

PCI is important and designed to keep your customer safe when processing credit cards.

Your Processor Clearent, keeps your account safe with Data Guardian. As Part of the data guardian program you need to complete a PCI questionnaire

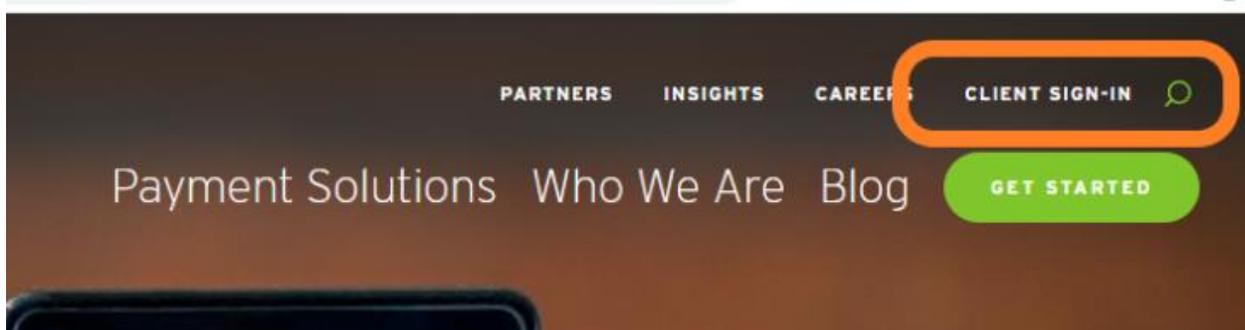
With this in mind here is a step by step set of instructions on how to complete your PCI survey for your card processing bank.

You can learn more about PCI and its importance here <https://www.pcisecuritystandards.org/>

Please Contact Clearent Support at 866 435 0666 or customersupport@clearent.com if you need help accessing Compass

If you need additional help completing your PCI you can contact PCI help desk at 855 864 1732

From a computer at your place of work access an internet browser and go to [Clearent.com](https://www.clearent.com) and sign in.



If you know your log in and password, you can skip the password reset and go forward to your home screen.

If you don't know your password

Choose the reset your password link

COMPASS SIGN IN

USERNAME

My user Id from the email instructions |

[Forgot your Username?](#)

PASSWORD

[Forgot your Password?](#)

Sign In To Compass

Copyright © 2020, Clearent, LLC. All Rights Reserved.

Your username came in an email to you, If you don't know your user name, you can call Clearent support at 866 435 0666. You may want to have a recent statement available to get your companies MID

RESET YOUR COMPASS PASSWORD

Enter your Username below to proceed. We'll email you a one-time passcode that will allow you to reset your password.

Username

Continue



RESET YOUR COMPASS PASSWORD



A one-time passcode has been emailed to:
THE EMAIL ON FILE FOR YOU

Please enter your one-time passcode below. If you haven't received your one-time passcode yet, please wait 20-30 seconds and check again.

Username

THE USER NAME YOU WERE PROVIDED

One-Time Passcode

LOOK FOR YOUR ONE TIME CODE AT THE ABOVE
EMAIL. IF YOU DONT RECOGNIZE THIS EMAIL CALL
SUPPORT AT 866 435 0666

Continue

This pass code will arrive from NoReply@clearent.com

Clearent

New One-Time Passcode - For security reasons, we are sending a one-time passcode to the email address listed for your account.

Make sure you Carefully read the password requirements. An Example of a good password is Myxbr412

Don't add special characters . / (



You have successfully unlocked your password and may reset it.

RESET YOUR COMPASS PASSWORD

Please enter your new password below.

- Must be at least 7 characters long.
- Must have at least 1 uppercase letter.
- Must have at least 1 lowercase letter.
- Must have at least 1 numeric character.

Username

Your User Id Appears Here

Your New Password

Verify Your New Password

Continue



You have successfully reset your password! Please close this window and sign in.

RESET YOUR COMPASS PASSWORD

Go back to Clearent.com and click sign in again.

From your home page chose Data Guardian

MERCHANT HOME

Welcome [Logout](#)
[Sergio](#)
Viewing Business

January 2020
Navigate to a monthly time period
January 2020 | < > [Take me to the current month](#)

Refer a friend and get a \$25 bonus - call 314-732-0515 for details.

Viewing your transaction data **Monthly** Daily Deposits Fee Detail

Deposit Summary

Net Sales (All Card Types) MTD	\$2,802.80
Settled Volume MTD	\$2,802.80
Chargebacks	\$0.00
Adjustments	\$0.00
Withholding	\$0.00
Discount and Fees Collected Daily	\$0.00
Month-End Balance	N/A
Total Discount and Fees	\$0.00
NET DEPOSIT	\$2,802.80

Volume History by Month (All Card Types)

Industry: Restaurant
DataGuardian? [Yes](#)
556 N Guadalupe St
Santa Fe, NM, 87501
505-690-8511

[Statements & Tax Forms](#)

Merchant Controls

- Change Merchant
- Transaction Search
- View Equipment
- DataGuardian**

Settings / Help

- Account Settings
- Change Password
- User Guide

Clearent, LLC
222 South Central, Suite 700
Clayton, MO 63105
E-mail us at customersupport@clearent.com
or call 866.435.9666.

Select Data Guardian

Select the first tab Merchant Information and confirm that your Merchant information is correct in part one.

Home Contact Us [CHAT](#)

CLEARENT™
INTELLIGENT PROCESSING

Merchant Information Questionnaire Selection

Merchant Information

Part 1 Merchant Information

Please confirm that the information below is correct:

Scroll down to Part 2. You are a Retailer

Part 2 Type Of Merchant Business

Check all that apply:

Retailer ⓘ

Part 3. Answer No to all questions

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.)?

Part 4, section 1, Choose Terminal

Part 4 Processing Solution

What solution do you use to process credit cards? [Learn More](#)



Moto/E-commerce



Terminal



Part 4, section 2, Answer NO

Do you store any sensitive cardholder data electronically?

Part 4, Section 3, Choose IP, Then select Add Solutions

Terminal

Do you connect this solution through a Cellular or a Dial-up or an IP Connection?

Dial-up IP Dial-Up and IP Cellular

Please add your Terminal solution information.

Add Solutions

You have a Vendor (Pax Computer Technology)

Model ----- if you have a BrewPOS system your model is A35 or s300

Add Terminal Solution ×

Please enter your Terminal solution information.

VENDOR *
PAX Computer Technology (Shenzhen) Co Ltd

Model/Application *

[Add additional](#) [If you don't see your solution, click here to type it in manually.](#)

Cancel **Save**

Terms and conditions. Check the box and choose Save and continue

I have read and agreed to [the terms & conditions](#)

Select Questionnaire Manually **Save & Continue**

Agree and Continue

Confirm your eligibility to take questionnaire B-IP



1. You certify that you use a standalone terminal that is connected to the Internet.
2. You certify that your standalone terminal is not connected to any other systems within your network.
3. Your device does not rely on any other device (e.g., computer, mobile phone, tablet, etc.) to connect to the payment processor.
4. You retain only paper reports or receipts with cardholder data, and these documents are not received electronically.



agree that the statements above are true.

Continue

The next section is the Questionnaire B-IP. Start this section by choosing the Start Questionnaire button at the lower right of the screen, you may need to scroll down.

SECTION 1 - REQUIREMENT 1 Install and maintain a firewall configuration to protect data 9 Questions	SECTION 2 - REQUIREMENT 2 Do not use vendor-supplied defaults for system passwords and other security parameters 7 Questions	SECTION 3 - REQUIREMENT 3 Protect stored cardholder data 5 Questions
SECTION 4 - REQUIREMENT 4 Encrypt transmission of cardholder data across open, public networks 7 Questions	SECTION 5 - REQUIREMENT 6 Develop and maintain secure systems and applications 3 Questions	SECTION 6 - REQUIREMENT 7 Restrict access to cardholder data by business need to know 3 Questions
SECTION 7 - REQUIREMENT 8 Identify and authenticate access to system components 5 Questions	SECTION 8 - REQUIREMENT 9 Restrict physical access to cardholder data 16 Questions	SECTION 9 - REQUIREMENT 11 Regularly test security systems and processes 4 Questions
SECTION 10 - REQUIREMENT 12 Maintain a policy that addresses information security for all personnel 8 Questions	SECTION 11 Network Scan	 Start Questionnaire

Section 1 Install and maintain a firewall configuration to protect data

Start Section

Select Start Section

Answer Yes to all questions in this section.

There are information boxes next to each question to explain them. You will in the end have to answer yes to all questions to pass PCI. These are not only best policy practices, they are expected by the payment industry to keep your customer's card data safe.

Sections 2-10

Repeat this process for sections 2 until the end of the survey.

We encourage you to read and learn about PCI and its importance to your company and the protection of card holder data.

Once you have completed the steps you choose continue to scan

Questionnaire B-IP In Progress

Your Network Scan status is still "In Progress". Please check back within 24-48 hours to see your scan results.

SECTION 1 Install and maintain a firewall configuration to protect data 9 Questions Pass	SECTION 2 Do not use vendor-supplied defaults for system passwords and other security parameters 7 Questions Pass	SECTION 3 Protect stored cardholder data 5 Questions Pass
SECTION 4 Encrypt transmission of cardholder data across open, public networks 7 Questions Pass	SECTION 5 Develop and maintain secure systems and applications 3 Questions Pass	SECTION 6 Restrict access to cardholder data by business need to know 3 Questions Pass
SECTION 7 Identify and authenticate access to system components 5 Questions Pass	SECTION 8 Restrict physical access to cardholder data 16 Questions Pass	SECTION 9 Regularly test security systems and processes 4 Questions Pass
SECTION 10 Maintain a policy that addresses information security for all personnel 8 Questions Pass	SECTION 11 Network Scan Non-Compliant	

Continue To Scan

Choose launch scan on the next screen

The screenshot displays the 'Network Scan Summary' interface. At the top, a progress bar shows five steps: Merchant Information, Questionnaire Selection, Questionnaire, Network Scan (highlighted in red), and Review and Sign. Below the progress bar, the 'ASV Compliance Status' is shown as 'Non-Compliant' in a red box. A note states: 'According to PCI DSS requirement 11.2, your scan target must have a passing scan every 90 days.' A 'SCAN TIMING' dropdown menu is set to 'Normal'. The 'Scan Targets' section shows a donut chart with '1 Total' and a legend for '1 IPv4' and '0 IPv6'. The 'Scan Target Status Summary' section includes a 'Schedule Scan' link and a table of status counts: 0 Not Started, 0 Queued, 0 Actively Scanning, 0 Compiling Scan Results, 0 Fail - Action Needed, 0 Action Required, 0 Pass, and 1 Expired. A 'Launch Scan' button is highlighted with an orange circle, and a 'Submit ASV Compliance' button is also visible.

Merchant Information > Questionnaire Selection > Questionnaire > **Network Scan** > Review and Sign

Network Scan Summary

ASV Compliance Status **Non-Compliant**

According to PCI DSS requirement 11.2, your scan target must have a passing scan every 90 days.

SCAN TIMING: Normal

Scan Targets

1 Total

1 IPv4, 0 IPv6

Scan Target Status Summary

Schedule Scan: [Create Schedule](#)

0 Not Started	0 Queued	0 Actively Scanning	0 Compiling Scan Results
0 Fail - Action Needed	0 Action Required	0 Pass	1 Expired

Last updated November 10, 2016 at 03:26 PM

Launch Scan | Submit ASV Compliance

Your done, no matter if you pass the scan or not, you have completed your survey.