

PCI Compliance Guide

Already have a login with SecureTrust? Please select login and skip to step 5.

Simply need to renew? Please skip to the end of page 11 to follow the "express renewal" guide.

Account Setup

Step 1: Go to <https://pci.securetrust.com/cardconnect>

Next, click the 'Get Started' button

Welcome to the CardConnect PCI Program



Getting Started with
SecureTrust™ PCI Manager is easy.

Register your business today.

Get Started

Already Registered? [Login](#)

Welcome to the CardConnect PCI Program . This program is designed to help you understand and respond to the data security needs of your business - especially if you accept credit cards for payment.

To get started, you **simply need to register**. The PCI wizard will walk you through the self-assessment process.


Step 2: Enter your company information and authorized contact details to begin the registration process. Click 'Next.'

<div> Business Information</div> <div>Company Name * <input type="text" value="CardConnect Test"/></div> <div>Merchant ID * <input type="text" value="12345654321"/></div> <div>Country * <input type="text" value="United States of America"/></div> <div>ZIP/Postal Code * <input type="text" value="19406"/></div>	<div> Contact Responsible For Certification</div> <div>First * <input type="text" value="First Name"/></div> <div>Last * <input type="text" value="Last Name"/></div> <div>Email * <input type="text" value="email@cardconnect.com"/></div> <div>Phone * <input type="text" value="877-828-0720"/></div>	<div> Resources Available</div> <div> 1-877-257-0239</div> <div> ccsupport@securetrust.com</div>
--	---	--

Step 3: Complete the creation of your account credentials and security questions. Check the box next to 'Accept License Agreement.' Click 'Register.'

1
Start

2
Activate


**Account Credentials**

Username *

j.consumer2020

Password *

Verify Password *


**Account Offering**

Cost

Covered by your relationship with CardConnect

Acknowledgement *

☒ Accept license agreement Show User Terms and Conditions

**Security Questions**

Question *

In what city was your mother born?

Answer *

FakeAnswer123

Question *

What was your favorite restaurant in college?

Answer *

FakeAnswer123


Question *

What was the first name of your first manager?

Answer *

FakeAnswer123

Step 4: Upon registering you will be taken to a summary page. Click 'Continue.'


**PCI Program**

Reporting To

CardConnect

Merchant ID

CardconnectRegTest


**Account Information**


Company


CardconnectRegTest

Customer ID

11749438

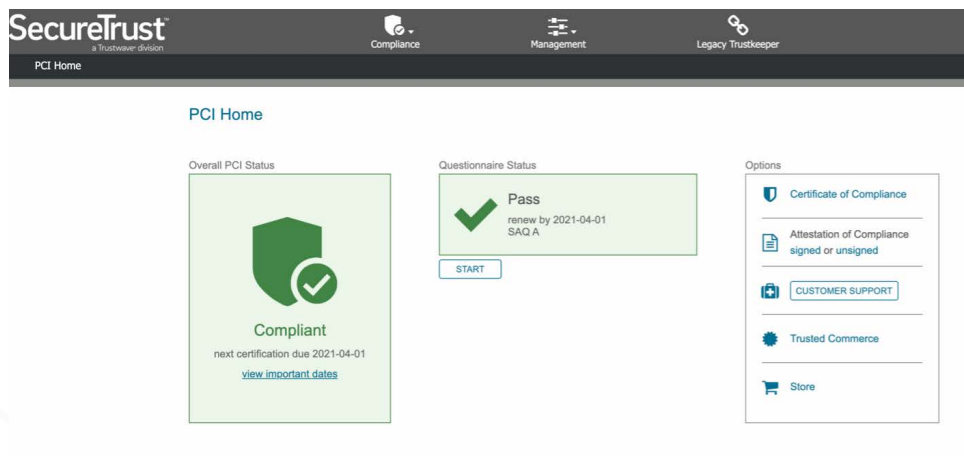
**Resources Available**

 1-877-257-0239

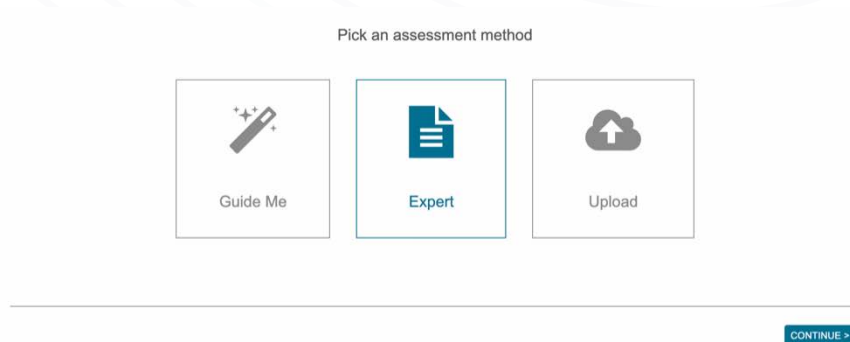
 ccsupport@securetrust.com

Page 2 of 12

Step 5: Now that you have registered and/or logged in, please select '**Start**' to begin. This will allow you to start your enrollment and/or renew it.



Step 6: Click '**Expert**' and hit continue to move on to the next page



PCI Profile

Step 7: Select the applicable way your organization accept credit cards.
For most ZoomGive users, please select the third checkbox as shown below:

The screenshot shows the 'PCI Questionnaire' progress bar at 15%. The left sidebar lists the steps: 1. PCI Profile (selected), 2. Company Profile, 3. Security Services, 4. Questionnaire, and 5. Confirmation. Under 'PCI Profile', the sub-steps are 'Acceptance Channels', 'Payment Products', and 'Form Selection'. The main content area is titled 'What Are The Ways You Accept Credit Card Payments' and includes the instruction 'Select all that apply'. There are three checkboxes: 'My business has a physical location where payments with a credit card are made in-person' (unchecked), 'My business allows payments with a credit card by mail or over the phone (MO/TO)' (unchecked), and 'My business has a website where payments with a credit card are made online' (checked).

Step 8: Select the checkbox "We do not use any devices..." and hit 'Next' to continue to the next page

The screenshot shows the 'PCI Questionnaire' progress bar at 22%. The left sidebar lists the steps: 1. PCI Profile (selected), 2. Company Profile, 3. Questionnaire, and 4. Confirmation. Under 'PCI Profile', the sub-steps are 'Acceptance Channels', 'Payment Products' (selected), and 'Form Selection'. The main content area is titled 'Payment Products' with a help icon. It includes the instruction 'Identify any devices (e.g. POS terminals, EFTPOS, payment software applications, services, etc.) you use to process credit card purchases from your customers in person, over the phone, or through mail order.' Below this is the 'Add payment product' section with radio buttons for 'Existing Device' (selected) and 'No match, add new payment product'. There is a 'Product Name' input field, a 'LOOKUP' button, and a 'P2PE Only' checkbox (unchecked). Below the input field is a 'Select version...' dropdown menu and an 'ADD' button. At the bottom, there is a checked checkbox for 'We do not use any devices to process card payments'. The footer contains 'SAVE & EXIT', 'BACK', 'NEXT', and a 'Help' icon.

Step 9: Select the form '**SAQ A**' and check off each eligible criteria while making sure they each apply to your merchant account with ZoomGive

PCI Questionnaire 28%

1 PCI Profile

Acceptance Channels
Payment Products
Form Selection

2 Company Profile

3 Questionnaire

4 Confirmation

Choose Your PCI Self-Assessment Questionnaire (SAQ)

Select the SAQ form most applicable to your business. Note that some forms have eligibility criteria that have to all be met. If you are unsure, click **Back** and select **Guide Me**, which will guide you through the process.

☒ PCI SAQ A 3.2.1 v1.0 ⓘ

☐ PCI SAQ A-EP 3.2.1 v1.0 ⓘ

☐ PCI SAQ B 3.2.1 v1.0 ⓘ

☐ PCI SAQ B-IP 3.2.1 v1.0 ⓘ

☐ PCI SAQ C 3.2.1 v1.0 ⓘ

☐ PCI SAQ C-VT 3.2.1 v1.0 ⓘ

☐ PCI SAQ D 3.2.1 v1.0 ⓘ

☐ PCI SAQ D-SP 3.2.1 v1.0 ⓘ

☐ PCI SAQ P2PE 3.2.1 v1.0 ⓘ

Confirm All Eligibility Criteria *

☒ Merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions;

☒ All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers;

☒ Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions;

☒ Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and

☒ Merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically.

☒ Additionally, for e-commerce channels:
The entirety of all payment pages delivered to the consumer's browser originates directly from a third-party PCI DSS validated service provider(s).

«

SAVE & EXIT

BACK

CONFIRM

Help

Company Profile

Step 10: Fill out the **Contact Details** if they are blank or have since changed

PCI Questionnaire 36%

1 PCI Profile

2 Company Profile

Contact Details
Account Details
Status Reporting
Qualified Integrator/Reseller
Websites
Service Providers

3 Questionnaire

4 Confirmation

Primary Contact Information

Let's confirm your best contact information so we can ensure you are kept up to date on any important data security and compliance issues like when the PCI certificate expires.

Name

Email

Phone

«

SAVE & EXIT

BACK

NEXT

Help

Step 11: Select 'Next' to advance to the next page. Confirm the **Account Details** are accurate and make changes if necessary

PCI Questionnaire 39%

1 PCI Profile

2 **Company Profile**

3 Questionnaire

4 Confirmation

Contact Details

Account Details

Status Reporting

Qualified Integrator/Reseller

Websites

Service Providers

General Info ⓘ

Company ZoomGive

Industry * Charitable Organization

Primary Contact * Scott Roseveare[sroseveare] ⓘ

Secondary Contact Please Select... ⓘ

Mailing Address * 3941 Park Dr. Ste 20545

City * El Dorado Hills

Country * United States of America

State/Province * California

ZIP/Postal Code * 95762

Additional Info

Service Providers *

Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?

☐ Yes ☒ No

Multiple Acquirer *

Does your company have a relationship with more than one acquirer (e.g. merchant services provider, bank, etc.)?

☐ Yes ☒ No

Payment Card Activity * ⓘ

Generally, how does your business store, process and/or transmit cardholder data (limit to 1000 characters)?

A third party processes payments from a 3rd-party link. We never see or store credit card numbers or sensitive client information.

Environment Under Assessment * ⓘ

Briefly describe the environment and/or systems covered by this assessment (limit to 1000 characters).

Organization consists of 10+ employees and has an e-commerce

SAVE & EXIT BACK NEXT Help

Step 12: Confirm the Merchant ID is accurate and select 'Next' to advance to the next page

PCI Questionnaire 43%

1 PCI Profile

2 **Company Profile**

3 Questionnaire

4 Confirmation

Contact Details

Account Details

Status Reporting

Qualified Integrator/Reseller

Websites

Service Providers

PCI Assessment and Status Reporting

Program Sponsor Marathon Solutions ⓘ

On File Merchant ID 496306423880 Primary ✓

Step 13: Select the check box "We do not use any third party companies for initiating or maintaining payment systems" and continue to the next page

PCI Questionnaire 46%

1 PCI Profile

2 **Company Profile**

3 Questionnaire

4 Confirmation

Contact Details

Account Details

Status Reporting

Qualified Integrator/Reseller

Websites

Service Providers

Qualified Integrator or Reseller (QIR)

Provide the name of the third-party company you use to install, configure, or support these products. These companies or individuals may be known as integrators and/or resellers or even IT consultants.

Company

☒ Add

Qualified Integrator/Reseller LOOKUP

ADD

☒ We do not use any third party companies for installing or maintaining our payment systems

SAVE & EXIT BACK NEXT Help

Step 14: Add your website URL and click "Add" if you are accepting payments on the website with your ZoomGive merchant account. Make sure to also check the box before advancing to the next page

PCI Questionnaire 50%

1 PCI Profile

2 Company Profile

- Contact Details
- Account Details
- Status Reporting
- Qualified Integrator/Reseller
- Websites**
- Service Providers

3 Questionnaire

4 Confirmation

«

E-Commerce Websites

Identify all websites where your customers can make online purchases.

Domain Name	Added By	Action
zoomgive.com	astonezg	

URL

☒ Add

ADD

☐ ZoomGive has full authority to allow Trustwave to monitor the above website.

SAVE & EXIT **BACK** **NEXT** Help

Step 15: To add CardConnect/Fiserv (the merchant account processor ZoomGive partners with), type "**Fiserv**" in the search box and then click '**Lookup**' - a list will populate

PCI Questionnaire 53%

1 PCI Profile

2 Company Profile

- Contact Details
- Account Details
- Status Reporting
- Qualified Integrator/Reseller
- Websites
- Service Providers**

3 Questionnaire

4 Confirmation

«

Service Providers

Identify any service providers you use either to host your website or to handle the credit card processing from website or mail/telephone orders, and specify the type of services provided.

Company

☒ Existing Provider ☐ No match, add new

LOOKUP

490 service providers found

FISERV, INC

FISERV - XP2

Fiserv - LOS

Fiserv - CUSA

Fiserv - OnCU

Fiserv - Accel

Fiserv - Acumen

Services

Select Provided Services...

ADD

SAVE & EXIT **BACK** **NEXT** Help

Step 16: Select 'FISERV INC' so that the line is highlighted and then click 'Add.' Then under the 'Services' drop down, select 'Payment Processing.' You can now move on to the next page

PCI Questionnaire 53%

1 PCI Profile

2 Company Profile

Contact Details

Account Details

Status Reporting

Qualified Integrator/Reseller

Websites

Service Providers

3 Questionnaire

4 Confirmation

Service Providers ⓘ

Identify any service providers you use either to host your website or to handle the credit card processing from website or mail/telephone orders, and specify the type of services provided.

Company

☒ Existing Provider ☐ No match, add new

Fiserv LOOKUP

490 service providers found

FISERV, INC

FISERV - XP2

Fiserv - LOS

Fiserv - CUSA

Fiserv - OnCU

Fiserv - Accel

Fiserv - Acumen

Services

Payment Processing

ADD

SAVE & EXIT BACK NEXT Help

Questionnaire

Step 17: For the following pages, please go through the questionnaire and select the answers as they apply to your business. Examples are below:

PCI Questionnaire 78%

1 PCI Profile

2 Company Profile

3 Questionnaire

System Settings ⚠

Application and Systems Security ⚠

Account Security ⚠

Physical Access Controls ⚠

Security Policies and Procedures ⚠

Acknowledge and Submit

4 Confirmation

Questionnaire PCI SAQ A 3.2.1 v1.0 ⓘ Remaining 22 of 24

Section System Settings All 2

2.1 (a) Are vendor-supplied defaults always changed before installing a system on the network? Yes No Not Applicable

This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc..

2.1 (b) Are unnecessary default accounts removed or disabled before installing a system on the network? Yes No Not Applicable

SAVE & EXIT BACK NEXT Help

PCI Questionnaire 78%

- 1 PCI Profile
- 2 Company Profile
- 3 Questionnaire

System Settings

Application and Systems Security
Account Security
Physical Access Controls
Security Policies and Procedures
Acknowledge and Submit



- 4 Confirmation

Questionnaire PCI SAQ A 3.2.1 v1.0 Remaining 22 of 24

Section System Settings All 2

2.1(a)

Are vendor-supplied defaults always changed before installing a system on the network?

Yes

No

Not Applicable

This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).

2.1(b)

Are unnecessary default accounts removed or disabled before installing a system on the network?

Yes

No

Not Applicable

SAVE & EXIT

BACK

NEXT

 HelpPCI Questionnaire 83%

- 1 PCI Profile
- 2 Company Profile
- 3 Questionnaire

System Settings

Application and Systems Security
Account Security
Physical Access Controls
Security Policies and Procedures
Acknowledge and Submit



- 4 Confirmation

Questionnaire PCI SAQ A 3.2.1 v1.0 Remaining 20 of 24

Section Application and Systems Security All 2

6.2(a)

Are all system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches?

Yes

No

Not Applicable

6.2(b)

Are critical security patches installed within one month of release?

Yes

No

Not Applicable

Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.

SAVE & EXIT

BACK

NEXT

 HelpPCI Questionnaire 87%

- 1 PCI Profile
- 2 Company Profile
- 3 Questionnaire

System Settings

Application and Systems Security
Account Security
Physical Access Controls
Security Policies and Procedures
Acknowledge and Submit



- 4 Confirmation



Are policies and procedures for user identification management controls defined and in place for non-consumer users and administrators on all system components, as follows:

8.1.1

Are all users assigned a unique ID before allowing them to access system components or cardholder data?

Yes

No

Not Applicable

8.1.3

Is access for any terminated users immediately deactivated or removed?

Yes

No

Not Applicable

8.2

In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users?

Yes

No

Not Applicable

- Something you know, such as a password or passphrase
- Something you have, such as a token device or smart card
- Something you are, such as a biometric

8.2.3(a)

Are user password parameters configured to require passwords/passphrases meet the following?

Yes

No

Not Applicable

- A minimum password length of at least seven characters
- Contain both numeric and alphabetic characters

Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.

8.5

Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows:

Yes

No

Not Applicable

- Generic user IDs and accounts are disabled or removed;
- Shared user IDs for system administration activities and other critical functions do not exist; and
- Shared and generic user IDs are not used to administer any system components?

SAVE & EXIT

BACK

NEXT

 Help

PCI Questionnaire 91%

1 PCI Profile

2 Company Profile

3 Questionnaire

- System Settings
- Application and Systems Security
- Account Security
- Physical Access Controls
- Security Policies and Procedures
- Acknowledge and Submit

4 Confirmation



Questionnaire PCI SAQ A 3.2.1 v1.0 Remaining 8 of 24

Section Physical Access Controls

All 9

- [9.5](#) Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? Yes No Not Applicable
- For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.*
- [9.5 \(a\)](#) Is strict control maintained over the internal or external distribution of any kind of media? Yes No Not Applicable
- Do controls include the following:
- [9.6.1](#) Is media classified so the sensitivity of the data can be determined? Yes No Not Applicable
- [9.6.2](#) Is media sent by secured courier or other delivery method that can be accurately tracked? Yes No Not Applicable
- [9.6.3](#) Is management approval obtained prior to moving the media (especially when media is distributed to individuals)? Yes No Not Applicable
- [9.7](#) Is strict control maintained over the storage and accessibility of media? Yes No Not Applicable
- [9.8 \(a\)](#) Is all media destroyed when it is no longer needed for business or legal reasons? Yes No Not Applicable

SAVE & EXIT

BACK

NEXT

Help

PCI Questionnaire 91%

1 PCI Profile

2 Company Profile

3 Questionnaire

- System Settings
- Application and Systems Security
- Account Security
- Physical Access Controls
- Security Policies and Procedures
- Acknowledge and Submit

4 Confirmation



Questionnaire PCI SAQ A 3.2.1 v1.0 Remaining 8 of 24

Section Physical Access Controls

All 9

- [9.5](#) Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? Yes No Not Applicable
- For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.*
- [9.5 \(a\)](#) Is strict control maintained over the internal or external distribution of any kind of media? Yes No Not Applicable
- Do controls include the following:
- [9.6.1](#) Is media classified so the sensitivity of the data can be determined? Yes No Not Applicable
- [9.6.2](#) Is media sent by secured courier or other delivery method that can be accurately tracked? Yes No Not Applicable
- [9.6.3](#) Is management approval obtained prior to moving the media (especially when media is distributed to individuals)? Yes No Not Applicable
- [9.7](#) Is strict control maintained over the storage and accessibility of media? Yes No Not Applicable
- [9.8 \(a\)](#) Is all media destroyed when it is no longer needed for business or legal reasons? Yes No Not Applicable

Is media destruction performed as follows:

- [9.8.1 \(a\)](#) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed? Yes No Not Applicable
- [9.8.1 \(b\)](#) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents? Yes No Not Applicable

SAVE & EXIT

BACK

NEXT

Help

PCI Questionnaire 95%

1 PCI Profile

2 Company Profile

3 Questionnaire

- System Settings
- Application and Systems Security
- Account Security
- Physical Access Controls
- Security Policies and Procedures
- Acknowledge and Submit

4 Confirmation



Questionnaire PCI SAQ A 3.2.1 v1.0 Remaining 3 of 24

Section Security Policies and Procedures

All 6

Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:

- [12.8.1](#) Is a list of service providers maintained, including a description of the services(s) provided? Yes No Not Applicable
- [12.8.2](#) Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment?
- Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*
- [12.8.3](#) Is there an established process for engaging service providers, including proper due diligence prior to engagement? Yes No Not Applicable
- [12.8.4](#) Is a program maintained to monitor service providers' PCI DSS compliance status at least annually? Yes No Not Applicable
- [12.8.5](#) Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity? Yes No Not Applicable

Has an incident response plan been implemented in preparation to respond immediately to a system breach, as follows:

SAVE & EXIT

BACK

NEXT

Help

Confirmation

Congratulations!

You have completed the renewal process.

Make sure to '**Acknowledge & Submit**' to move onto the '**Confirmation**' page before exiting.

PCI Questionnaire

100%

1 PCI Profile

2 Company Profile

3 Questionnaire

4 Confirmation

System Settings

Application and Systems Security

Account Security

Physical Access Controls

Security Policies and Procedures

Acknowledge and Submit

✓

✓

✓

✓

✓

✓

PCI SAQ A 3.2.1 v1.0

✓ Thank you for completing and reviewing your PCI Self-Assessment Questionnaire (SAQ).

➔ Click **Acknowledge & Submit** below to confirm your attestation and electronically sign the document.

Tip

🔍 If you would like to review any part of the form, click on the **section name** in the left sidebar to jump to that step.

SAVE & EXIT

BACK

ACKNOWLEDGE & SUBMIT

Help

Express Renewal

If there has been no significant changes (see below) to your processing, you may be eligible for [Express Renewal](#).

PCI Questionnaire

30%

1 PCI Profile

2 Company Profile

3 Security Services

4 Wizard

5 Questionnaire

6 Confirmation

PCI Profile Summary

Express Renewal

Fast Track Compliance enabled by PCI Express Renewal

➔ Congratulations. It appears that you are eligible for PCI Express Renewal.

Express Renew Recommended

✎ Choose this option if your credit card payments business environment did not have an [significant changes](#) since last time. We will automatically reload your completed Self-Assessment Questionnaire and you will have the option to review the form before re-submitting.

Start new Assessment

📄 Choose this option to start a fresh, new guided assessment. The PCI Wizard will still be available to help complete the questionnaire quicker.

🔍 Be sure to review and update this year's form to ensure they are inline with any other changes in your cardholder data environment.

SAVE & EXIT

BACK

NEXT

Help

Generally, a change would be deemed significant if it would impact the security of cardholder data. This change may include storing, transmitting or processing credit card data. For example, if you start accepting credit card payments on a new e-commerce website in addition to your store front OR changed your POS equipment to a different system or configuration.

Page 11 of 12

If you select **Express Renewal**, you will be taken to a completed questionnaire based on your previous year's questionnaire.

PCI Questionnaire 80%

Questionnaire **5** Questionnaire

- Eligibility ☒
- Firewall Configuration ☒
- System Settings ☒
- Stored Data Protection ☒
- Transmitted Data Protection ☒
- Application and Systems Security ☒
- Access Restrictions ☒
- Account Security ☒
- Physical Access Controls ☒
- Monitoring and Testing ☒
- Security Policies and Procedures ☒
- Hosting Providers ☒
- Acknowledge and Submit ☐

Questionnaire PCI SAQ B-IP 3.2.1 v1.0 Remaining 0 of 95

Section Firewall Configuration All 12

Are firewall and router configuration standards established and implemented to include the following:

1.1.2 (a)	Is there a current network diagram that documents all connections between the cardholder data environment and other networks, including any wireless networks?	Yes	No	Not Applicable
1.1.2 (b)	Is there a process to ensure the diagram is kept current?	Yes	No	Not Applicable
1.1.4 (a)	Is a firewall required and implemented at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone?	Yes	No	Not Applicable
1.1.4 (b)	Is the current network diagram consistent with the firewall configuration standards?	Yes	No	Not Applicable
1.1.6 (a)	Do firewall and router configuration standards include a documented list of services, protocols, and ports, including business justification and approval for each?	Yes	No	Not Applicable

SAVE & EXIT BACK NEXT Help

After reviewing the completed questionnaire, you may verify the statements below, sign and submit the questionnaire to complete your SAQ for the year.

cardpointe PCI Questionnaire

PCI Questionnaire 100%

Security Services **3** Wizard **4** Questionnaire **5** Confirmation **6**

- Eligibility ☒
- Firewall Configuration ☒
- System Settings ☒
- Stored Data Protection ☒
- Transmitted Data Protection ☒
- Anti-Virus Protection ☒
- Application and Systems Security ☒
- Access Restrictions ☒
- Account Security ☒
- Physical Access Controls ☒
- Access Tracking ☒
- Monitoring and Testing ☒
- Security Policies and Procedures ☒
- Hosting Providers ☒
- Acknowledge and Submit ☒

Confirmation of Compliant Status

Verify ☐ PCI DSS Self-Assessment Questionnaire C, Version 3.2.1 rev 1.0, was completed according to the instructions therein.

☐ All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.

☐ I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.

☐ 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.

☐ No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.

1. Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

2. The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

3. Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

If you need to submit the Attestation of Compliance (AOC) to your processor or bank, please review the entire AOC to ensure all applicable fields are completed prior to submission. There are certain fields in the AOC that are not systematically pre-filled and will require your attention. For example, Parts 2B & 2E are fields that require your input. Additionally, there may be other input fields that need to be completed.

Merchant Acknowledgement

Company Test Account_RM_2

Sign ☐ I am hereby signing and intend to authenticate this document

Title

Executive Officer

Today's Date 2020-08-07

SAVE & EXIT BACK SUBMIT Help

PCI Profile Summary