost you your business.

Completing the annual questionnaire and paying your yearly fees may be a hassle, but it's time spent making sure you're not just doing business, you're doing *smart* business. There are fraudsters out there actively monitoring companies for vulnerabilities so they may steal credit card information. If you're a small business, you're at greater risk of data compromise. Large corporations are spending superfluous amounts of money to ensure their brand, their customers, and their livelihoods are protected, so hackers are focusing on smaller businesses which may not be as focused on data protection.

How to Complete Your SAQ!

Step 1 – Please log onto https://pci.trustwave.com/cardconnect. Trustwave is a company which handles PCI requirements for merchants. They have a help desk established at **1-800-363-1621.** Feel comfortable in calling them to assist you. You will want to keep track of the password that you setup for next year's verification.

Step 2 – The first screen will require your Merchant ID # (MID), your name, dba name, and address.

Step 3 – The next screen will take you to the start of the questions. First you will be asked how you take cards, via the web, over the phone, with a terminal. Answer all that apply.

Step 4 – The second screen will ask you if you use a third-party web hosted integration, which is Event Rental Systems. ERS is integrated with Electronic Money Company's processor and gateway, Card Connect. Card Connect's gateway is what connects your ERS website to the processing of credit cards. There is a drop down list and you will have to add Card Connect since it is not already there.

Step 5 – Continue on through the rest of the questionnaire. The hint that Trustwave gives is that all of the answers should be YES or N/A, not applicable.

In otherwords, **YES** you have security measures and policies in place to protect against fraud. And **YES**, ERS and Card Connect are both compliant with PCI requirements. If you see a small circle with an 'i" in the middle of it, this indicates more "information" is available so you can gain more understanding about that question.

Step 6 - If you don't pass at the end of the questionnaire, it will tell you exactly which question failed and why, so you can go back and correct it.

Step 7 – Be aware that all merchants who process on the internet will be required to comply with quarterly scans of your internet. The scans search for viruses implanted by fraudsters to steal credit card numbers as well as other customer information like the expiration date and their billing address. Most terminals are also connected to the internet and must be scanned quarterly as well. If you don't pass a scan, Trustwave will tell you exactly why you did not pass. (Warning: The explanation will be written in "Geek" and you may need to hire an IT person to understand what needs to be fixed in your system.) Feel free to check with us first. We have some experience with this but I will warn you again that we are not Geeks either.

Step 8 – Trustwave provides a **CERTIFICATE** at the end of the questionnaire. The certificate is proof that you were certified on this date and is an important document to keep. We suggest that you put the certificate in a frame and hang it on the wall so that customers can see that you are PCI compliant and concerned about protecting their credit card information. You will also be notified that you are compliant inside your Card Connect portal.

Step 9 - Reminder – Each year you will need to complete the survey again. You will receive a reminder from Trustwave to do the SAQ again by email 90, 60 and 30 days prior to the anniversary of your certification. It will be easier the second time around and you can also call Trustwave and tell them all the answers are the same as the last time. Remember that if you do not get it done by the anniversary of your certification, then you will be charged $19.95/month on your credit card statement until you do get it done.