CLEARGAGE®

Completing Your Self-Assessment Questionnaire

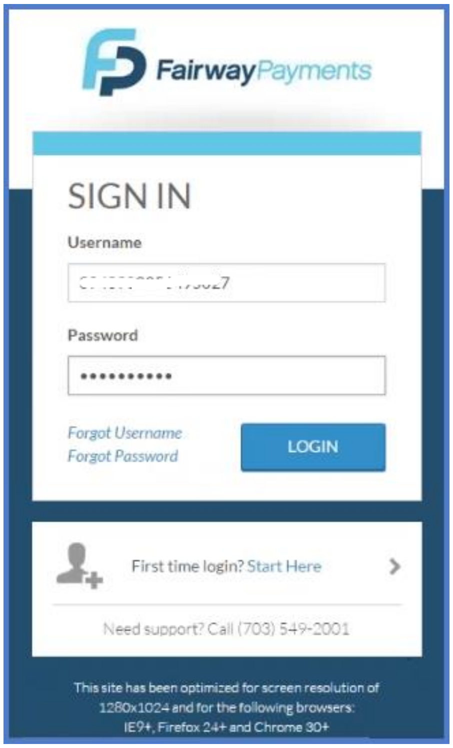
This document has been prepared as a guideline only. If you have questions specific to your situation contact the support number on the login screen (703) 549-2001. Depending upon some of your answers, you may see screens and questions that are *not* included in this guide. All answers should be reflective of your own company, ClearGage does not take responsibility for the way in which you answer questions.

Contents

Getting Started

Now that the Sage merchant account has been set up you will need to complete a Self-Assessment Questionnaire for PCI Certification. This is required because you play a vital role in protecting the cardholder data for each of your patients or clients.

You will have received an email from vthelp@sagepayments.com that contains directions and login information you need in order to complete your assessment.



SIGN IN

Username: [redacted]

Password: ••••••••••

Need support? Call (703) 549-2001

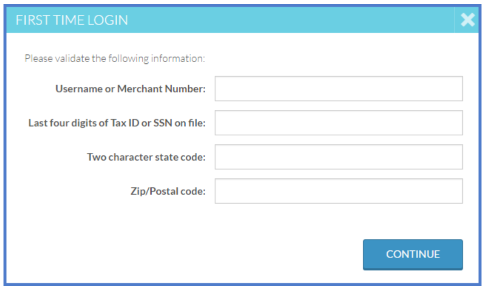
This site has been optimized for screen resolution of 1280x1024 and for the following browsers: IE9+, Firefox 24+ and Chrome 30+

The website to use is https://www.pciapply.com/pci2/fpi

The email from Sage provides you with your Merchant Account number and that is your User Name.

Your Password is the last 5 digits of your Merchant Account Number plus your two character state initials. i.e. 12345FL

If you need assistance in addition to this guide document please call the support line provided on the login page: 703-549-2001.



FIRST TIME LOGIN

Please validate the following information:

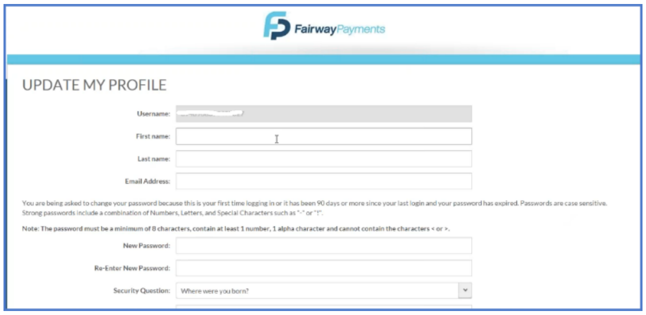
Username or Merchant Number:

Last four digits of Tax ID or SSN on file:

Two character state code:

Zip/Postal code:

Once logged in you will be asked to complete your profile information



UPDATE MY PROFILE

Username: [redacted]

First name:

Last name:

Email Address:

You are being asked to change your password because this is your first time logging in or it has been 90 days or more since your last login and your password has expired. Passwords are case sensitive. Strong passwords include a combination of Numbers, Letters, and Special Characters such as "-" or "!".

Note: The password must be a minimum of 8 characters, contain at least 1 number, 1 alpha character and cannot contain the characters < or >.

New Password:

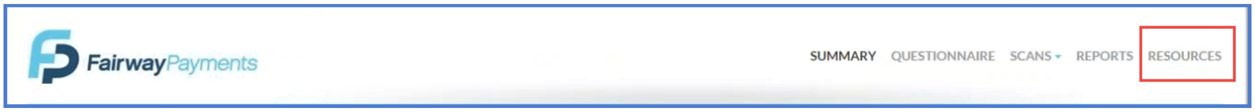
Re-Enter New Password:

Security Question: Where were you born?

Click “Submit”

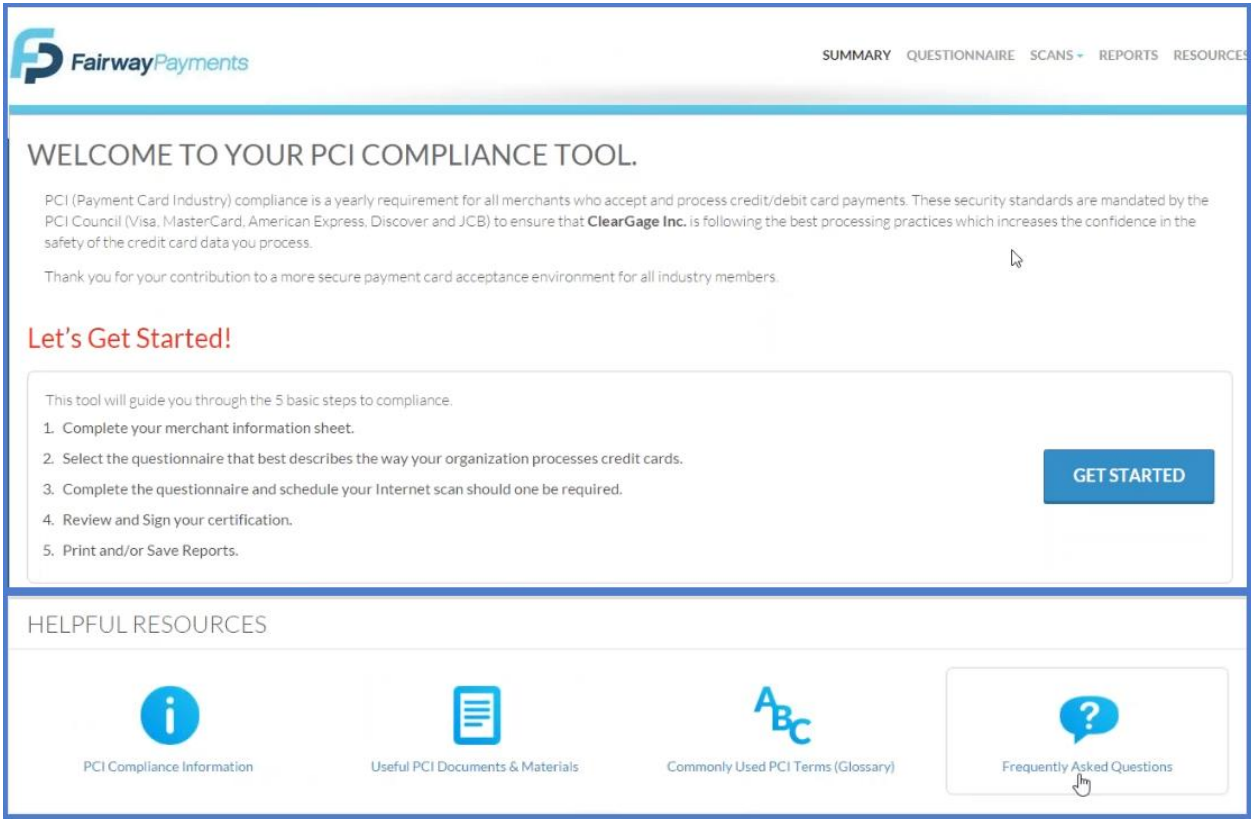
Resources

At any time you may click on the resources link in the upper right of the screen to obtain additional information. Selected documents have also been posted in the ClearGage Resource Center



Beginning the Process

First there will be an informational screen “Welcome to Your PCI Compliance Tool. There are some helpful links to documents at the bottom of this page.



WELCOME TO YOUR PCI COMPLIANCE TOOL.

PCI (Payment Card Industry) compliance is a yearly requirement for all merchants who accept and process credit/debit card payments. These security standards are mandated by the PCI Council (Visa, MasterCard, American Express, Discover and JCB) to ensure that **ClearGage Inc.** is following the best processing practices which increases the confidence in the safety of the credit card data you process.

Thank you for your contribution to a more secure payment card acceptance environment for all industry members.

Let’s Get Started!

This tool will guide you through the 5 basic steps to compliance.

1. Complete your merchant information sheet.
2. Select the questionnaire that best describes the way your organization processes credit cards.
3. Complete the questionnaire and schedule your Internet scan should one be required.
4. Review and Sign your certification.
5. Print and/or Save Reports.

GET STARTED
HELPFUL RESOURCES
PCI Compliance Information
Useful PCI Documents & Materials
Commonly Used PCI Terms (Glossary)
Frequently Asked Questions

Review the information on this screen and click “Get Started”.

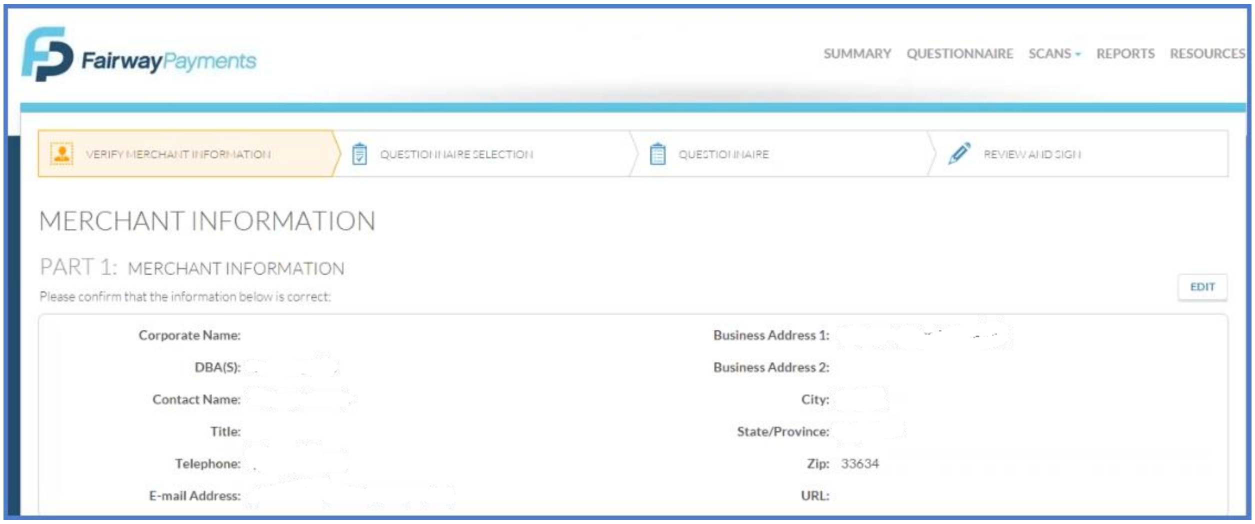
Starting the Questionnaire

There are four stages to the questionnaire and these are shown at the top of your screen so you can keep track of where you are.

Stage 1 Verify Merchant Information

In the Screen shot below we are at the Verify Merchant Information stage.
There are 3 parts to this stage

1. Verify your Merchant Information and use the edit button to make any changes.



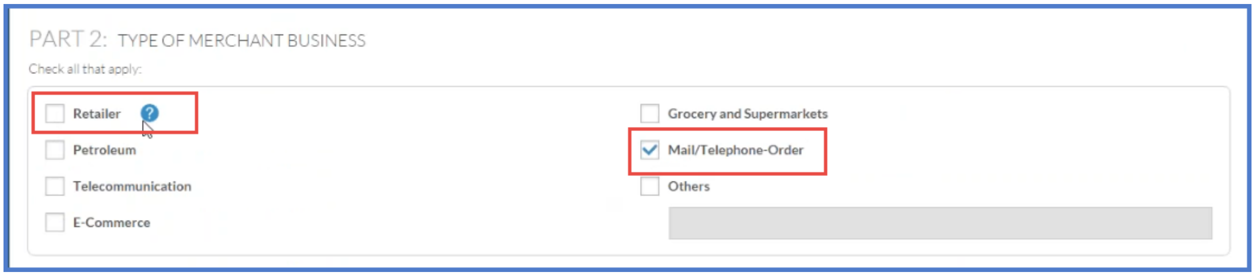
MERCHANT INFORMATION

PART 1: MERCHANT INFORMATION

Please confirm that the information below is correct:

Corporate Name:		Business Address 1:	
DBA(S):		Business Address 2:	
Contact Name:		City:	
Title:		State/Province:	
Telephone:		Zip:	33634
E-mail Address:		URL:	

2. Identify the type of Merchant Business
    a. If you are using ClearGage to process Payment Plans only and have a MOTO account, then check Mail/Telephone-Order ONLY.
    b. If you are using ClearGage to process Point of Sale (POS) transactions as well as Payment Plans and have a Retail account then check Retailer AND Mail/Telephone-Order.

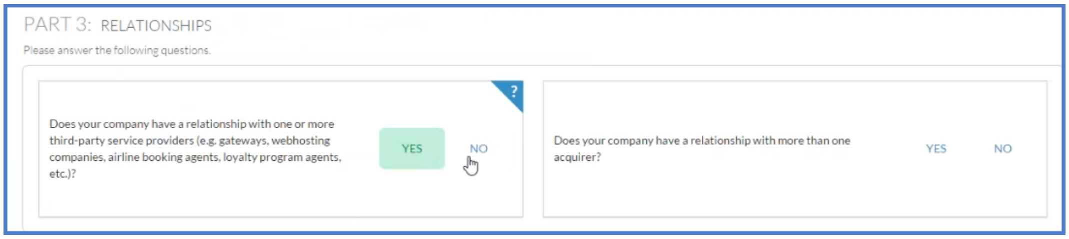


PART 2: TYPE OF MERCHANT BUSINESS

Check all that apply:

☐ Retailer	☐ Grocery and Supermarkets
☐ Petroleum	☑ Mail/Telephone-Order
☐ Telecommunication	☐ Others
☐ E-Commerce	

3. Relationships.
    a. Answer Yes to the first question
    b. If you are using another merchant account as well as Sage/ClearGage answer yes to the second question



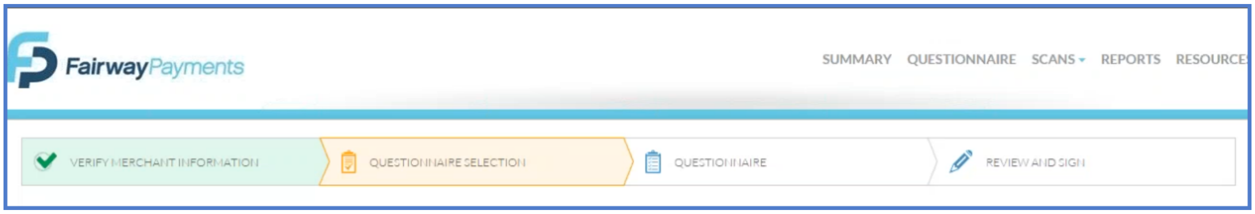
PART 3: RELATIONSHIPS

Please answer the following questions.

Does your company have a relationship with one or more third-party service providers (e.g. gateways, webhosting companies, airline booking agents, loyalty program agents, etc.)? [✓ YES] NO

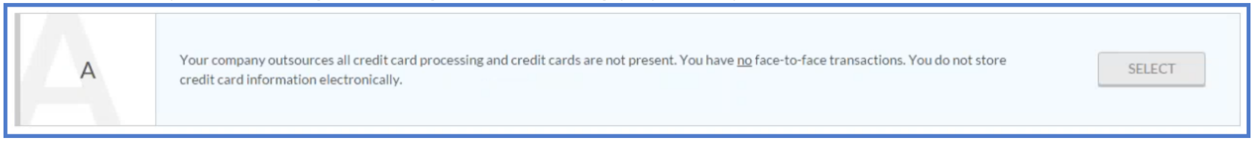
Does your company have a relationship with more than one acquirer? YES NO

Stage 2 Questionnaire Selection



In order to be sure that you are completing the correct Self-Assessment Questionnaire do the following:

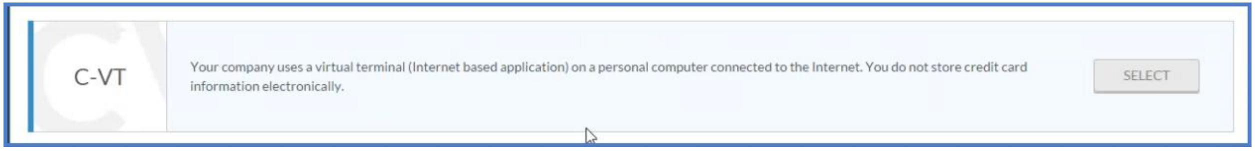
1. To the question "Would you like assistance in choosing the questionnaire that is appropriate for your company?" Answer "No"
2. Then, from the list that is presented select one of the following:
   a. A – if you are using ClearGage for recurring payment plan transactions ONLY



A

Your company outsources all credit card processing and credit cards are not present. You have no face-to-face transactions. You do not store credit card information electronically.

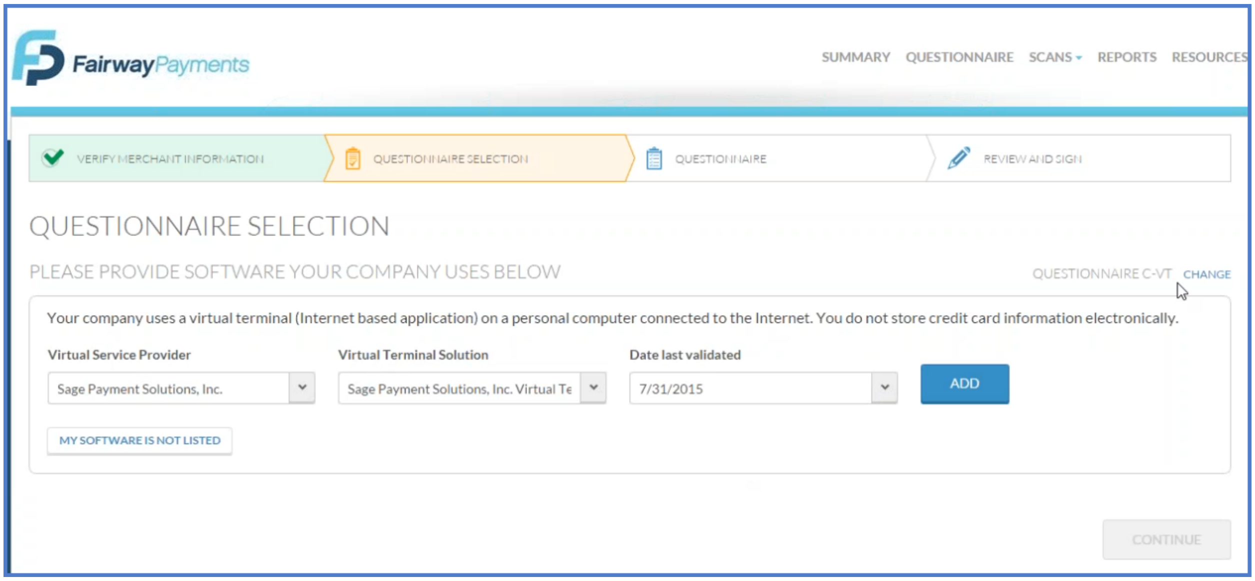
   b. C-VT - if you are using ClearGage for your retail Point Of Sale transactions AND your recurring payment plan transactions.



C-VT

Your company uses a virtual terminal (Internet based application) on a personal computer connected to the Internet. You do not store credit card information electronically.

3. In the drop-down boxes select Sage Payment Solutions In as the Virtual Service Provider, Sage Payment Solutions, Inc. Virtual Terminal as the Virtual Terminal Solution and 7/31/15 as the Date last validated.



QUESTIONNAIRE SELECTION

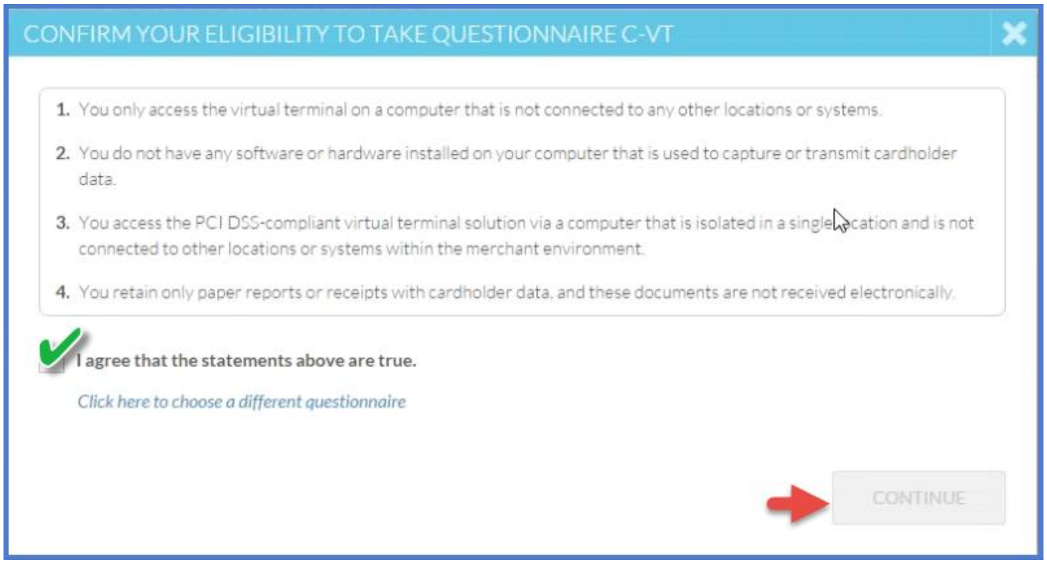
PLEASE PROVIDE SOFTWARE YOUR COMPANY USES BELOW

QUESTIONNAIRE C-VT CHANGE

Your company uses a virtual terminal (Internet based application) on a personal computer connected to the Internet. You do not store credit card information electronically.

Virtual Service Provider	Virtual Terminal Solution	Date last validated
Sage Payment Solutions, Inc.	Sage Payment Solutions, Inc. Virtual Te	7/31/2015

Click “ADD” and then “Continue”



CONFIRM YOUR ELIGIBILITY TO TAKE QUESTIONNAIRE C-VT

1. You only access the virtual terminal on a computer that is not connected to any other locations or systems.
2. You do not have any software or hardware installed on your computer that is used to capture or transmit cardholder data.
3. You access the PCI DSS-compliant virtual terminal solution via a computer that is isolated in a single location and is not connected to other locations or systems within the merchant environment.
4. You retain only paper reports or receipts with cardholder data, and these documents are not received electronically.

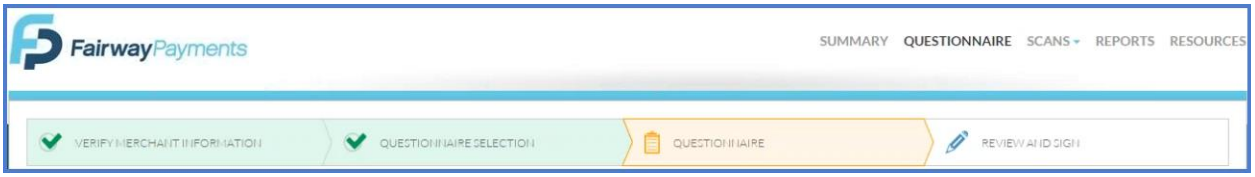
☑ I agree that the statements above are true.

Click here to choose a different questionnaire

Statement 1 of this screen is saying that you are using a computer that is at your location and is not connected via a network or via an internet connection that is used by some other business.
Statement 2 means that you do not, knowingly, have any other software on your computer that is going to capture and store any of the information entered or swiped using the ClearGage application.
Statement 3 means that the computer you are using is not on someone else’s network. For example, the business next door.
Statement 4 means that cardholder information is not being sent to someone else contained on a report. Receipts can be sent electronically but those do not include any cardholder data.

Check the “I Agree” box and click “Continue”

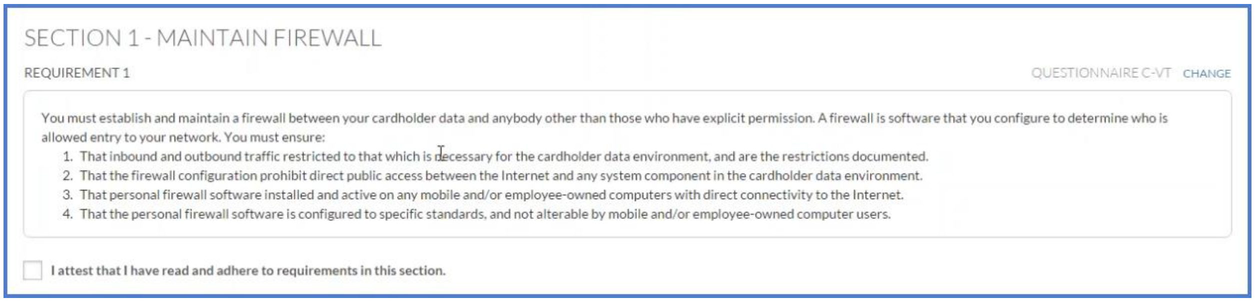
Stage 3 Questionnaire



This step is the actual completion of the SAQ – Self-Assessment Questionnaire. There are 9 sections within this step. For each section you will need to check the "I Attest" box and click "Continue" to move forward through the questionnaire.

Section 1 – Maintain Firewall.

The goal of having a firewall set up is to ensure that there is no public access and someone could not park in front of your location and get access to any cardholder data. You do need to have firewall protection in place.



SECTION 1 - MAINTAIN FIREWALL

REQUIREMENT 1

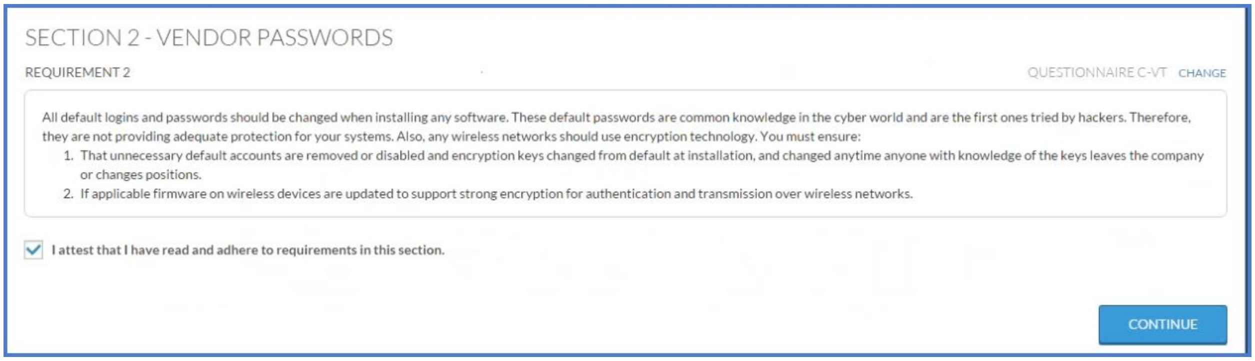
You must establish and maintain a firewall between your cardholder data and anybody other than those who have explicit permission. A firewall is software that you configure to determine who is allowed entry to your network. You must ensure:

1. That inbound and outbound traffic restricted to that which is necessary for the cardholder data environment, and are the restrictions documented.
2. That the firewall configuration prohibit direct public access between the Internet and any system component in the cardholder data environment.
3. That personal firewall software installed and active on any mobile and/or employee-owned computers with direct connectivity to the Internet.
4. That the personal firewall software is configured to specific standards, and not alterable by mobile and/or employee-owned computer users.

□ I attest that I have read and adhere to requirements in this section.

Section 2 – Vendor Passwords

To comply with this section, you should be using strong passwords to log in to any devices that are used when entering/processing credit card information as well as the ClearGage application. This also includes passwords to servers if you have servers or other network equipment. Strong passwords are generally 8 or more characters with at least 1 Number, Capital letter, and Symbol. It is generally advised that login information not be shared among multiple people.



SECTION 2 - VENDOR PASSWORDS

REQUIREMENT 2

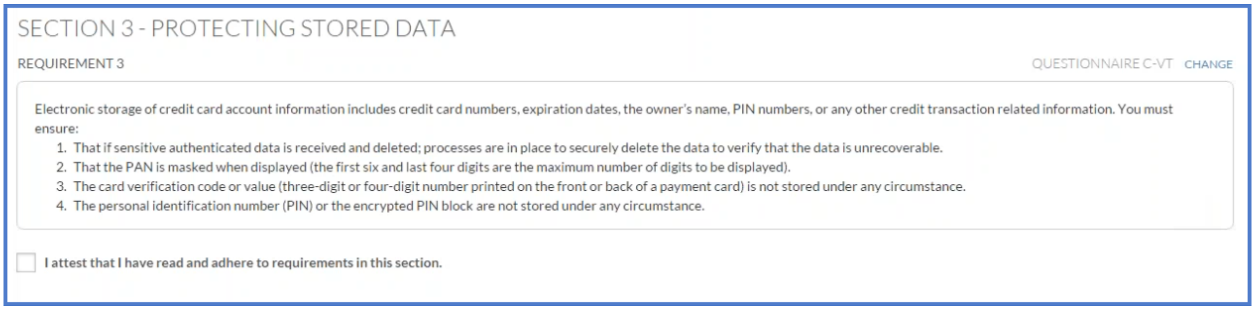
All default logins and passwords should be changed when installing any software. These default passwords are common knowledge in the cyber world and are the first ones tried by hackers. Therefore, they are not providing adequate protection for your systems. Also, any wireless networks should use encryption technology. You must ensure:

1. That unnecessary default accounts are removed or disabled and encryption keys changed from default at installation, and changed anytime anyone with knowledge of the keys leaves the company or changes positions.
2. If applicable firmware on wireless devices are updated to support strong encryption for authentication and transmission over wireless networks.

☑ I attest that I have read and adhere to requirements in this section.

Section 3 – Protecting Stored Data

The ClearGage Application is configured so that we do comply with the statements below.



SECTION 3 - PROTECTING STORED DATA

REQUIREMENT 3

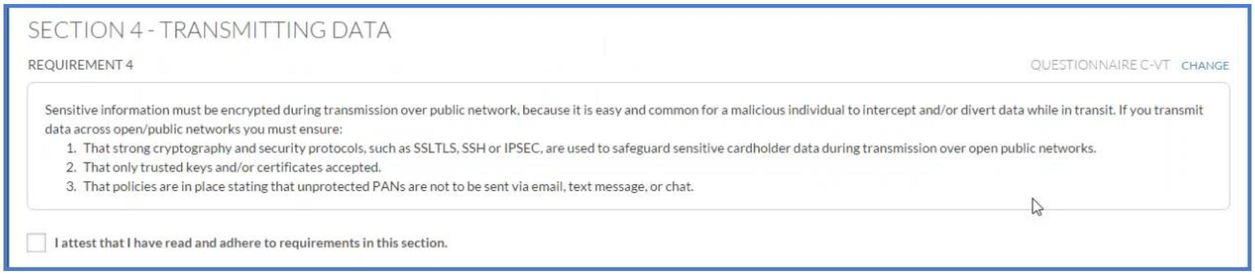
Electronic storage of credit card account information includes credit card numbers, expiration dates, the owner's name, PIN numbers, or any other credit transaction related information. You must ensure:

1. That if sensitive authenticated data is received and deleted; processes are in place to securely delete the data to verify that the data is unrecoverable.
2. That the PAN is masked when displayed (the first six and last four digits are the maximum number of digits to be displayed).
3. The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance.
4. The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance.

□ I attest that I have read and adhere to requirements in this section.

Section 4 – Transmitting Data

Again, the ClearGage application is configured to comply with the requirements for this section.



SECTION 4 - TRANSMITTING DATA

REQUIREMENT 4

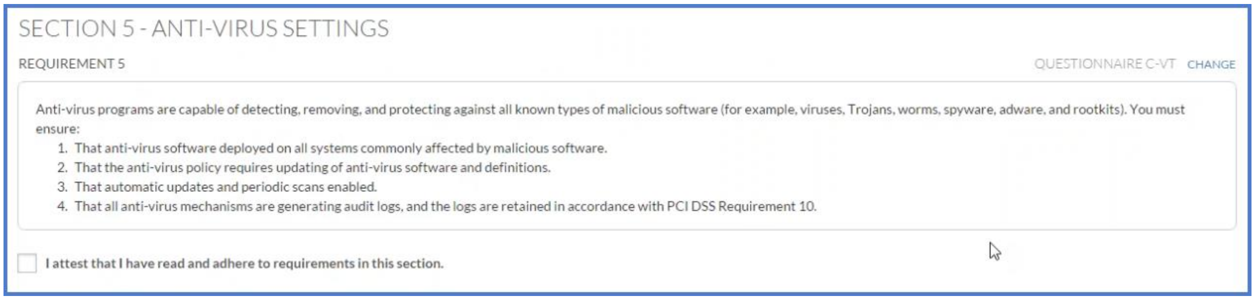
Sensitive information must be encrypted during transmission over public network, because it is easy and common for a malicious individual to intercept and/or divert data while in transit. If you transmit data across open/public networks you must ensure:

1. That strong cryptography and security protocols, such as SSLTLS, SSH or IPSEC, are used to safeguard sensitive cardholder data during transmission over open public networks.
2. That only trusted keys and/or certificates accepted.
3. That policies are in place stating that unprotected PANs are not to be sent via email, text message, or chat.

□ I attest that I have read and adhere to requirements in this section.

Section 5 – Anti-virus Settings

The requirement is that anti-virus protection is in place on any computer you are using with the ClearGage system to process credit card payments.



SECTION 5 - ANTI-VIRUS SETTINGS

REQUIREMENT 5

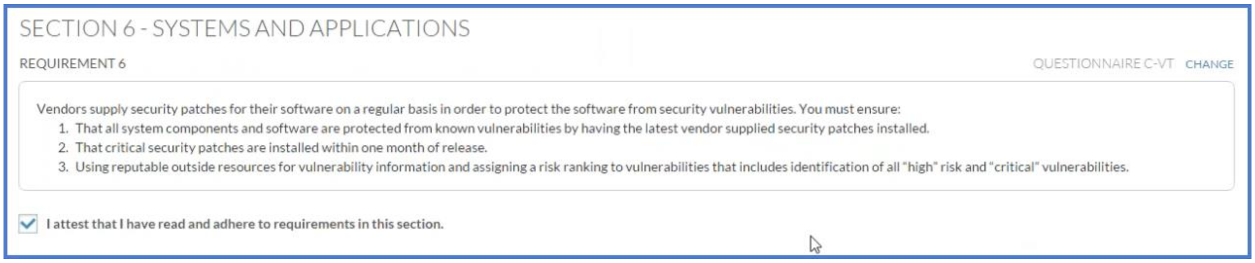
Anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits). You must ensure:

1. That anti-virus software deployed on all systems commonly affected by malicious software.
2. That the anti-virus policy requires updating of anti-virus software and definitions.
3. That automatic updates and periodic scans enabled.
4. That all anti-virus mechanisms are generating audit logs, and the logs are retained in accordance with PCI DSS Requirement 10.

□ I attest that I have read and adhere to requirements in this section.

Section 6 – Systems and Applications

ClearGage automatically applies patches and updates to all of its software and equipment. You should also be ensuring that your Windows updates, for example, are up-to-date on each computer and any servers that you are using as well as anti-virus updates.



SECTION 6 - SYSTEMS AND APPLICATIONS

REQUIREMENT 6

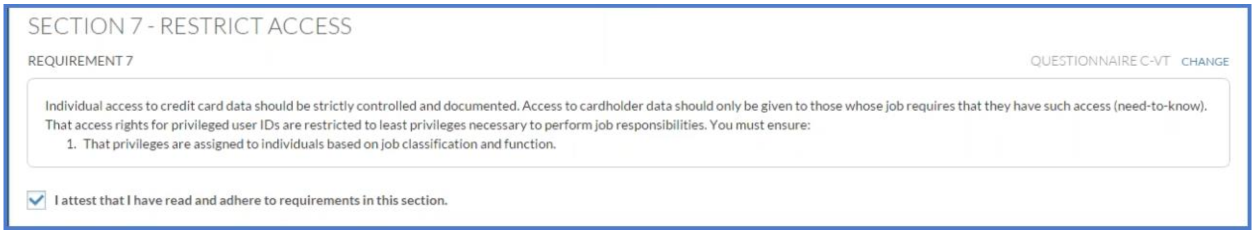
Vendors supply security patches for their software on a regular basis in order to protect the software from security vulnerabilities. You must ensure:

1. That all system components and software are protected from known vulnerabilities by having the latest vendor supplied security patches installed.
2. That critical security patches are installed within one month of release.
3. Using reputable outside resources for vulnerability information and assigning a risk ranking to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities.

☑ I attest that I have read and adhere to requirements in this section.

Section 7 – Restrict Access

There is no access to cardholder data within the ClearGage application.   However, you should be training staff that they cannot write down card information and if that is necessary then the information should be properly destroyed once no longer needed.



SECTION 7 - RESTRICT ACCESS

REQUIREMENT 7

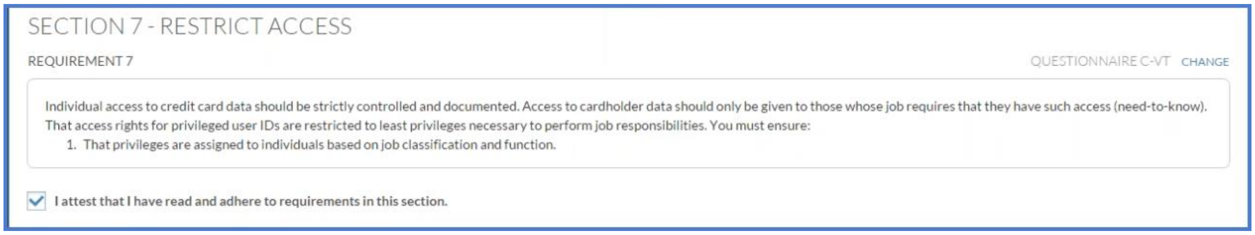
Individual access to credit card data should be strictly controlled and documented. Access to cardholder data should only be given to those whose job requires that they have such access (need-to-know). That access rights for privileged user IDs are restricted to least privileges necessary to perform job responsibilities. You must ensure:

1. That privileges are assigned to individuals based on job classification and function.

☑ I attest that I have read and adhere to requirements in this section.

Section 8 – Physical Access

As with Section 7, there is no access to cardholder data within ClearGage. Your staff training should include information about not writing cardholder information down and if it is necessary to do so then the information should be properly destroyed once no longer needed.



SECTION 7 - RESTRICT ACCESS

REQUIREMENT 7

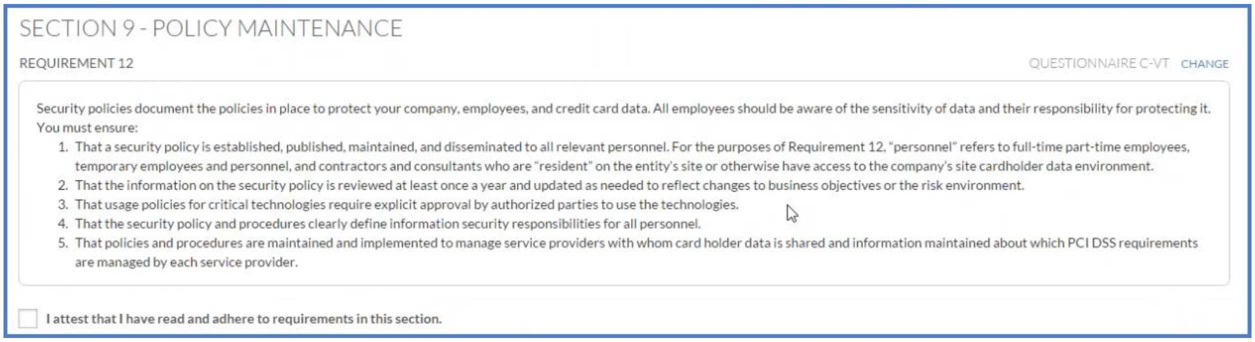
Individual access to credit card data should be strictly controlled and documented. Access to cardholder data should only be given to those whose job requires that they have such access (need-to-know). That access rights for privileged user IDs are restricted to least privileges necessary to perform job responsibilities. You must ensure:

1. That privileges are assigned to individuals based on job classification and function.

☑ I attest that I have read and adhere to requirements in this section.

Section 9 – Policy Maintenance

As a business, you are required to have a written policy that states that all employees working at your location are included. Identifying who (what job roles) have access to the ClearGage application and the task of taking/entering credit card information. Stating their responsibility in maintaining the confidentiality of credit card information.



SECTION 9 - POLICY MAINTENANCE

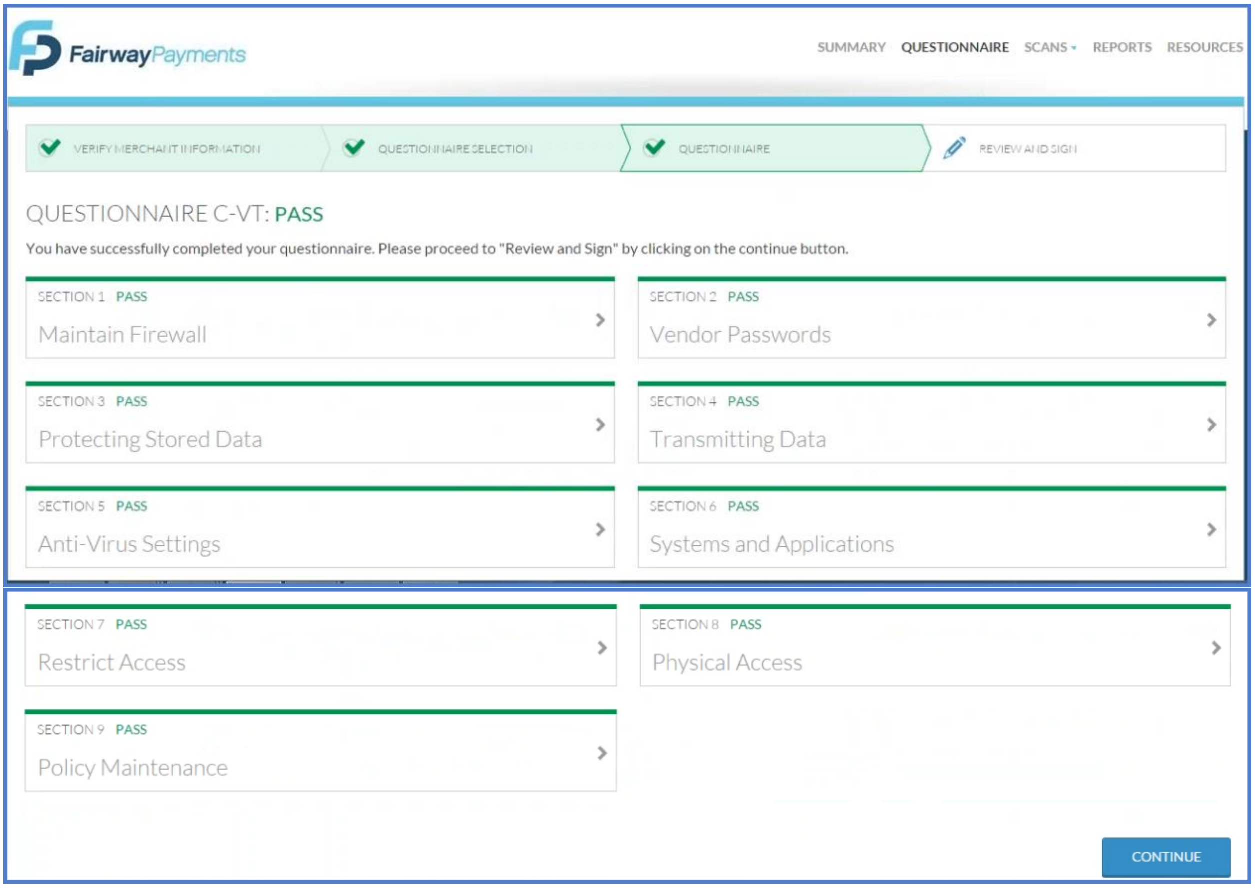
REQUIREMENT 12

Security policies document the policies in place to protect your company, employees, and credit card data. All employees should be aware of the sensitivity of data and their responsibility for protecting it. You must ensure:

1. That a security policy is established, published, maintained, and disseminated to all relevant personnel. For the purposes of Requirement 12, "personnel" refers to full-time part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site or otherwise have access to the company's site cardholder data environment.
2. That the information on the security policy is reviewed at least once a year and updated as needed to reflect changes to business objectives or the risk environment.
3. That usage policies for critical technologies require explicit approval by authorized parties to use the technologies.
4. That the security policy and procedures clearly define information security responsibilities for all personnel.
5. That policies and procedures are maintained and implemented to manage service providers with whom card holder data is shared and information maintained about which PCI DSS requirements are managed by each service provider.

□ I attest that I have read and adhere to requirements in this section.

The last screen in the Questionnaire step will indicate whether or not you have passed the questionnaire and will provide a summary of each of the sections.



QUESTIONNAIRE C-VT: PASS

You have successfully completed your questionnaire. Please proceed to "Review and Sign" by clicking on the continue button.

SECTION 1 PASS
Maintain Firewall

SECTION 2 PASS
Vendor Passwords

SECTION 3 PASS
Protecting Stored Data

SECTION 4 PASS
Transmitting Data

SECTION 5 PASS
Anti-Virus Settings

SECTION 6 PASS
Systems and Applications

SECTION 7 PASS
Restrict Access

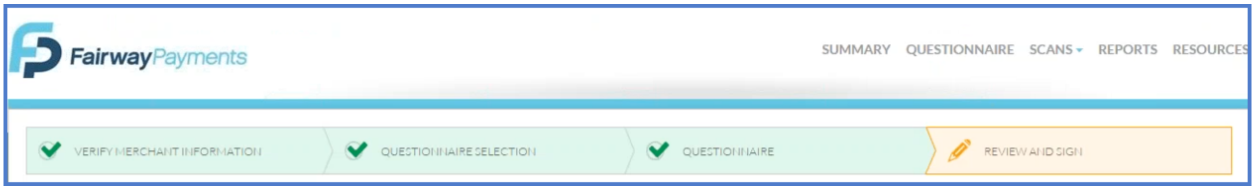
SECTION 8 PASS
Physical Access

SECTION 9 PASS
Policy Maintenance

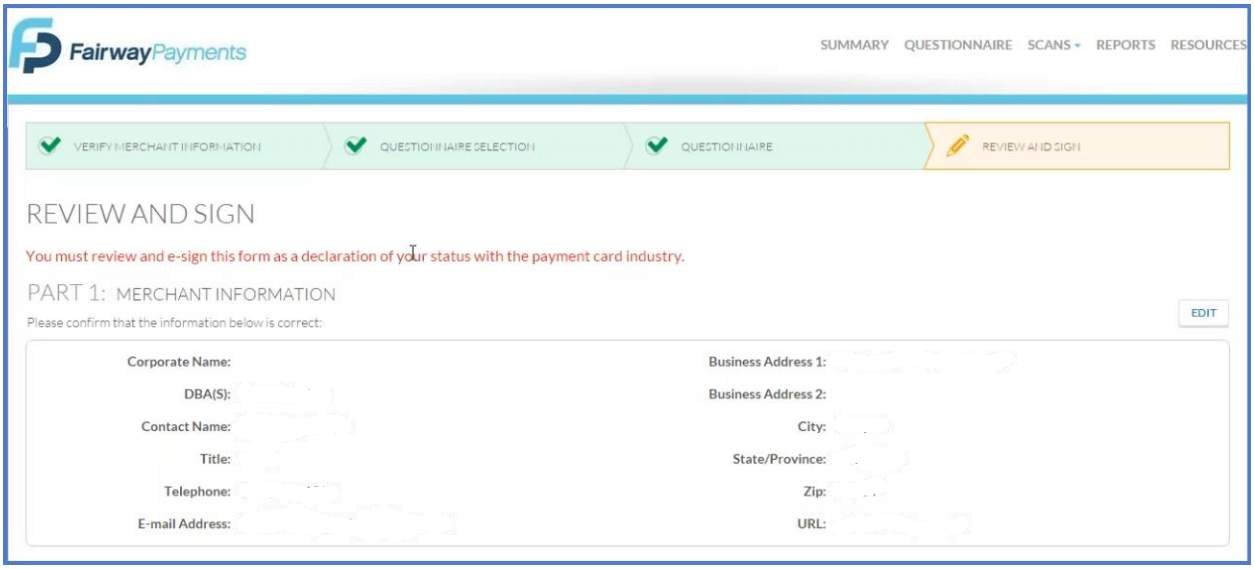
Click "Continue" to move to the final stage.

If your answers along the way resulted in the need for a vulnerability scan, you may not see the "Pass" information right away. The scan can take up to 24 hours. Log back into this site again tomorrow to see your results.

Stage 4 Review and Sign



Here you are provided with an opportunity to review all of the information in your submission.



REVIEW AND SIGN

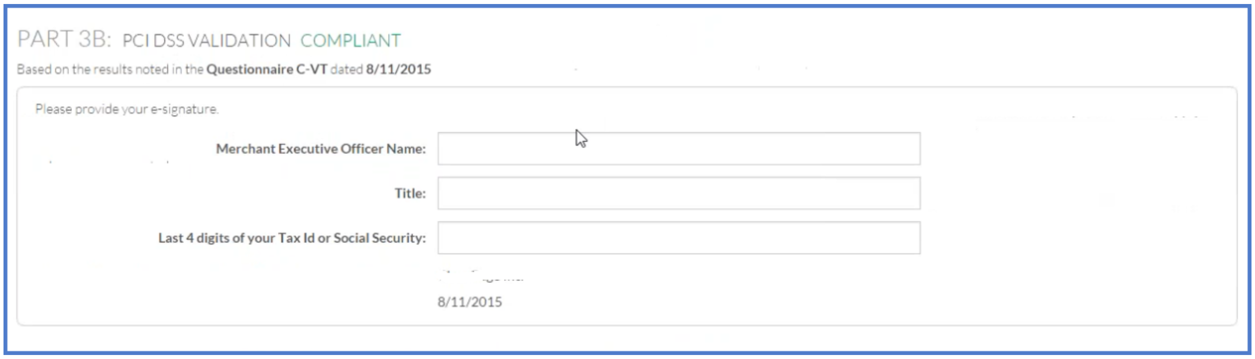
You must review and e-sign this form as a declaration of your status with the payment card industry.

PART 1: MERCHANT INFORMATION

Please confirm that the information below is correct:

Corporate Name:		Business Address 1:	
DBA(S):		Business Address 2:	
Contact Name:		City:	
Title:		State/Province:	
Telephone:		Zip:	
E-mail Address:		URL:	

Scroll to the bottom and complete the e-signature information and click “Submit”



PART 3B: PCI DSS VALIDATION COMPLIANT

Based on the results noted in the **Questionnaire C-VT** dated **8/11/2015**

Please provide your e-signature.

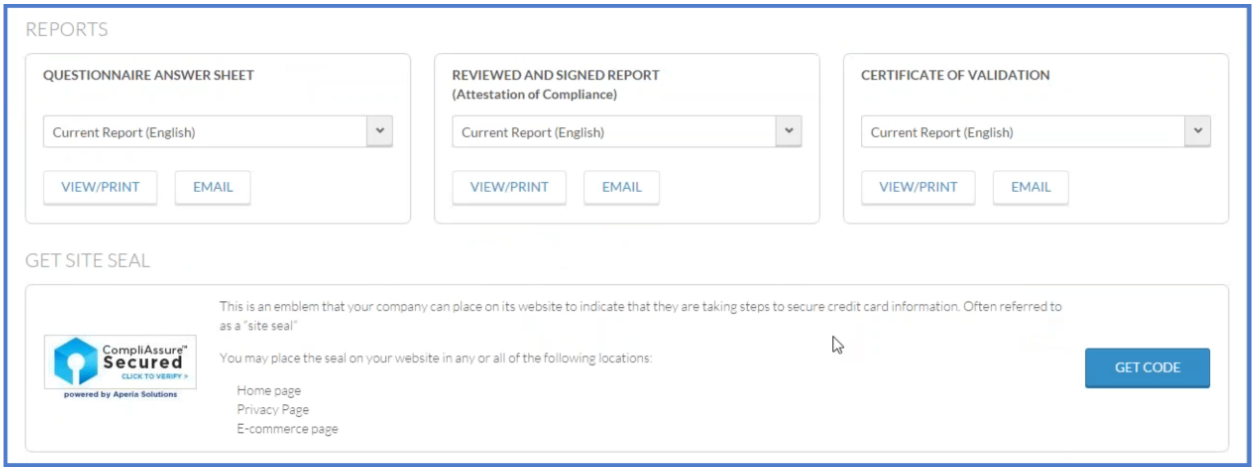
Merchant Executive Officer Name:

Title:

Last 4 digits of your Tax Id or Social Security:

8/11/2015

You can Print and/or Email the reports (recommended) so that you have them for your records and at the bottom of the page you are able to click on “Get Code” if you would like to have the HTML code in order to place the site seal on your website.



REPORTS

QUESTIONNAIRE ANSWER SHEET

Current Report (English)

VIEW/PRINT | EMAIL

REVIEWED AND SIGNED REPORT (Attestation of Compliance)

Current Report (English)

VIEW/PRINT | EMAIL

CERTIFICATE OF VALIDATION

Current Report (English)

VIEW/PRINT | EMAIL

GET SITE SEAL

This is an emblem that your company can place on its website to indicate that they are taking steps to secure credit card information. Often referred to as a "site seal"

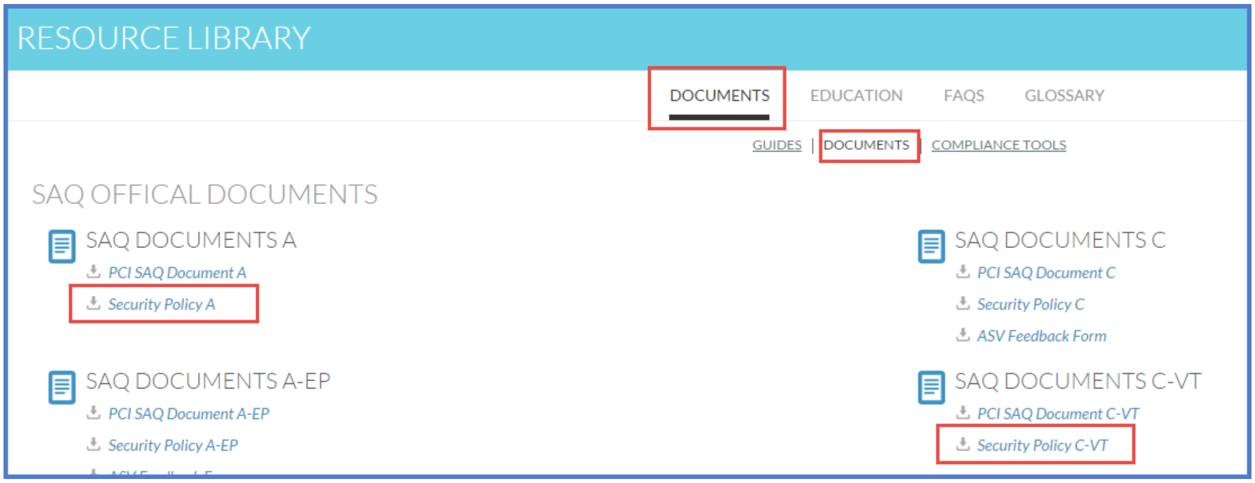
You may place the seal on your website in any or all of the following locations:

Home page
Privacy Page
E-commerce page

GET CODE

Sample Security Policies

You may obtain sample policy statement by Clicking on Resources in the upper right corner of this website. Then click on “Documents”, “Documents” (again), and select the policy that matches the questionnaire you are completing.



RESOURCE LIBRARY

DOCUMENTS | EDUCATION | FAQS | GLOSSARY

GUIDES | DOCUMENTS | COMPLIANCE TOOLS

SAQ OFFICAL DOCUMENTS

SAQ DOCUMENTS A
- PCI SAQ Document A
- Security Policy A

SAQ DOCUMENTS A-EP
- PCI SAQ Document A-EP
- Security Policy A-EP

SAQ DOCUMENTS C
- PCI SAQ Document C
- Security Policy C
- ASV Feedback Form

SAQ DOCUMENTS C-VT
- PCI SAQ Document C-VT
- Security Policy C-VT

Alternatively, you may go to the Resource Center in the ClearGage application and look for the PCI heading. You may use these policy samples as the starting point to craft your own.