

PCI Questionnaire Step-by-Step Guide

Non 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.

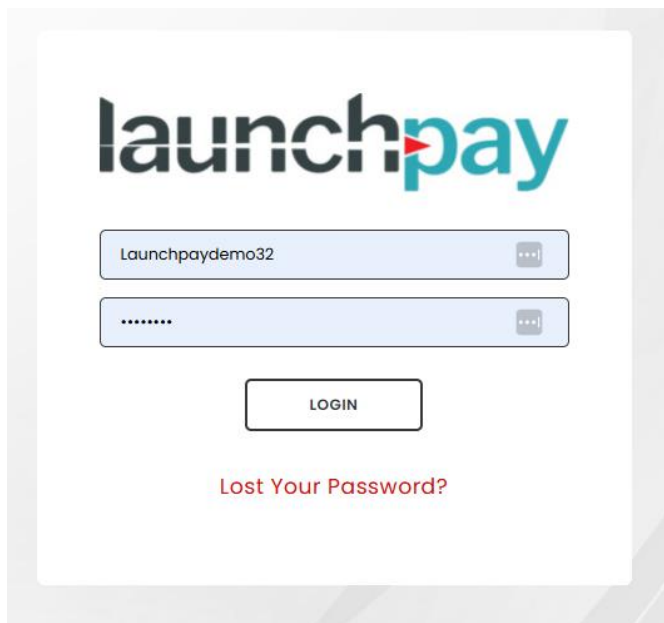
How to Become PCI Compliant

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 masked password '.....'. Each field has a small 'x' icon to its right. Below the input fields is a rectangular 'LOGIN' button. At the bottom of the login area is a red link that says 'Lost Your Password?'. The entire login form is set against a light gray background with a subtle gradient.

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

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 **eCommerce Only**.

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 A next to **My customers either click on a link to make a payment, or are taken to a third party's site to pay.**

eCommerce Only	
My customers either click on a link to make a payment, or are taken to a third party's site to pay	A
My customers pay directly on my website	A-EP
I use a webserver that redirects customers to my service provider's URL, or has an embedded payment page	A

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

Eligibility

You Have Chosen > My customers either click on a link to make a payment, or are taken to a third party's site to pay

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

- The merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
- All processing of account data is entirely outsourced to PCI DSS compliant third-party service provider (TPSP)/payment processor;
- The merchant does not electronically store, process, or transmit any account data on merchant systems or premises, but relies entirely on a TPSP(s) to handle all these functions;
- The merchant has confirmed that TPSP(s) are PCI DSS compliant for the services being used by the merchant; and
- Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Additionally, for e-commerce channels:

- All elements of the payment page(s)/form(s) delivered to the customer's browser originate only and directly from a PCI DSS compliant TPSP/payment processor.

CONFIRM

Use the following answers to the questions:

Do you store full payment card information in paper format or on removable electronic media? Full payment data includes the full card number, expiration date, and CVV number.

- NO

If cardholder data is shared with service providers, is there a list of service providers maintained, with responsibilities for cardholder security clearly defined in writing, and proof of their PCI DSS status required?

- YES

Do your agreements with all Service Providers clearly state who is responsible for the security of cardholder data?

- YES

Are passwords always changed before installing a system on the network? (For example, if your cable provider sends you a new router, they assign a password to it so that you can log in the first time. Do you change the password once you log in?)

- YES

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

- YES

Are unnecessary default accounts removed or disabled before installing a system on the network? (For example, if your cable provider sends you a new router, with a demo account set up, is the demo account deleted before you install the router?)

- YES


Do you create or manage user accounts that are used to access cardholder data?

- NO


Question	Yes	No
Do you store full payment card information in paper format or on removable electronic media? Full payment data includes the full card number, expiration date, and CVV number.	<input type="radio"/>	<input checked="" type="radio"/>
If cardholder data is shared with service providers, is there a list of service providers maintained, with responsibilities for cardholder security clearly defined in writing, and proof of their PCI DSS status required?	<input checked="" type="radio"/>	<input type="radio"/>
Do your agreements with all Service Providers clearly state who is responsible for the security of cardholder data?	<input checked="" type="radio"/>	<input type="radio"/>
Are passwords always changed before installing a system on the network? (For example, if your cable provider sends you a new router, they assign a password to it so that you can log in the first time. Do you change the password once you log in?)	<input checked="" type="radio"/>	<input type="radio"/>
Do you have an Incident Response Plan in place? If not, click here to download a template.	<input checked="" type="radio"/>	<input type="radio"/>
Are unnecessary default accounts removed or disabled before installing a system on the network? (For example, if your cable provider sends you a new router, with a demo account set up, is the demo account deleted before you install the router?)	<input checked="" type="radio"/>	<input type="radio"/>
Do you create or manage user accounts that are used to access cardholder data?	<input type="radio"/>	<input checked="" type="radio"/>

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

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



Questions



Your Questionnaire is complete. Click here to submit it.

SUBMIT MY QUESTIONNAIRE

ALL

✓ SECTION 12

✓ SECTION 9

✓ SECTION 8

✓ SECTION 3

✓ SECTION 2

Step 4: Attest & Obtain Your Certificate

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

Attestation of Compliance

→ 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.
→ PCI DSS controls will be maintained at all times, as applicable to the merchant's environment.

Attested by

Title

An authorized representative of Merchant Name (Company Name)

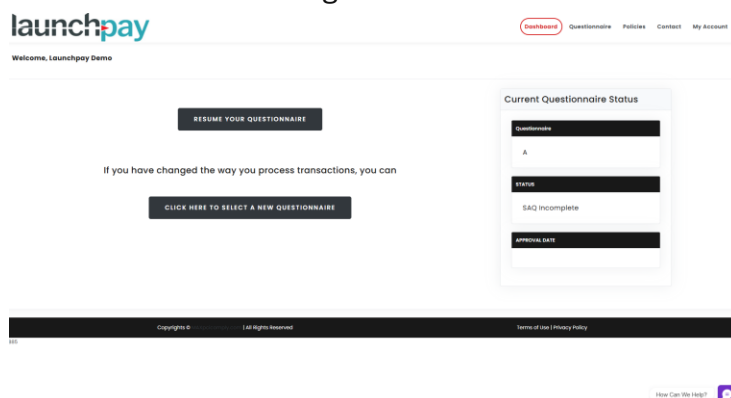
Launchpay Demo

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:



They are also available by phone or email at:

- Phone: 800-803-8515
- Email: support@maxpcicomply.com