Simplêfy®

Client Support and Information Services

PCI Compliance Guidebook

530 New Los Angeles Ave. #115-358
Moorpark, CA 93021
Phone 888.341.2999 • Fax 877.280.0885

Table Of Contents

Purpose Of This Guidebook

The purpose of this PCI (Payment Card Industry) Compliance Guidebook is to assist small to medium size businesses in complying with the Payment Card Industry Data Security Standard (PCI DSS) and in completing your required Annual Self-Assessment Questionnaire (SAQ).

This Guidebook is not a detailed explanation of the PCI DSS nor is any information contained herein to be construed as the definitive authority on all things PCI DSS related especially since the PCI DSS changes over time as security threats and Payment Card Industry decisions dictate.

NOTE: If any links within this guidebook are found to be no longer valid, please notify Carl Alexander, Director of IT, Simplêfy, Inc., calexander@simplefy.com.

Version 1.0 October 2014

What Is PCI Compliance And What Does It Accomplish?

PCI (Payment Card Industry) Compliance, also known as the PCI Data Security Standard (PCI DSS) is a set of Security Standards designed to help merchants protect credit card and cardholder data from theft both online and off.

Adherence to the Standard will help minimize the chance that a criminal could gain access to credit card data, cardholder information, and even your business and personal information within your environment. CAVEAT: Adherence to the Standard will **not** guarantee that an experienced hacker cannot gain access to your environment and steal any information however being PCI Compliant will reduce your liability should a breach occur.

A possible side benefit of PCI Compliance is that if your cardholder environment is more secure, generally your overall business environment will be also, although that depends upon whether you apply the security standards across the enterprise to non-credit card related information systems and environments.

Do I Need To Be PCI Compliant?

If you accept, transmit, or store ANY cardholder data, then you **MUST** be PCI DSS Compliant. This is true no matter what your organizational or business type is, and regardless of the number of credit card transactions or dollar amount of those transactions.

What Are The Penalties For Noncompliance?

If you do not comply with the PCI DSS Requirements, the payment brands may, at their discretion, fine your acquiring bank $5,000 to $100,000 per month for PCI compliance violations. The banks will most likely pass this fine on downstream till it eventually hits you. The bank will also likely terminate your relationship with them or increase the cost of your transaction fees. The card industry penalties are not widely publicized, but they can be catastrophic to your business. Merchants that do not comply with PCI DSS may be subject to fines, card replacement costs, costly forensic audits, brand damage, etc., should a breach event occur and they were not PCI Compliant.

What Is An SAQ?

An SAQ is a Security Assessment Questionnaire which serves the purpose of helping you identify potential vulnerabilities within your cardholder environment so that you can take steps to correct them thus making your credit card processing environment more secure against theft of cardholder data.

Types Of SAQ's

SAQ-A

SAQ-A is for merchants who take payments Card-Not-Present payments over the Internet where the cardholder data is collected by a third party service provider or on a custom payment page hosted directly on the payment gateway. Cardholder data is **not** collected on the Merchants website at any time. When completing the SAQ-A, the merchant is acknowledging that they believe that the Third Party taking the cardholder data is PCI Compliant. A vulnerability scan is not required since that scan should already be taking place within the third-party's environment in meeting their PCI DSS requirements. Not applicable to face-to-face channels.

SAQ-A-EP (New with PCI 3.0)

SAQ-A-EP is for e-commerce merchants who outsource all payment processing to PCI-DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Applicable only to e-commerce channels.

SAQ-B

SAQ-B is for either merchants using the old fashioned imprinter ("knuckle buster") and carbon based credit card payment slips or, more commonly, a dial-up terminal that does not store cardholder data and does not use the Internet for the transmission of cardholder data. Merchants using wireless credit card terminals, and payment applications with their smartphones or tablet PCs using wireless cell coverage (i.e. **not** connected to the Internet via Wi-Fi) are often allowed use of SAQ-B as well. A vulnerability scan is not required. Not applicable to e-commerce channels.

SAQ-B-IP (New with PCI 3.0)

SAQ-B-IP is for merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. Not Applicable to e-commerce channels.

SAQ-C

SAQ-C is for merchants who use any POS device or payment application running on a computer that uses the Internet to transmit cardholder data to the payment gateway. Electronic Storage of cardholder data on these devices is not permitted. A quarterly vulnerability scan of the IP (Internet Protocol) Address **is** required. Not applicable to e-commerce channels.

SAQ-C-VT

SAQ-C-VT is for merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. Not applicable to e-commerce channels.

SAQ-D

SAQ-D is used for all other merchant types not mentioned above and service providers who are considered eligible to complete an SAQ. Some examples of merchants who need to complete an SAQ-D are those who write or modify their own software to accept credit card payments over the Internet or on their website, as well as service providers performing similar functions for a merchant. A quarterly vulnerability scan of the IP (Internet Protocol) Address for the POS System, Computer running the Payment Application Software or Website using a custom Payment Application **is** required.

SAQ-P2PE-HW (New with PCI 3.0)

SAQ-P2PE-HW is for merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. Not applicable to e-commerce channels.

SAQ's For Multiple Locations

If your business locations process under the same Tax ID, and use the same equipment and/or software and policies at all locations, then you may be able complete one SAQ covering all locations. Otherwise each MID with different equipment or software would need to complete an SAQ appropriate to its method of processing. Contact your Simplêfy representative to see if you can chain some or all of your locations.

How To Get Started

Before you can begin completing your Annual PCI SAQ, you will first need to establish an Account with Trustwave. Trustwave is the PCI DSS Approved Scanning Vendor (ASV) selected by Simplêfy to perform your quarterly PCI Scans (if applicable) and process and submit your Annual SAQs to the Payment Card Industry Associations and Affiliates to show compliance. You also have the option, though we don't recommend it, to use and pay for your own ASV, but you will, in addition to completing the SAQs and Scans, be required to send Simplêfy your quarterly passing scan results, Completed SAQ and Certificates of Attestation and Compliance.

Establishing Your Trustwave Account

There are two ways to establish your Trustwave Account:

1. **www.CheckMyPCI.com (**This site is more for informational purposes and acts as a gateway that will take you to (the second option below):

2. **https://login.trustwave.com/portal-core/home/pci-user-registration/sponsorCode=digfg&locale=en_us**

In either case, you will end up at the web address in item 2 above.

Once you arrive at the website, you will need the following information to get started with the registration process:

1. Your Company Name
2. Your Merchant ID #
3. Your Country
4. Your State/Province
5. Your Zip Code
6. Your Email Address

After filling in the relevant fields with the information above, click on the Next Button on the lower right corner of the form.

The next form will ask you how you process credit cards. The options are:

1. Website
2. Mail/Telephone

3. In Person

Check those that apply to your processing environment and click on the Green Next Button located to the right of the options.

Then choose how you process credit cards.

How you process

1. Dial up or Paper

2. Mobile/Tablet

1. Internet (if you chose Internet, you will also be presented with the following options: 1. POS, Virtual Terminal or Other)

Select an option and then click on the Green Next Button and answer any additional questions you may be asked.

When you get to the page that asks you to create a Username, it will show your email address as the default. Simplêfy recommends that you change the Username from your email address to the MID # of the location you are enrolling, especially if you have multiple locations and MID#'s or if you are an employee or consultant for the company.

For the Password, Simplêfy recommends that you create a password that is secure, i.e. at least 8 characters long with at least one UPPER and one lower case letter and one number and a special character such as #$@!.

The reason for a secure password is that, if a hacker should somehow obtain your username to your Trustwave account and crack your password, they would have access to sensitive security information about your cardholder environment.

Follow the directions to complete your registration. Upon completion you can then complete your SAQ and set up your scan targets (IP Addresses of your POS, Computer, or ecommerce website to be scanned (if applicable), learn about PCI, and download PCI related documents. If you don't want to complete the SAQ or set up scan targets at this time you can log out and log back in at a more convenient time.

Logging Off

To log off click on the Gear Symbol located in the upper right hand corner of your Trustwave Dashboard and click on the Log Out link.

Logging On

To return to your Trustwave Dashboard at any time go to the following URL:

https://login.trustwave.com/portal-core/home

enter your Username and Password and click on the Login button.

If You Forgot Your Username

If you forgot your Username, click on the Username link below the Login button. You will be asked for your email. Enter your email and click the Send My User Name button. Trustwave will then send an email with your Username to the email address you created when you first set up the account. If you do not receive the email from Trustwave within a few hours from submitting it, please contact Simplêfy for assistance.

If You Forgot Your Password

If you forgot your Password, click on the Password link below the Login button. You will be asked for your Username. Enter your email and click the Send My Password button. Trustwave will then send an email to the email address you created when you set up the account. If you do not receive the email from Trustwave within a few hours from submitting it, please contact Simplêfy for assistance.

Changing User Information, Password Or Security Questions

After you log back into your Trustwave Dashboard you can change your contact information, email address or security questions by clicking on the Gear Icon in the upper right hand corner of your Trustwave Dashboard and clicking on the Preferences Link. A small window opens and you can then modify the fields under either the User Information Tab or the Security Information Tab. When you complete the changes, click on the Save Button.

Adding Or Changing Scan Targets

If you are an e-commerce Merchant or use a Point-of-Sale (POS) or other device that connects to the Internet, you should have a Scanning Tab located at the top of your Trustwave Dashboard.

Click on the Scanning Tab, then click on Scan Setup and then click on the Add Scan Location Button and complete the fields. For Internet Based POS Systems or Software running on computers, you will need the public IP Address of any computer or device that connects to the Internet to transmit card holder data.

If you do not know this public IP Address, you can obtain it by using a web browser and going to:

http://www.simplefy.com/merchant-support.html.

To the right of the words Support Information you will see "Your IP Address is: ###.###.###.###" in orange letters. You would enter that IP Address in the IP Address field of the scan target.

If your POS System does not have a web browser, you should be able to plug a laptop computer into the Ethernet Outlet on the wall or router and then use a web browser to obtain it.

If you have more than one computer/POS that handles credit card transactions, you should check each one. (Generally, all computers within a given location will have the same Public IP Address because they are usually sharing a router however, it is always best to make sure).

Viewing And Printing Scan Reports

If you are an e-commerce Merchant or use a Point-of-Sale (POS) or other device that connects to the Internet, you should have a Scanning Tab located at the top of your Trustwave Dashboard. Click on the Scanning Tab then click on Scan Results Tab. You can then view your scan results for each scan target or click on the PDF Report Button to download the Scan Report to your computer.

Disputing Or Correcting Scan Results

If you are an e-commerce Merchant or use a Point-of-Sale (POS) or other device that connects to the Internet, you should have a Scanning Tab located at the top of your Trustwave Dashboard. Click on the Scanning Tab then click on Scan Results Tab.

Disputing. On some occasions, the Trustwave Scanner will find vulnerabilities and mark them as failing even though they may not be because your IT Department has some compensating controls in place or is using a version of software that is not affected by the vulnerability found or there may be a false positive. In these instances, your IT personnel can click the checkmark of the failed item(s) and then click on the Dispute Finding Button. They will then need to present Trustwave with satisfactory information as to why the finding is incorrect or if an exception is to be made. They should be prepared to answer any questions provided to them by Trustwave. Until the issue is resolved, the account will be considered to be in a failing status.

Correcting. Most of the time, the vulnerability is real and your IT will need to take steps to correct it. Oftentimes there may be several vulnerabilities that can all be corrected with a single action such as an update to software or an upgrade to the latest version of the software. In such cases, after your IT person makes corrective actions, he can login to your Trustwave Dashboard following the directions above, click on the Scan Setup Tab and then click on the Scan Now Link. This will schedule a new scan to determine whether the corrections made have been effectual. Your IT person may have to do these scans several times and make corrections as necessary until the scan passes.

In both cases above all of the failing PCI vulnerabilities must be addressed until passing. It is important to note that you only need to correct failing PCI vulnerabilities although it is a good idea to strive to correct all vulnerabilities found.

It should be noted that for PCI reporting purposes, Trustwave submits your scan results to the acquirer quarterly; however you should be aware that Trustwave scans your environment on a monthly basis and compares your results to newly discovered vulnerabilities. It is therefore possible to pass a vulnerability scan one month only to fail the next month's scan. Whenever you are notified by Trustwave that you have a failed scan you should immediately have your IT personnel correct the problem.

Answering the SAQ's

Regardless of which SAQ you need to complete for an account, Simplêfy recommends that you use Trustwave's Step-by-Step SAQ Wizard instead of answering the more detailed Expert Level SAQ Documents. The Wizard will keep track of answers that need further review in a "to-do" list.

Be honest with your answers. You should not change the answer of a question just to get past a question as that would defeat the purpose of completing the SAQ. If your answer is flagged and added to the "to-do" list, find out why and make corrections to your credit card processing environment that will enhance its security and allow you to honestly provide a passing answer. If you get lost in the questions or think that you are being asked complicated network related questions when all you have is a dial up terminal, you can click on the Start Over Link on your Trustwave Dashboard. It is located on the left side of the screen in the same section where you began your SAQ.

If you need help understanding a question, or have any other problems, please contact calexander@simplefy.com with your question or for further assistance.

Downloading Certifications And Seals

Once you have successfully completed your Annual SAQ and Quarterly Scans (If applicable) you can download your Certificates of Compliance and Attestation of Compliance. If you are an e-commerce merchant you can also download code that you can place on your website that will allow you to display Trustwave's Trusted Commerce Seal.

You can find these download links in the box in the middle of your Trustwave Dashboard. They are listed in this order: Trusted Commerce Seal, Certificate of Compliance and Attestation of Compliance. If you are not an e-commerce Merchant then the Trusted Commerce Seal link might not be available to you.

You do not need to send us these documents unless requested. Trustwave automatically sends them to the acquiring institution.

Security Policy Documents

Trustwave provides several Security Policy Documents you can download from your Trustwave Dashboard under the Security Policy Tab. These are simple, example templates that you can edit in a word processor or rich text editor and tailor to your business needs.

Security Awareness Training

Trustwave provides two types of Security Awareness Training, Basic and Premium. Under the Training Tab, select your Industry and then select your Training Options. The Basic Option allows you to have up to10 trainees, while the Premium lets you have an unlimited number of employees train and have access to a portal account, configurable training and progress reporting.

Trustwave Store

The Store Tab on your dashboard provides you access to order and pay for any additional Trustwave Products or Services that you may want or need. These include Website Security, PCI Network Protection, Premium Support, Vulnerability Management, Computer Security, Security Awareness Education and Two-Factor Authentication.

What To Do If Compromised?

If you believe or know you have had a security breach related to your cardholder environment you should follow the actions you outlined in your Incident Response Plan. If you do not have an incident response plan, Visa has a good instructional guidebook you can refer to located here:

http://usa.visa.com/download/merchants/cisp-what-to-do-if-compromised.pdf

You can read the guidebook and use relevant sections to help you create an incident response plan tailored to your business environment.

If you have been breached, you should immediately notify Simplêfy and we can assist you in notifying the acquiring bank and credit card providers for your account.

Other Resources

If you would like to read more about PCI DSS and keep up to date on any changes, please check you the following sources:

General Information

The PCI Security Standards Council: https://www.pcisecuritystandards.org/

https://www.pcisecuritystandards.org/security_standards/index.php

http://en.wikipedia.org/wiki/PCI_DSS

Validated Payment Applications

http://usa.visa.com/merchants/risk_management/data_security_demo/popup.html?popupwindow

Visa PAPB Validated Applications

https://www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php

Password Generators and Managers

For your convenience, I have included the following website that offers a free online Secure Password Generator:

http://passwordsgenerator.net/

You should change your passwords every 90 days. To help you remember and manage your passwords, you can download the free version of LastPass located here:

https://lastpass.com/misc_download2.php

Note: Some websites do not allow certain characters in passwords. For example, some web designers do not allow the following symbols in web form fields:

({ } [ ] ( ) / \ ' " ` ~ , ; : . < >)

The password generator at passwordsgenerator.com has a checkbox called "Exclude Ambiguous Characters" which will generate your password without using those symbols. You should make sure this checkbox is selected.

Enterprise Level Antivirus Software

http://enterprise.bitdefender.com/solutions/gravityzone/endpoint-security.html