

PCI Apply Set-up Instructions with Aperia

Once the store is set up to process with Clark Brands, an email will be sent from Clark Brands for your locations providing the URL to enroll in PCI Apply.com providing information needed to finalize portal registration , including Username and temporary password.

- Username = 13-digit Store Merchant ID #
- Temporary Password = Last Five digits of Merchant ID # and state initial.

Example- User Name= Merchant ID Name = 123456789101

Temporary Password = 89101WI

Note: If you have lost or forgotten your password contact Andres Romero or Jamie Tocki at Clark Crown Client Services for assistance. 1-877-462-5275 Ext 9

Example of Clark Brands communication.

Merchant Name: [Jamie Test](#)

PCI Merchant ID Number (last six digits): 000001

All merchants accepting credit/debit card payments are required by the Card Brands (VISA, MasterCard, AMEX, and Discover) to be Payment Card Industry (PCI) compliant. Merchants must ensure they safeguard all customer account data by achieving and maintaining PCI compliance. We have a user-friendly application with high-level support to quickly meet the requirements.

The PCI application can be found at www.clarkbrands.com/pcidss. The username is the complete merchant ID, which can also be found on the welcome letter and the password is the last five digits of the merchant ID and capitalized state abbreviation. For example, if the merchant ID is 335172123456 and is located in Illinois, the login information will be 335172123456 as the username with a password of 23456IL.

After you log into the portal, you will need to complete the profile for your location. In Part 4 -Processing solution, please select the product code for your POS and software version. This will auto populate this section with the information for your location.

Please log in to the portal to complete the self-assessment questionnaire (SAQ) and scan, if applicable, within 90 days from the day you start processing with Clark to avoid any non-compliance fees.

If you need help with your merchant number and/or have questions on which product code to select, please contact our Client Services team at 877-462-5275 or by email at clientservices@clarkbrands.com.

If you need any help with the self-assessment questionnaire (SAQ) and/or scanning, please call our PCI team at 1-877-393-8921.

NEXT

Change the Password.

- The location will receive a communication from Aperia- requesting the site to change the given password previously provided in the intro letter from Clark.

Address the Security Question.

- Choose and provide an answer to the security question. .

Example of Communication received via e-mail from PCI Apply

You are being asked to change your password because this is your first time logging in or it has been 90 days or more since your last login and your password has expired. Passwords are case sensitive. Strong passwords include a combination of Numbers, Letters, and Special Characters such as "-" or "!".

Note: The password must be a minimum of 8 characters, contain at least 1 number, 1 alpha character and cannot contain the characters < or >.

Old Password *	<input type="password"/>	<input type="password"/>
New Password *	<input type="password"/>	Re-Enter New Password *
SECURITY QUESTION * Where were you born?	<input type="text"/>	SECURITY ANSWER *

NEXT

Answer the Product Type question which pertains to the software version of the POS or Commander is operating with for the SAQ. If Product Type is not available use what is available.

Merchant Information Questionnaire Selection Questionnaire Review and Sign

Merchant Information

PRODUCT CODE
Gilbarco Passport-Version 20+

PRODUCT CODE
Not Applicable
Gilbarco Passport-Version 20+
Gilbarco Passport v11.01
Verifone Base 43
Verifone Base 44
Verifone Base 49
Verifone Base 51
Verifone v3.12
Virtual Terminal

NEXT PCI Compliance Tool – Guides you through the five basic steps to Compliance.

Welcome to your PCI Compliance Tool.

Why PCI Compliance matters?

- PCI (Payment Card Industry) Compliance is a yearly requirement for all merchants who accept and process credit/debit card payments.
- These security standards are mandated by the PCI Council (Visa, MasterCard, American Express, Discover and JCB) to ensure that Barb's test is following the best processing practices which increases the confidence in the safety of the credit card data you process.

Let's Get Started!

This tool will guide you through the 5 basic steps to compliance.



Merchant Information



Questionnaire Selection



Questionnaire and Network
Scan



Review and Sign



Print Reports

NEXT Confirm that the Merchant Information is Correct.

Part 1 Merchant Information

Please confirm that the information below is correct:

CORPORATE NAME	DBA(S)	CONTACT NAME	TITLE
-	Barb's test	Barb Nolan	-
ADDRESS	TELEPHONE	EMAIL ADDRESS	
750 Warrenville Road Lisle, Illinois 60532 United States of America	(877) 462-5275	bnolan@clarkbrands.com	

NEXT Indicate Payment Channel Used and check the appropriate box. In most case it will be "card present."

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) ⓘ
- E-Commerce ⓘ
- Card-present ⓘ

Are any payment channels not included in this assessment?

Yes

No

Card-present transactions happen when customers physically present their payment cards to merchants at a point of sale, like in retail stores, restaurants, or at an ATM. The card is swiped, inserted, or tapped to complete the transaction securely.

NEXT Address Relationship with Third Parties by checking yes or no. (Don't forget to 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

Save

Here is an example of a completed part 3 Relationship with Third Parties .

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 *
First Data

DESCRIPTION *
Processor








[Add additional](#)

Save

NEXT: Choose Your Processing Solution for Credit Cards

Part 4 Processing Solution

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

 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

Integrated Network ⊖ Collapse			
Solution Selection			
Vendor	Application	Version	Not Listed
Gilbarco Inc.	Passport EDH (Fiserv - First Data)	11.23.01.*	

Integrated Network Collapse			
Solution Selection			
Vendor	Application	Version	Not Listed
Gilbarco Inc.	Passport EDH (Fiserv - First Data)	11.23.01.*	

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

Select Questionnaire Manually

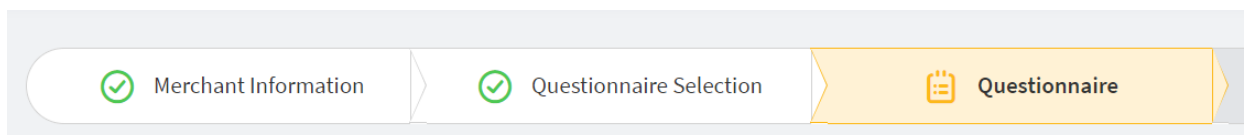
Save & Continue

Confirm your eligibility to take questionnaire C ✕

1. Your establishment has a payment application system and an Internet connection on the same device and/or same local network (LAN).
2. My payment application system is not connected to any other systems and/or locations.
3. You retain only paper reports or receipts with cardholder data, and these documents are not received electronically.

I agree that the statements above are true.

[Continue](#)



Most convenient /gas locations will be required to complete SAQ C.

If you have multiple locations that process with the same POS and utilize the same processing environment your locations can be chained to allow one SAQ for all locations. Contact Cark Client Services team for further details.

Questionnaire C In Progress

Please continue through all sections until complete.

<p>SECTION 1</p> <p>Install and maintain network security controls</p> <p>3 Questions</p> <p>Not Started</p>	<p>SECTION 2</p> <p>Apply Secure Configurations to All System Components</p> <p>10 Questions</p> <p>Not Started</p>	<p>SECTION 3</p> <p>Protect Stored Account Data</p> <p>5 Questions</p> <p>Not Started</p>
<p>SECTION 4</p> <p>Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks</p> <p>3 Questions</p> <p>Not Started</p>	<p>SECTION 5</p> <p>Protect All Systems and Networks from Malicious Software</p> <p>12 Questions</p> <p>Not Started</p>	<p>SECTION 6</p> <p>Develop and Maintain Secure Systems and Software</p> <p>8 Questions</p> <p>Not Started</p>
<p>SECTION 7</p> <p>Restrict Access to System Components and Cardholder Data by Business Need to Know</p> <p>4 Questions</p> <p>Not Started</p>	<p>SECTION 8</p> <p>Identify Users and Authenticate Access to System Components</p> <p>24 Questions</p> <p>Not Started</p>	<p>SECTION 9</p> <p>Restrict Physical Access to Cardholder Data</p> <p>14 Questions</p> <p>Not Started</p>
<p>SECTION 10</p> <p>Log and Monitor All Access to System Components and Cardholder Data</p> <p>18 Questions</p> <p>Not Started</p>	<p>SECTION 11</p> <p>Test Security of Systems and Networks Regularly</p> <p>8 Questions</p> <p>Not Started</p>	<p>SECTION 12</p> <p>Support Information Security with Organizational Policies and Programs</p> <p>14 Questions</p> <p>Not Started</p>
<p>SECTION 13</p> <p>Network Scan</p> <p>Not Started</p>	<p>SECTION 14</p> <p>Progress Report and Charts</p>	<p>Continue To Scan</p>



Once you have completed your appropriate PCI compliance Self Assessment Questionnaire (SAQ) be sure to schedule your scan.

ASV Compliance Status Not Started

To initiate network scan process, you need to have your IP Address/Domain scanned.

SCAN TIMING
Normal

Scan Targets



A scan target is necessary to launch a scan, please add a scan target.

Add Scan Target

Scan Target Status Summary



Your scan target has not been scanned.