

# PCI Compliance

## Setup Guide for Chalk It Pro Users

---

1	Log in to the PCI portal using credentials from your setup email.
2	Select Product Code ( <b>SAQ A – Pay by Invoice/HPP</b> ) and complete Merchant Information: Payment Channels, Relationships, and Processing Solution.
3	Complete the Questionnaire — read each section, check the attestation box, and click Continue.

*Need help? Call PCI Compliance Support: **844-870-2824** | Or click "Contact Us" in the PCI Portal.*

## Step 1 — Log In & Get Started

Check your email for your PCI portal credentials. When entering your username and password, **do not include any punctuation** — enter only the letters and numbers as shown.

Once logged in, click **Get Started** to proceed.

## Step 2 — Select Product Code

In the **upper right corner** of your screen, select the Product Code dropdown and choose:

**SAQ A – Pay by Invoice/HPP**

### Part 1 — Merchant Information

Review your pre-filled **Merchant Information** for accuracy. No changes are typically needed.

Home My Account Contact Us CHAT Welcome Nathan Steele - 743147596349 Logout English US

Summary Questionnaire Documents Resources

Merchant Information

PRODUCT CODE  
SAQ A - Pay by Invoice/HPP

Part 1 Merchant Information Edit

Please confirm that the information below is correct:

CORPORATE NAME	DBA(S)	CONTACT NAME	TITLE
	Chalk It Pro, LLC	Nathan Steele	-
ADDRESS	TELEPHONE	EMAIL ADDRESS	
United States of America		info@chalkitpro.com	

Is your organization a service provider as defined by the PCI Council (e.g., hosting providers, payment processors, managed service providers)? Yes No

### Part 2 — Merchant Business Payment Channels

- **Mail Order / Telephone Order (MOTO):** Select **NO**.
- **E-Commerce:** Select **NO**.
- Do not modify any other fields. Click **SAVE**.

Part 2 Merchant Business Payment Channels

Please answer the following questions:

Indicate all payment channels used by the business that are included in this assessment:

Mail order/telephone order (MOTO) Do you electronically store or transmit consumer account data? Yes No

E-Commerce Do you electronically store or transmit consumer account data? Yes No

Card-present Do you electronically store or transmit consumer account data? Yes No

Are any payment channels not included in this assessment? Yes No

Save

### Part 3 — Relationships

- First question: Select **YES**.
- Second and third questions: Select **NO**.
- **Service Provider:** Enter **Stax Payments**.
- **Description:** Enter **Chalk It Pro**.
- Click **Save**.

**Part 3 Relationships**  
Please answer the following questions.

Do you have relationships with third-party service providers that handle your account data, such as payment gateways or processors?  Yes  No

---

Do you engage with third-party service providers managing system components within your PCI DSS assessment scope?  Yes  No

---

Do you work with third-party service providers that could impact the security of your Cardholder Data Environment?  Yes  No

SERVICE PROVIDER \*  
Enter Service Provider Here

DESCRIPTION \*  
Name of Partner with whom you contract for payments


[Add additional](#)


[Save](#)


### Part 4 — Processing Solution


No changes should be required here, but this is typically what we see for this section. Check the box to agree to the end-user license agreement, then click **Save & Continue**.


**Part 4 Processing Solution**  
What solution do you use to process credit cards? [Learn More](#) PRODUCT CODE  
SAQ A - Pay by Invoice/HPP


  
Moto/E-commerce


  
Terminal

  
Mobile Processing

  
Standalone Computer

  
Integrated Network

  
P2PE

  
SPoC

Do you store any sensitive cardholder data electronically?  Yes  No

Does your business use network segmentation to affect the scope of your PCI DSS environment?  Yes  No

**Moto/E-commerce**  Collapse

How do you process payments?  
 Integrated Payment  
  JavaScript/Direct Post  
  Hosted Payment and iFrame  
  Dial Pay

Does your website use either a redirection mechanism or an embedded payment form?  
 Yes  
  No

**Solution Selection**

Service Provider	Service	Not Listed
Approved Software Provider	Link to Invoice Payment Page	✓

I have read and agreed to the [end-user license agreement](#)

[Select Questionnaire Manually](#)  
 [Save & Continue](#)

## Step 3 — Questionnaire

### Part 1 — Protect Stored Account Data

Read through the section carefully, check the box to attest, then click **Continue**.

Questionnaire A Pass Standard SAQ Change Questionnaire

You have completed 3 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](#)

### Part 2 — Restrict Physical Access to Cardholder Data

Read through the section carefully, check the box to attest, then click **Continue**.

Questionnaire A Pass Standard SAQ Change Questionnaire

You have completed 3 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](#)

### Part 3 — Support Information Security with Organizational Policies and Programs

Read through the section carefully, check the box to attest, then click **Continue**.

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](#)