SAQ User Guide
for
6Storage Merchants

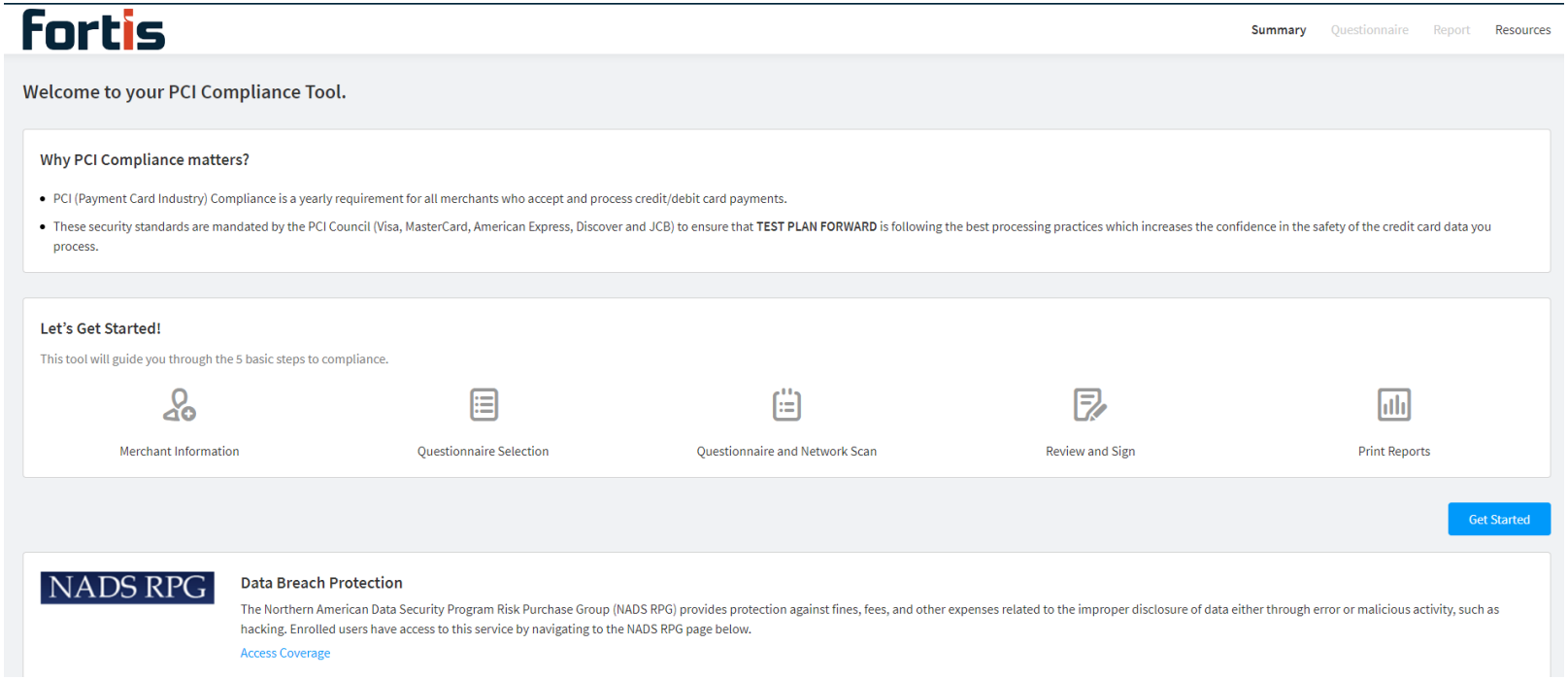
Overview

PCI Compliance is the responsibility of all entities that accept credit card payments for goods and services. Depending on your level of involvement in processing credit card transactions will determine the level of PCI compliance that must be achieved. Merchants that are using 6Storage as a processing solution are required to complete the Self-Assessment Questionnaire - A (SAQ-A). This user guide will lead the 6Storage Merchants through completing the SAQ-A.

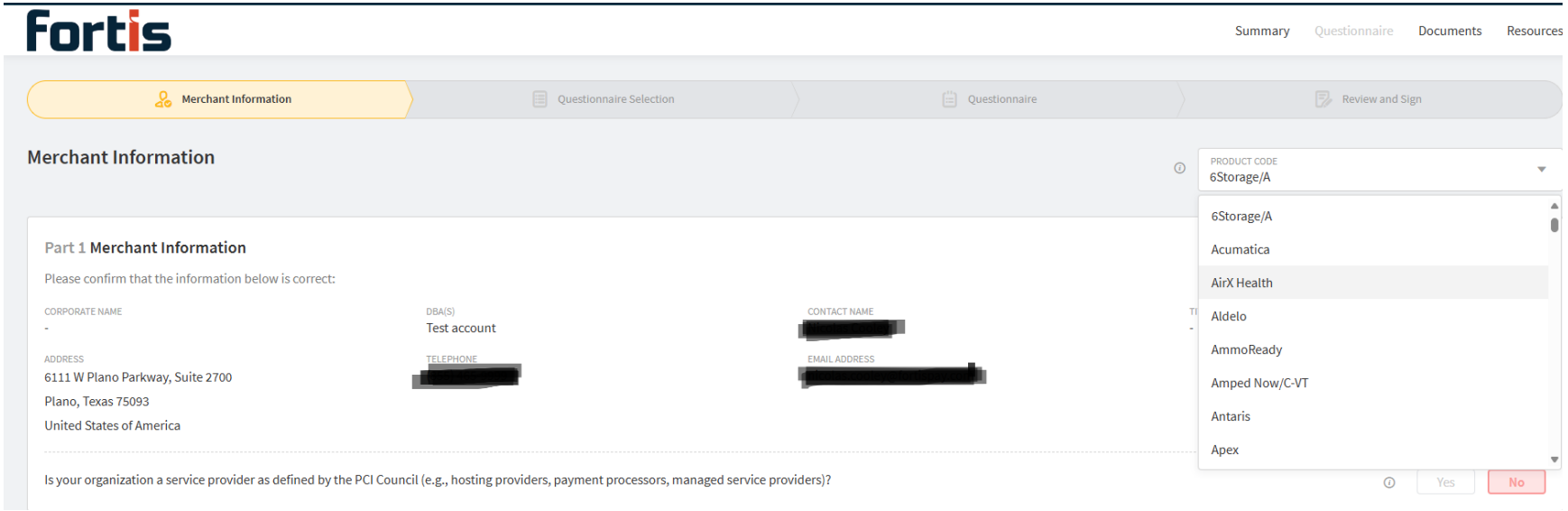
Getting Started

The merchant will receive a Welcome Email with instructions for logging into the PCI portal to complete compliance. The PCI compliance process should take approximately 15 minutes to complete. If the merchant requires assistance, they can contact the PCI Helpdesk by calling 855-826-2128 Option 1. After logging into the PCI Portal, please follow these instructions.

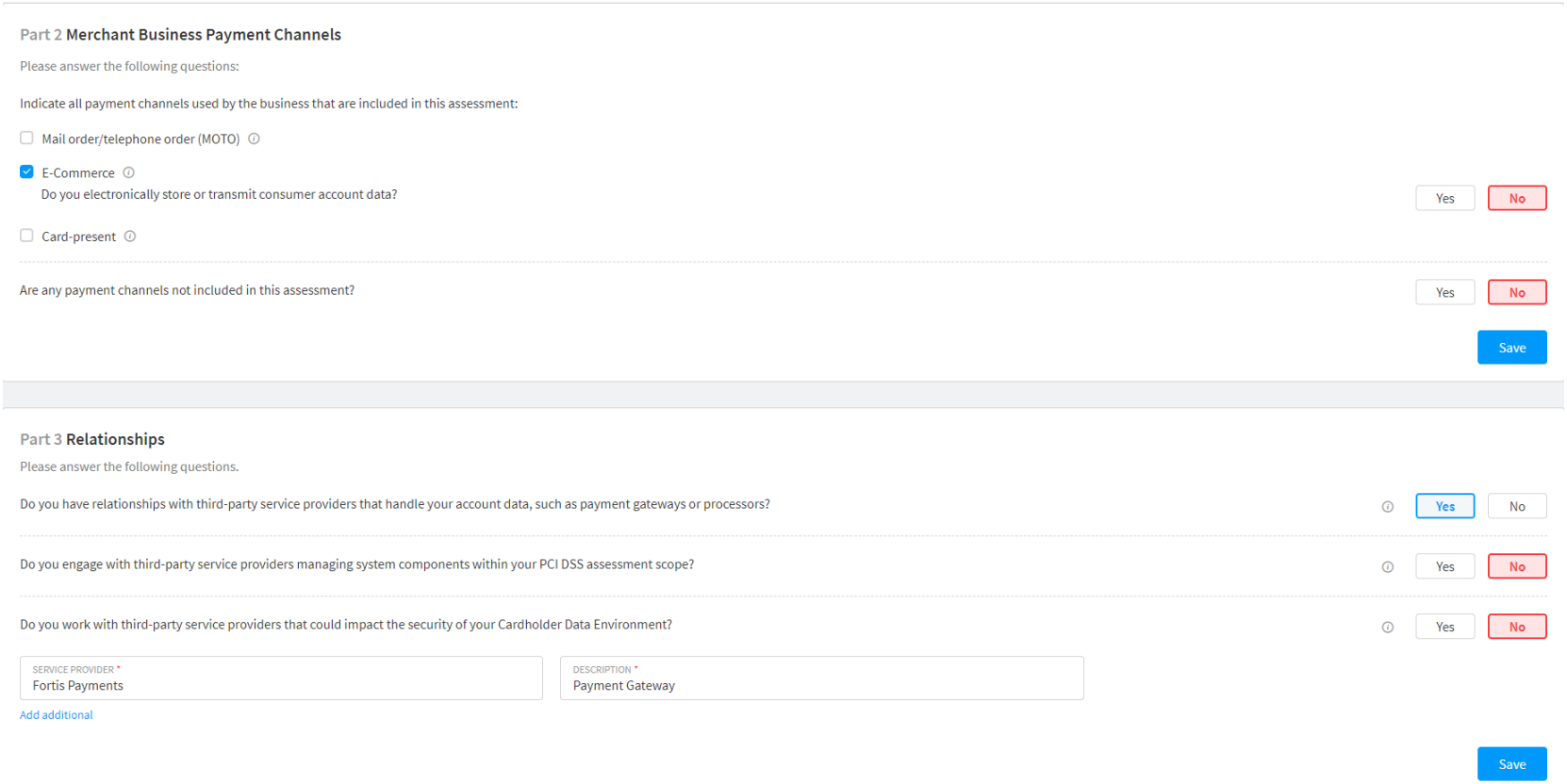
1. Select the blue “Get Started” button.



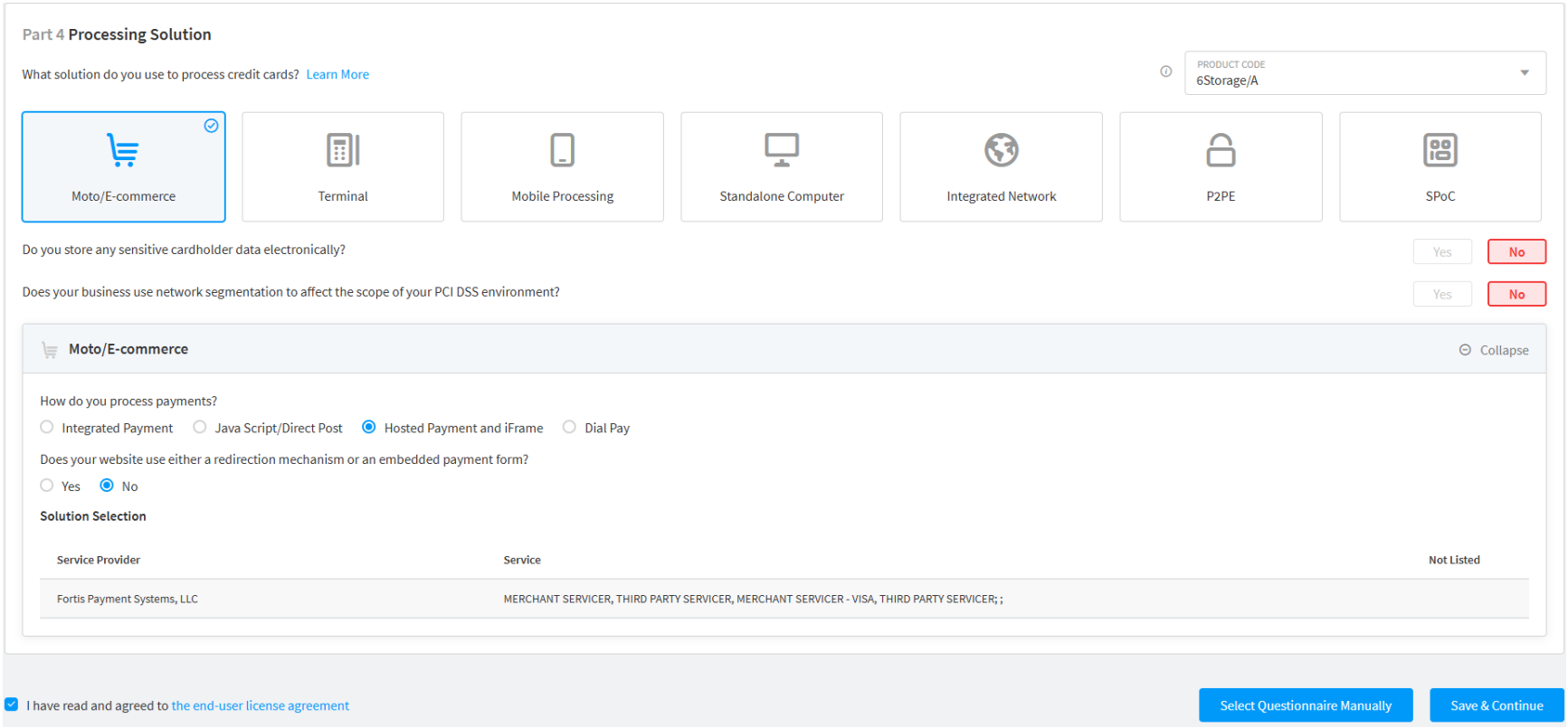
2. Verify that your information in Part 1 is correct and select “6Storage/A” from the Product Code drop down menu. The selection of a Product Code will complete some of the answers to the required questions. Please verify the questions are accurate for how you process payments.



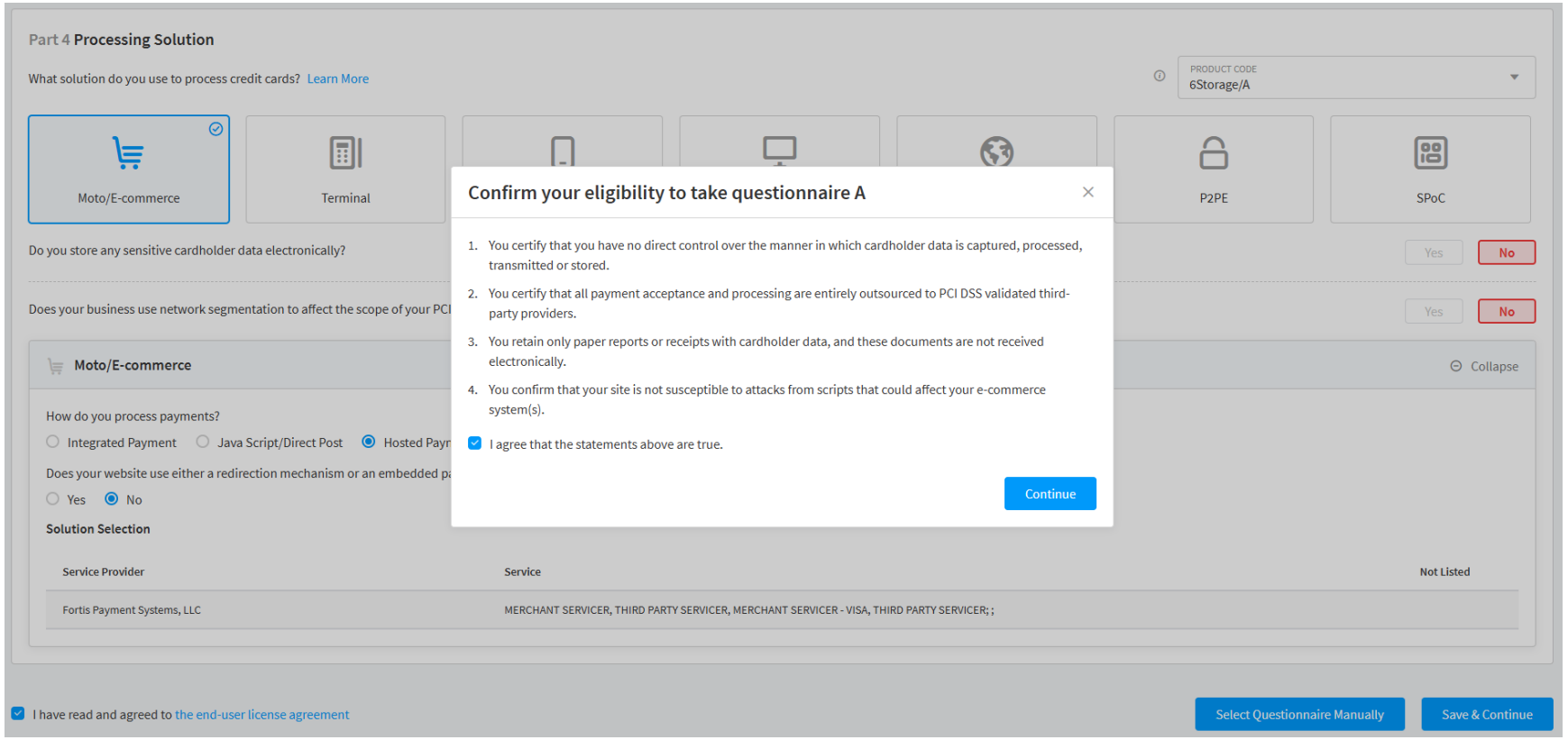
3. Select E-Commerce if it is not selected and answer the question. When asked if you are storing consumer account data you can answer “No,” unless you are storing customers account data on your systems. If you are unsure contact the Fortis PCI team 855-465-9999. Part 3 relationships should be completed for you, if not see below screen shot.



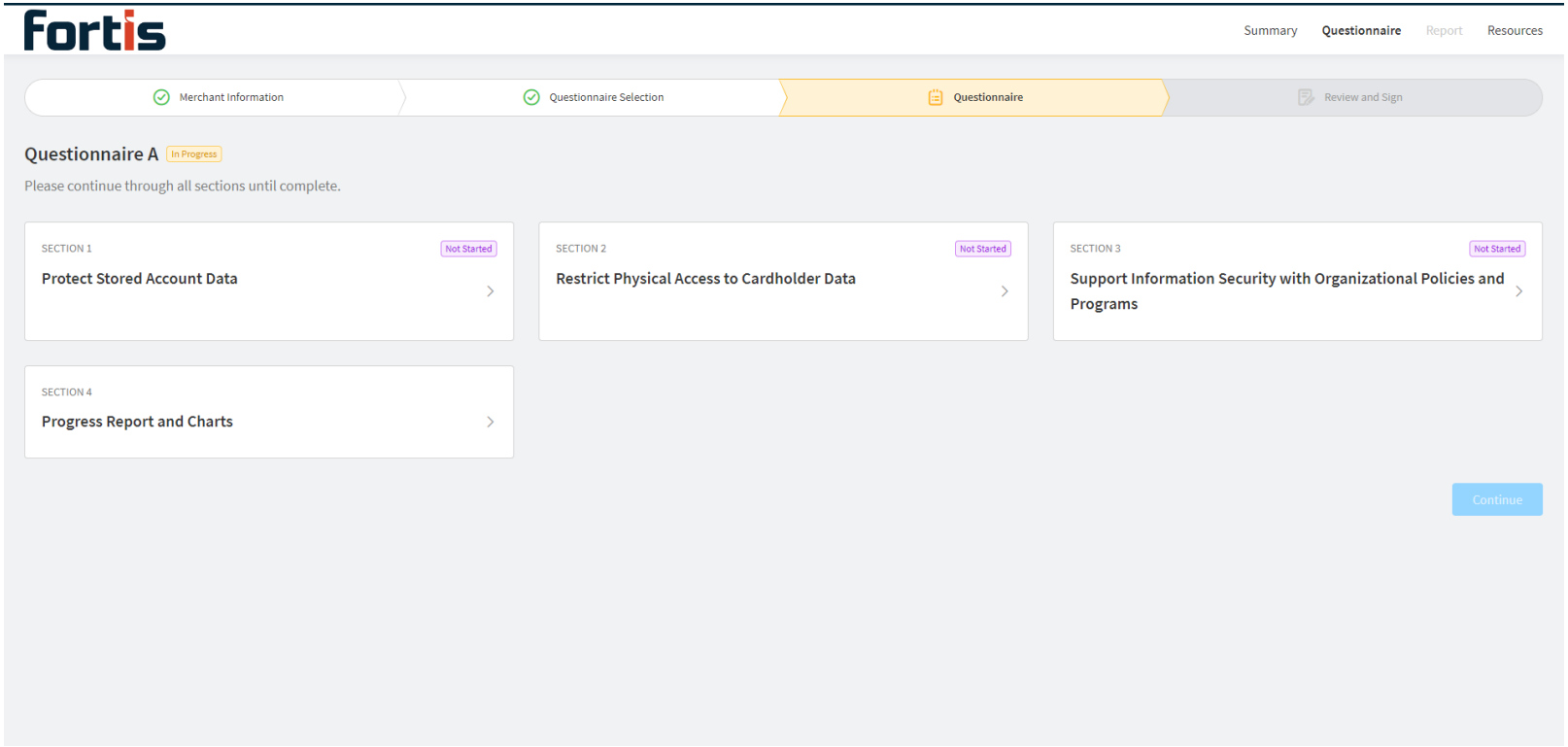
4. Part 4 should also be completed for you, if not please follow the example below. Once this is completed select the “I have read and agree” box and save and continue.



5. Confirm eligibility to complete SAQ-A by selecting I agree statement and press continue.



6. Complete the questionnaire sections by clicking “Section 1” reading the guideline and attesting to statements. Select continue after each section is completed. Note: Section 4 is not required.



Summary **Questionnaire** Report Resources

Merchant Information | Questionnaire Selection | **Questionnaire** | Review and Sign

Questionnaire A In Progress

Standard SAQ Change Questionnaire

You have completed **0** of **4** sections Show all Sections

Section 1 Protect Stored Account 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.

Continue

Summary Questionnaire Report Resources

Merchant Information | Questionnaire Selection | Questionnaire | Review and Sign

Questionnaire A In Progress

Standard SAQ Change Questionnaire

You have completed **1** of **4** sections Show all Sections

Section 2 Restrict Physical Access to Cardholder Data

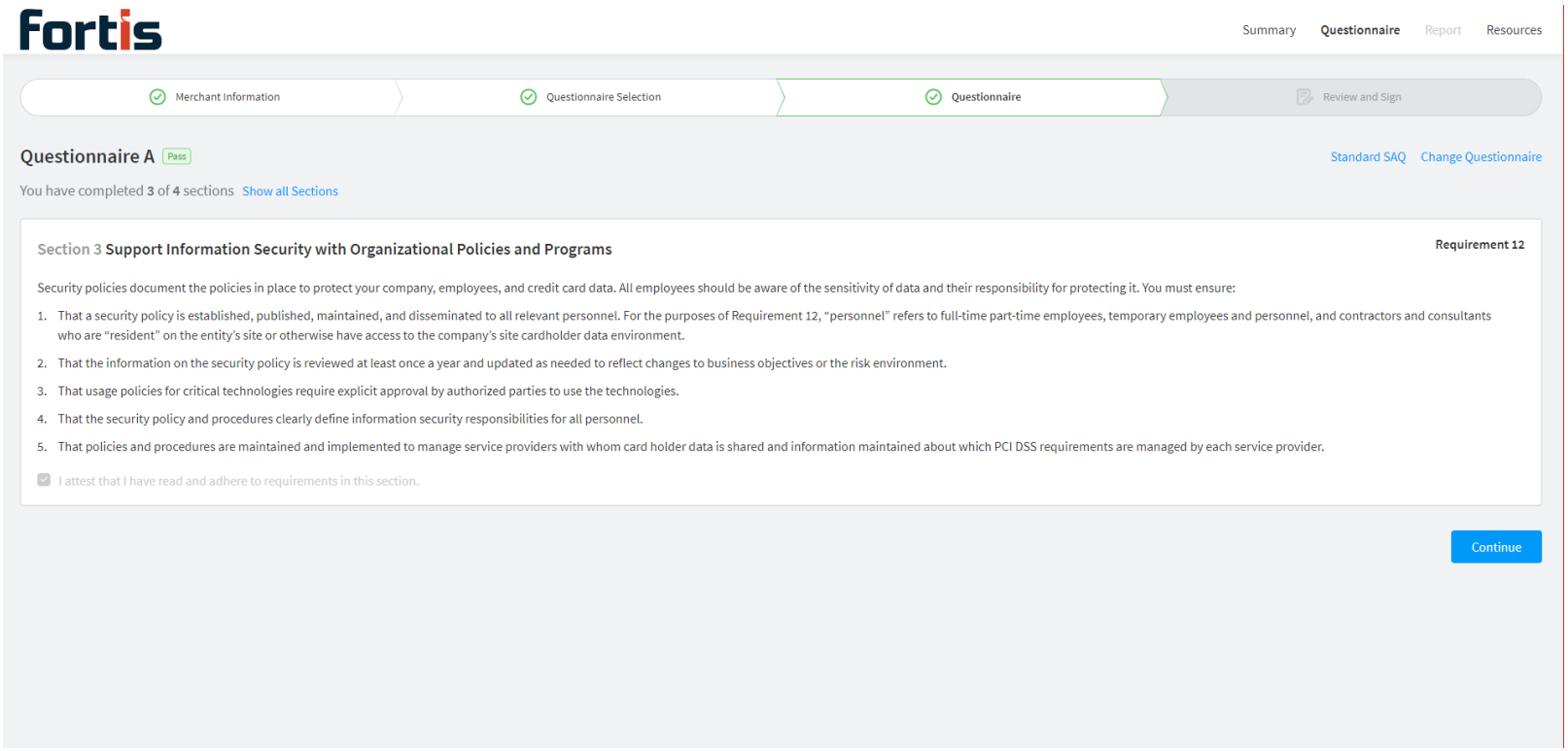
Requirement 9

Cardholder data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected while it is on removable or portable media, printed out, or left on someone's desk. You must ensure:

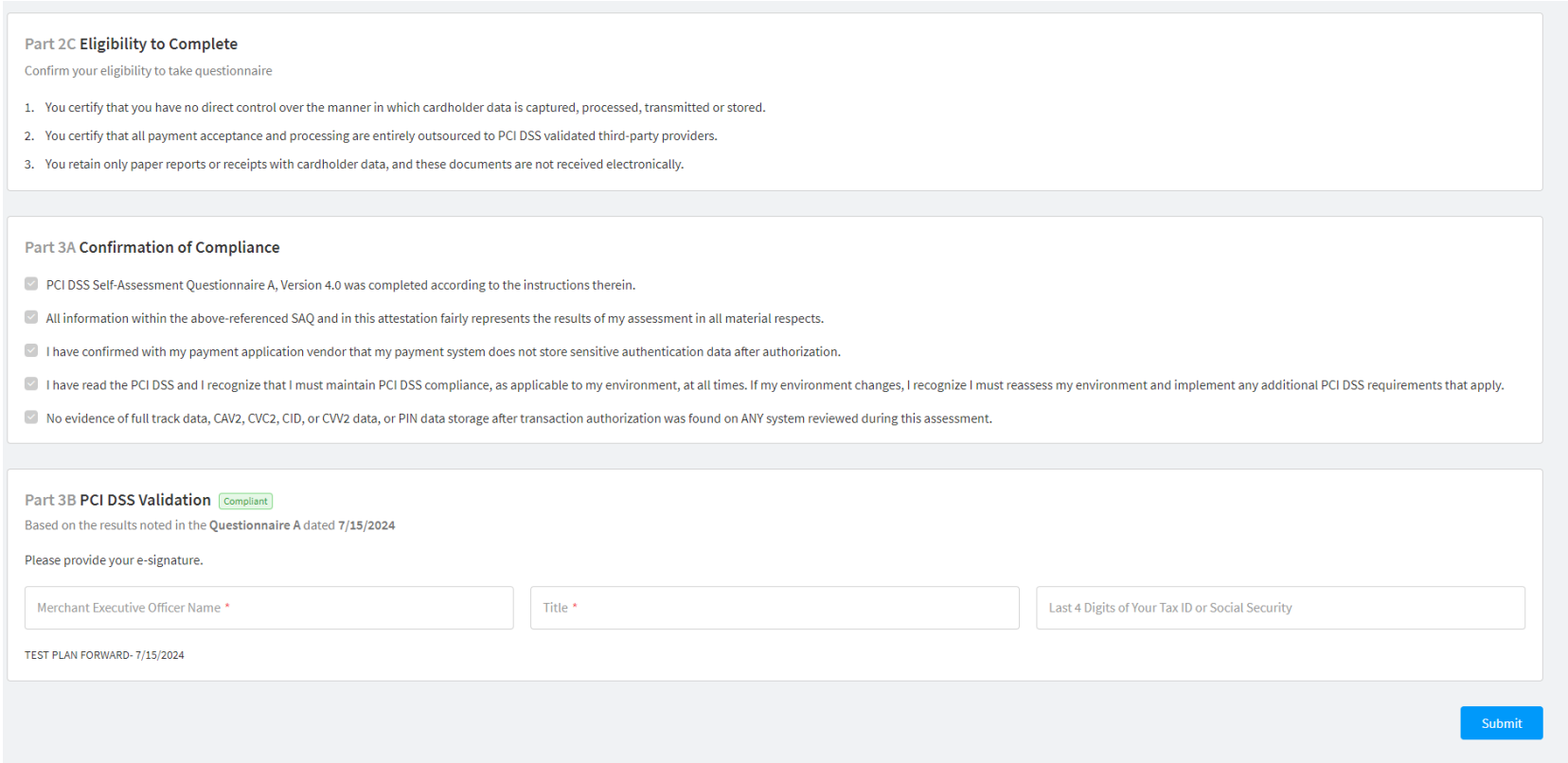
1. That all media is physically secured.
2. That strict control is maintained over the internal or external distribution of any kind of media.
3. That media is classified so the sensitivity of the data can be determined.
4. That media sent by secured courier or other delivery methods can be accurately tracked.
5. That logs are maintained to track media that is moved from secured areas has management approval prior to moving the media.
6. That the destruction of data is done by means of shredding, burning or pulping when it is no longer needed for business or legal reasons.

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

Continue


Fortis
Summary
Questionnaire
Report
Resources
Merchant Information
Questionnaire Selection
Questionnaire
Review and Sign
Questionnaire A
Pass
Standard SAQ
Change Questionnaire
You have completed 3 of 4 sections
Show all Sections
Section 3 Support Information Security with Organizational Policies and Programs
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.
Continue

7. Verify all information is correct and electronically sign at the bottom of the page.



Part 2C **Eligibility to Complete**

Confirm your eligibility to take questionnaire

1. You certify that you have no direct control over the manner in which cardholder data is captured, processed, transmitted or stored.
2. You certify that all payment acceptance and processing are entirely outsourced to PCI DSS validated third-party providers.
3. You retain only paper reports or receipts with cardholder data, and these documents are not received electronically.

Part 3A **Confirmation of Compliance**

- [x] PCI DSS Self-Assessment Questionnaire A, Version 4.0 was completed according to the instructions therein.
- [x] All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
- [x] I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
- [x] I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times. If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.
- [x] No evidence of full track data, CAV2, CVC2, CID, or CVV2 data, or PIN data storage after transaction authorization was found on ANY system reviewed during this assessment.

Part 3B **PCI DSS Validation** Compliant

Based on the results noted in the **Questionnaire A** dated **7/15/2024**

Please provide your e-signature.

Merchant Executive Officer Name *

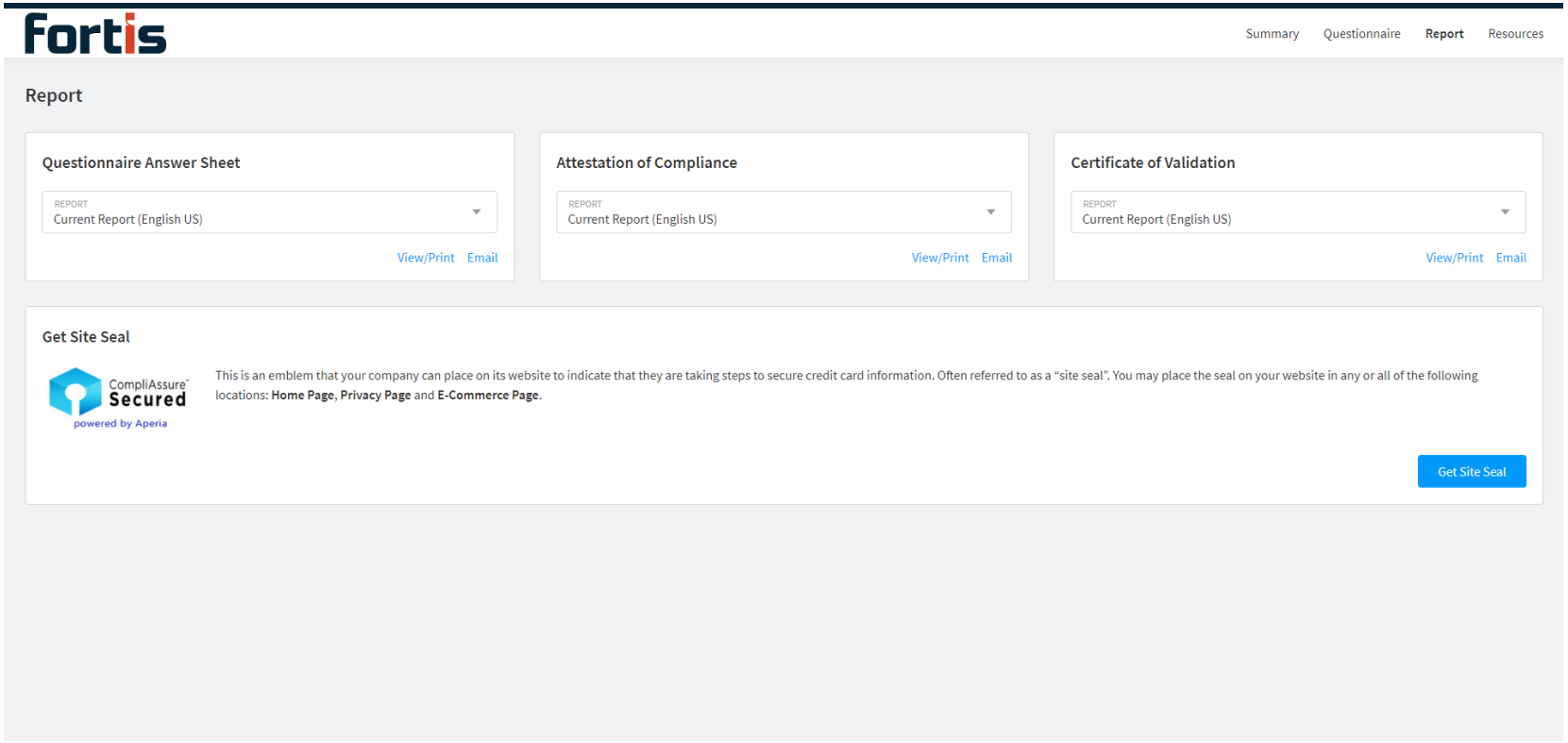
Title *

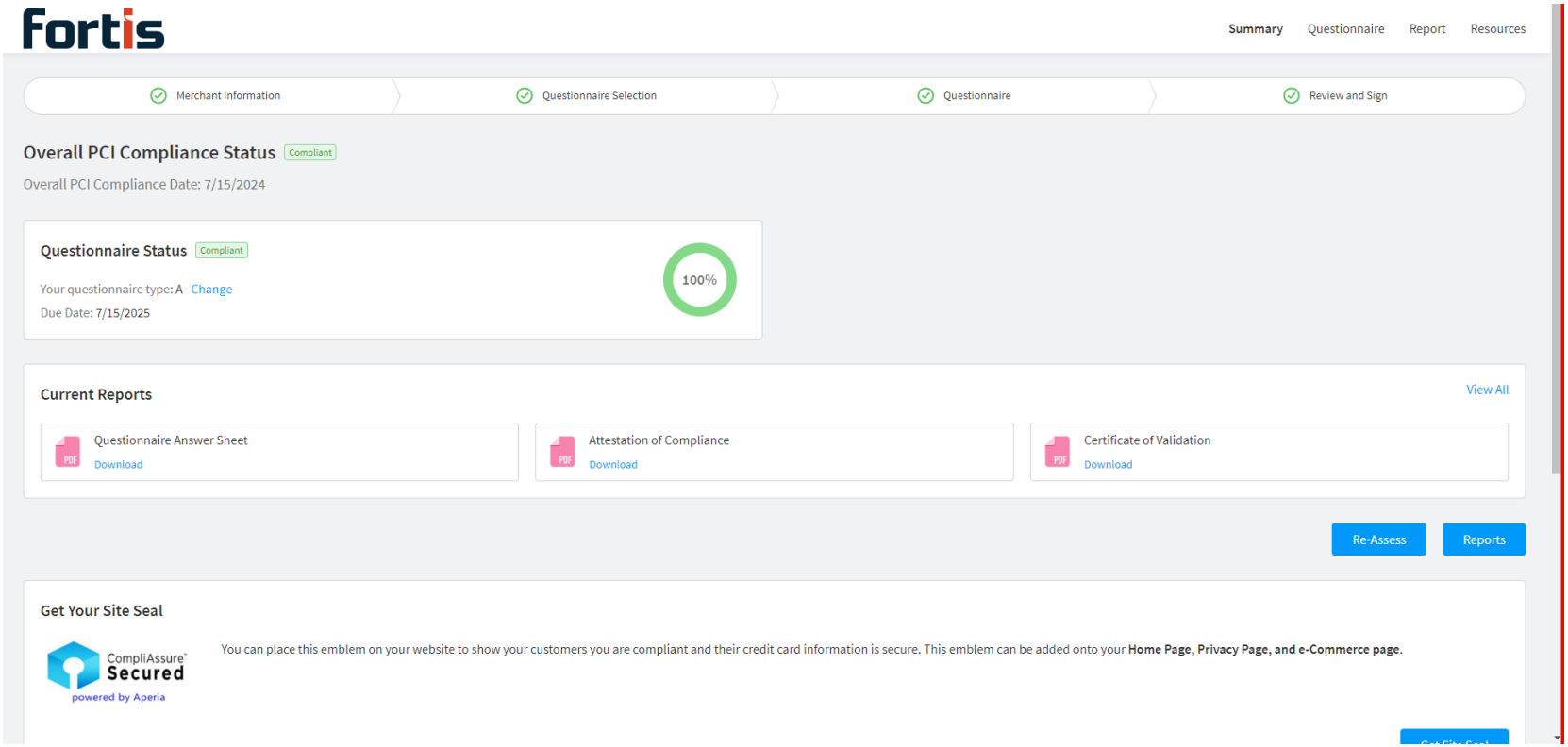
Last 4 Digits of Your Tax ID or Social Security

TEST PLAN FORWARD- 7/15/2024

Submit

8. You will be able to download your PCI compliance documentation.





Congratulations, you have completed PCI compliance! You will have peace of mind knowing you are doing your part to protect customers' data!

FAQs

- Who do I contact if I need assistance? You can contact the PCI Helpdesk by calling 855-826-2128 option 1.

- Do I have to complete PCI Compliance? All merchants that collect credit card payments are required to attest to their role in processing credit card information.

- What happens if I don't complete compliance? Failure to complete compliance will result in being assessed a monthly PCI Non-compliance fee.

- How long is compliance valid? Compliance is good for one year from the date compliance was completed.

- Will I receive notification that PCI compliance is going to expire? Thirty days before compliance expires you will receive an email. However, it is recommended that you create a calendar reminder for 10-15 days before expiration in the event there is an email failure (i.e. email sent to spam folder or glitch in automated email system).