

# PCI Questionnaire Step-by-Step Guide

POS Device Users

## What is PCI Compliance?

The Payment Card Industry Data Security Standard (PCI Standard) is an information security standard for any organization that processes, stores, or transmits cardholder data. TapGoods partners with our merchant processor, Launchpay, and our PCI partner, MAXpci to provide you with a seamless PCI compliance program.

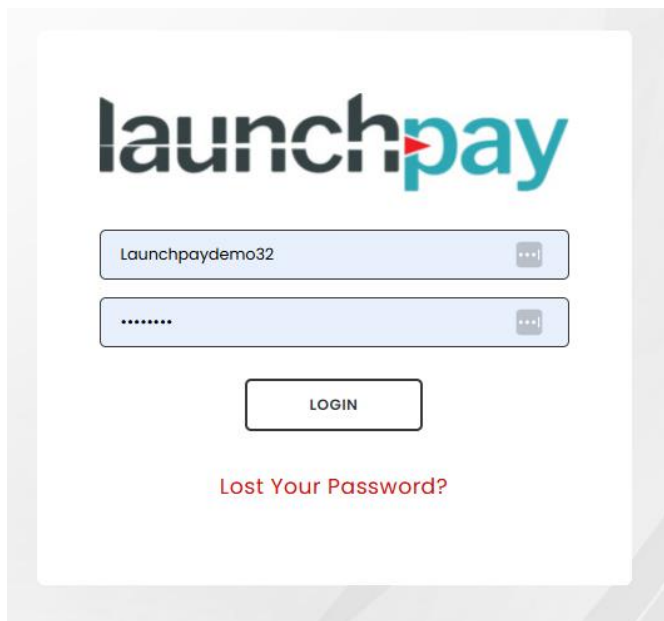
## How to Become PCI Compliant

You will complete an annual questionnaire to become PCI compliant. You will receive emails directly from MAXpci with information, instructions, and resources to complete the questionnaire. Follow the step-by-step guide below to complete your questionnaire.

### Step 1: Log In


Go to [PCI Compliance Portal](#) and enter:

- **Username:** Your Merchant ID Number (located in your Launchpay BackOffice portal)
- **Initial Password:** Comply1!

A screenshot of the Launchpay login interface. At the top is the 'launchpay' logo in black and teal. Below it are two input fields: the first contains the text 'Launchpaydemo32' and the second contains a series of dots for a password. Each field has a small icon on the right. Below the fields is a 'LOGIN' button. At the bottom, there is a link that says 'Lost Your Password?' in red text.

## Step 2: Begin the Questionnaire

On the Dashboard, you can view your current questionnaire status if you previously started it, or click **Click Here to Select a New Questionnaire** to begin.



[Dashboard](#) [Questionnaire](#) [Policies](#) [Contact](#) [My Account](#)

Welcome, Launchpay Demo

Ready to get started?


CLICK HERE TO SELECT A NEW QUESTIONNAIRE

**Current Questionnaire Status**

Questionnaire
Not Started
STATUS
Not Started
APPROVAL DATE
Not Started

## Step 3: Complete the Questionnaire

Do you store cardholder data electronically? Select **No**. The full cardholder data is stored at the processor level.



[Dashboard](#) [Questionnaire](#) [Policies](#) [Contact](#) [My Account](#)

Process

CARD HOLDER TYPE

+

QUESTIONNAIRE TYPE

+

QIR VERIFICATION

+

ELIGIBILITY

+

PRE-QUESTION

+

QUESTIONS

+

ATTESTATION

+

DOWNLOAD CERTIFICATE


### Let's Get Started

In order to demonstrate your PCI compliance, a questionnaire must be completed each year. The first step in selecting the correct questionnaire is understanding how your company handles cardholder data.

#### Do You Store Cardholder Data Electronically ?

YES

NO



Cardholder data means the full card number. If you are storing this electronically, then you should select **Yes**.

Storing the first 6 digits, or last 4 digits, of a card number does not mean that you are storing cardholder data electronically, and you should select **No**.

Select either **Yes** or **No** on this screen. Viewing the video is not required and does not impact your questionnaire or compliance.

CARD HOLDER TYPE

QUESTIONNAIRE TYPE

QIR VERIFICATION

ELIGIBILITY

PRE-QUESTION

QUESTIONS

ATTESTATION

DOWNLOAD CERTIFICATE

launchpay

Dashboard **Questionnaire** Policies Contact My Account

launchpay

Welcome to Launchpay's Streamlined PCI Solution

To assist you with keeping cardholder data secure, we have created a Security Awareness video. The link to the video was sent to you via email. Have you watched it?

**NOTE:** Watching the video is not required in order to complete the compliance process.

YESNO

Copyrights © All Rights ReservedTerms of Use | Privacy Policy

Select the option for **Face to Face**.

CARD HOLDER TYPE

QUESTIONNAIRE TYPE

QIR VERIFICATION

ELIGIBILITY

PRE-QUESTION

QUESTIONS

ATTESTATION

DOWNLOAD CERTIFICATE


launchpay

Dashboard **Questionnaire** Policies Contact My Account

Questionnaire Select Type


How Do Your Customers Pay You?

[Click one of the boxes below]




Face to Face

Customers present their credit cards in person.




eCommerce Only

Customers visit our website and enter their credit card information.



Mail / Phone

Customers send us their credit card information by mail or they call us.



Other Ways

I process transactions in more than one way.

Select the **B-IP** next to **I use a terminal that uses an IP-based connection**.

Face to Face

I call a toll free number and enter credit card information

B

I use a terminal that uses an IP-based connection

B-IP

I process transactions on a POS system, OR by logging into software installed on my computer, OR by logging into a secure Virtual Terminal and swiping credit cards through a card reader

C

Click **Confirm** at the bottom of the page.

## Eligibility

You Have Chosen > I use a terminal that uses an IP-based connection

Merchant certifies eligibility to complete this shortened version of the Self Assessment Questionnaire because:

- The merchant uses only standalone, PCI-listed approved PTS POI devices (excludes SCRs and SCRPs) connected via IP to merchant's payment processor to take customers' payment card information;
- The standalone, IP-connected POI devices are validated to the PTS POI program as listed on the PCI SSC website (excludes SCRs and SCRPs);
- The standalone, IP-connected PTS POI devices are not connected to any other systems within the merchant environment (this can be achieved via network segmentation to isolate PTS POI devices from other systems);
- The only transmission of account data is from the approved PTS POI devices to the payment processor;
- The PTS POI device does not rely on any other device (e.g., computer, mobile phone, tablet, etc.) to connect to the payment processor;
- The merchant does not store account data in electronic format; and
- Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

If you are an eCommerce merchant, you have selected the wrong SAQ. You must select SAQ A or SAQ A-EP.

CONFIRM

## Use the following answers to the questions:

Do you use only an IP-terminal that is not connected to your network?

- YES

Do you have a Security Policy that addresses policies for keeping cardholder secure by assigning roles and responsibilities for personnel, and restricting access to it to only individuals with a need for access? [For help with your Security Policy, click here](#)

- YES

Do you discuss and review the security policy with all personnel at least once a year, including ensuring that personnel is aware of their responsibilities?

- YES

Do you restrict physical access to wall jacks or routers used by the device you use to process transactions? Examples of this would be a jack located in a public lobby that accesses the same connection used by your device to process transactions.

- YES

Do only the last four, or the first six, numbers of a card appear on printed receipts?

- YES

Do your customers send full credit or debit card information to you over the internet? Examples of this would be in an email, or by typing it into a chat box.

- NO

Are external vulnerability scans performed quarterly, after any changes to your network, and until all vulnerabilities are resolved? MaxPCI will perform these for you once the SAQ is completed.

- YES

Do you have an Incident Response Plan in place? If not, [click here](#) to download a template.

- YES

Are all employees trained to maintain an inventory of all devices, visually inspect all devices periodically, to be aware of suspicious behavior and to report any suspected tampering or replacement of devices?

- YES

Do you maintain a list of all devices, including the make, model, location, and identifying number for each, that process transactions?

- YES

Is the list of devices updated as new equipment is added, or equipment is replaced, so that the list is current at all times?

- YES

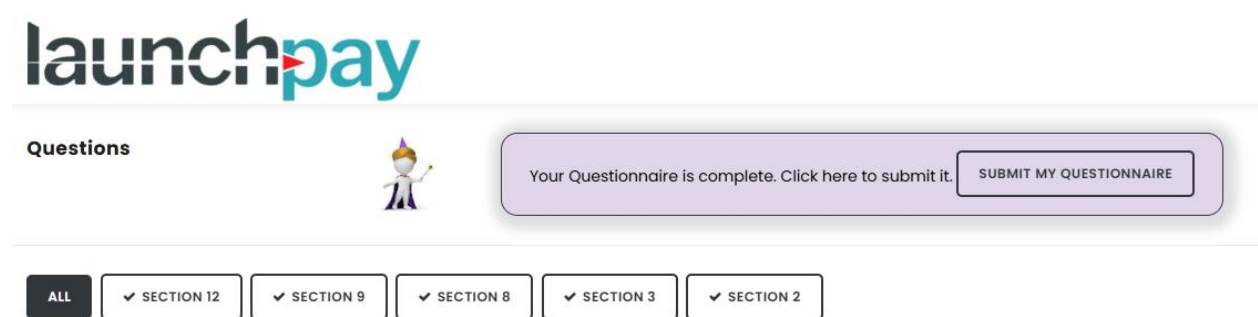
Do you have a formal security awareness program that is reviewed with all personnel?

- YES

Question	Yes	No
Do you use only an IP-terminal that is not connected to your network?	✓	<input type="radio"/>
Do you have a Security Policy that addresses policies for keeping cardholder secure by assigning roles and responsibilities for personnel, and restricting access to it to only individuals with a need for access? <a href="#">For help with your Security Policy, click here</a>	✓	<input type="radio"/>
Do you discuss and review the security policy with all personnel at least once a year, including ensuring that personnel is aware of their responsibilities?	✓	<input type="radio"/>
Do you restrict physical access to wall jacks or routers used by the device you use to process transactions? Examples of this would be a jack located in a public lobby that accesses the same connection used by your device to process transactions.	✓	<input type="radio"/>
Do only the last four, or the first six, numbers of a card appear on printed receipts?	✓	<input type="radio"/>
Do your customers send full credit or debit card information to you over the internet? Examples of this would be in an email, or by typing it into a chat box.	<input type="radio"/>	✓
Are external vulnerability scans performed quarterly, after any changes to your network, and until all vulnerabilities are resolved? MaxPCI will perform these for you once the SAQ is completed.	✓	<input type="radio"/>
Do you have an Incident Response Plan in place? If not, <a href="#">click here</a> to download a template.	✓	<input type="radio"/>
Are all employees trained to maintain an inventory of all devices, visually inspect all devices periodically, to be aware of suspicious behavior and to report any suspected tampering or replacement of devices?	✓	<input type="radio"/>
Do you maintain a list of all devices, including the make, model, location, and identifying number for each, that process transactions?	✓	<input type="radio"/>
Is the list of devices updated as new equipment is added, or equipment is replaced, so that the list is current at all times?	✓	<input type="radio"/>
Do you have a formal security awareness program that is reviewed with all personnel?	✓	<input type="radio"/>

Click **Submit** at the bottom of the page.

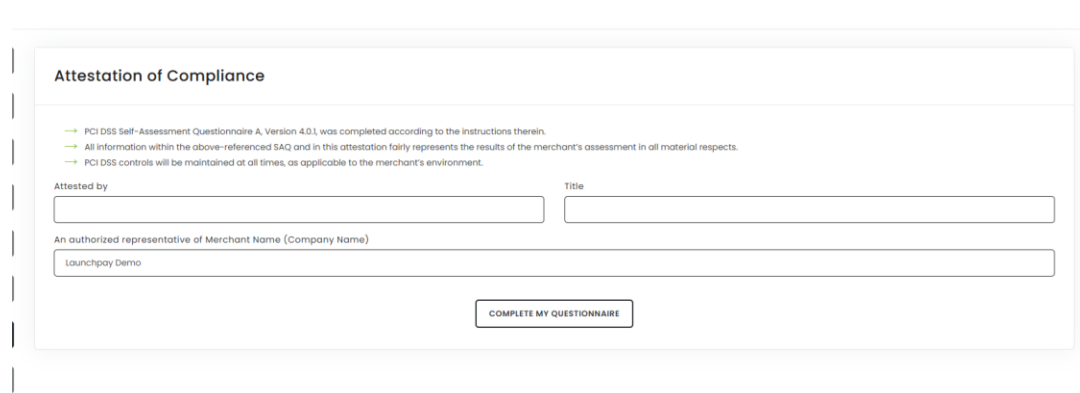
Click **Submit My Questionnaire** at the top of the page.



The screenshot shows the top section of the Launchpay interface. On the left is the 'launchpay' logo. Below it, the word 'Questions' is displayed next to a small cartoon character of a person with a party hat. To the right, a purple banner contains the text 'Your Questionnaire is complete. Click here to submit it.' and a button labeled 'SUBMIT MY QUESTIONNAIRE'. Below the banner, a row of buttons allows navigation between sections: 'ALL', 'SECTION 12', 'SECTION 9', 'SECTION 8', 'SECTION 3', and 'SECTION 2'. Each section button has a checkmark icon.

#### Step 4: Attest & Obtain Your Certificate

Fill in company information and select **Complete My Questionnaire**.




The screenshot shows the 'Attestation of Compliance' form. It includes three green checkmarks with accompanying text: 'PCI DSS Self-Assessment Questionnaire A, Version 4.0.1, was completed according to the instructions therein.', 'All information within the above-referenced SAQ and in this attestation fairly represents the results of the merchant's assessment in all material respects.', and 'PCI DSS controls will be maintained at all times, as applicable to the merchant's environment.' Below this, there are input fields for 'Attested by' and 'Title'. A larger field for 'An authorized representative of Merchant Name (Company Name)' contains the text 'Launchpay Demo'. At the bottom right of the form is a button labeled 'COMPLETE MY QUESTIONNAIRE'.

#### Step 5: Meet the Deadline to Avoid Fees

**Complete this process within 60 days** to avoid a **\$25.00 monthly PCI non-compliance fee**.

Anytime throughout the process, reach out directly to MAXpci by clicking the **purple chat button** in the bottom right corner:



[Dashboard](#)[Questionnaire](#)[Policies](#)[Contact](#)[My Account](#)

Welcome, Launchpay Demo

RESUME YOUR QUESTIONNAIRE

If you have changed the way you process transactions, you can

CLICK HERE TO SELECT A NEW QUESTIONNAIRE


Current Questionnaire Status

Questionnaire
A
STATUS
SAQ Incomplete
APPROVAL DATE

Copyrights © 2020 maxpci.com | All Rights Reserved

Terms of Use | Privacy Policy

985

[How Can We Help?](#)

They are also available by phone or email at:

- Phone: 800-803-8515
- Email: [support@maxpcicomply.com](mailto:support@maxpcicomply.com)