

## Trustwave SAQ B "Wizard" Level Guidance

**SAQ B** is *only* applicable for merchants who normally process credit cards using a credit card terminal using an analog phone line. It does *not* include processing credit cards through a computer or a website. Contact UM Treasury for assistance if this doesn't apply to your situation. This template could vary slightly from your screens viewed depending on if you have different selections/circumstances.

You should see one of the two screens below. If your *merchant account is new*, you should see the screen to left. If you are *renewing the SAQ* for this year, you should see the screen to the right or Screen 3 (two pages below).

### Screen 1 – SAQ for a brand new merchant account

#### Registration

You will arrive at the Trustwave website from the Trustwave email invitation link. Registration is a one-time occurrence for the merchant account. Look for **red text** for UM Treasury guidance. **Red** outlined boxes require entry.

Enter data on the right side of screen and click "Continue>>."

**These fields should be pre-filled**

**Complete these fields**

Company Name: Mcard  
Merchant ID: 123456789  
Country: United States of America  
ZIP/Postal Code: 48109

Authorized Contact  
Primary Contact:  This is for the actual PCI certification user, who will be the primary person contacting support.  
First Name:   
Last Name:   
Email:   
Phone Number:

Continue >>

### Screen 1 – Renewing the annual SAQ

After logging in, you'll see the "PCI Home" screen. Simply click "Start" to begin.

Trustwave TrustKeeper

PCI Manager | PCI Home | Merchant Profile | Documents | Trusted Commerce | User Management

no system notifications

**Click "Start"**

PCI Certification Status

PCI Self-Assessment  
Summary | History & Documents  
Recent: 2016-02-09 ✓

Trusted Commerce Seal  
Placing this seal on your website indicates that you are taking steps to secure credit card information.  
More Info

PCI Status  
Next Certification Deadline: 2017-02-09

Certificate of Compliance  
Attestation of Compliance

Screen 2 – SAQ for a brand new merchant account

Create a log in. Note: If you have more than one merchant account, you'll need to create separate Trustwave logons (usernames) for each. It's highly recommended that you create answers for the "Security Questions" to assist if you cannot recall your logon created in the future.

Click "Register"

Screen 2 – Renewing the annual SAQ

You will either see the screen **below** or the one on the **next page** (Screen 3).

If you see the screen just below,

Do **NOT** select "Express Renewal."\*  
Select "Start new Self-Assessment."  
Then click "Next" to begin.

\*New PCI compliance requirements/questions are easily missed using "Express Renewal."

## Account Profile

Screen 3

Trustwave®  
TrustKeeper™

PCI

messages

**PCI Manager**    PCI Home    Merchant Profile    Documents    Trusted Commerce

no system notifications

**Tell us about your business**

**Select "In Person" and/or "Mail/Telephone" depending on how you process credit card transactions.**

**Do *not* select Website - Contact UM Treasury for help.**

1 How do you accept credit cards? Select all that apply.

Customers can make purchases with their credit cards on my website.

Website

Customers can make purchases by mail or by telephone.

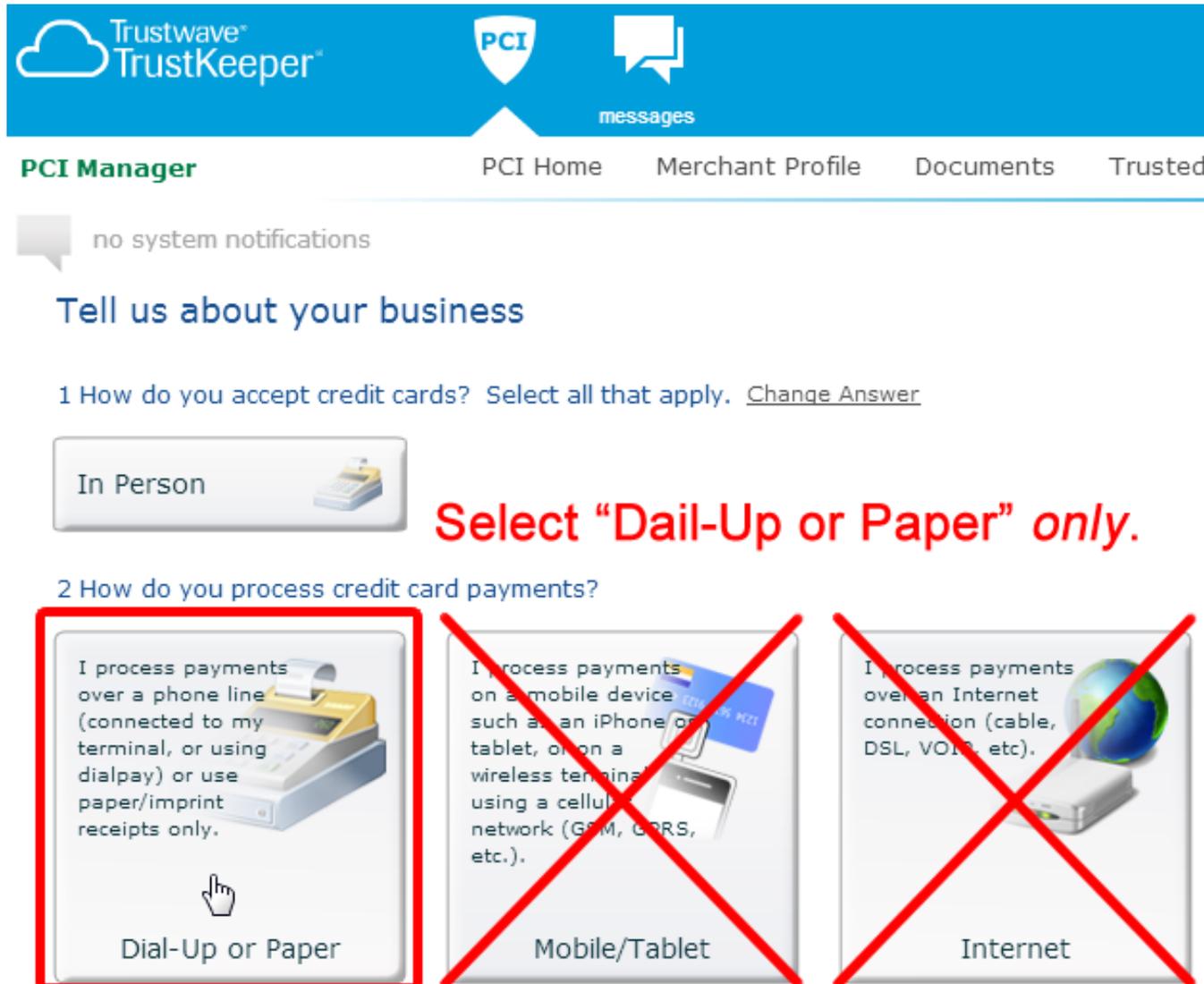
Mail/Telephone

Customers can make purchases by visiting my store, office, restaurant, etc.

In Person

**Next**

Screen 4



The screenshot shows the PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header, the navigation bar includes "PCI Manager", "PCI Home", "Merchant Profile", "Documents", and "Trusted". A notification bubble indicates "no system notifications". The main content area features the heading "Tell us about your business" and a survey question: "1 How do you accept credit cards? Select all that apply. [Change Answer](#)".

Below the question, there is a button labeled "In Person" with a credit card terminal icon. A red annotation "Select 'Dial-Up or Paper' only." is overlaid on this button. Below this, question "2 How do you process credit card payments?" is shown with three options:

- Dial-Up or Paper:** "I process payments over a phone line (connected to my terminal, or using dialpay) or use paper/imprint receipts only." This option is highlighted with a red border and a mouse cursor icon.
- Mobile/Tablet:** "I process payments on a mobile device such as an iPhone or tablet, or on a wireless terminal using a cellular network (GSM, GPRS, etc.)." This option is crossed out with a large red X.
- Internet:** "I process payments over an Internet connection (cable, DSL, VOIP, etc.)." This option is also crossed out with a large red X.

Screen 5

Trustwave®  
TrustKeeper™

PCI

messages

PCI Manager

PCI Home

Merchant Profile

D

no system notifications

## Tell us about your business

1 How do you accept credit cards? Select all that apply. [Change Answer](#)

In Person 

2 How do you process credit card payments? [Change Answer](#)

Dial-Up or Paper 

 [Continue >>](#) 

Screen 6

The screenshot displays the Trustwave TrustKeeper PCI Manager interface. At the top, there is a blue header with the TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation menu with links for PCI Home, Merchant Profile, Security Policy, Training, Documents, and Trusted Commerce. A notification bubble indicates "no system notifications". The main content area features a progress bar with four steps: 1 Overview, 2 Merchant Profile, 3 Business Environment, and 4 Questionnaire. Step 1 is highlighted in green. Below the progress bar, there are three columns of content. The first column, under "Next Steps", contains a red instruction: "No input required, just click 'Next' below". The second column, "2 Merchant Profile", lists "Contact Info", "Account Details", and "Review Merchant IDs" with an icon of a person and an email symbol. The third column, "3 Business Environment", lists "Products and Payment Applications", "Web Sites", "Service Providers", and "Network Vulnerability Scan Setup (if applicable)" with an icon of buildings. The fourth column, "4 Questionnaire", describes it as the largest step and lists "Choose Express Renewal, if qualified", "Complete the PCI Self-Assessment Questionnaire, using the PCI Wizard or expert form", and "Review and Submit your Self-Assessment" with a questionnaire icon. At the bottom right, a red arrow points to a green "Next" button with a mouse cursor hovering over it.

Trustwave TrustKeeper

PCI messages

PCI Manager PCI Home Merchant Profile Security Policy Training Documents Trusted Commerce

no system notifications

Start Over

1 Overview 2 Merchant Profile 3 Business Environment 4 Questionnaire

**Next Steps**

*No input required, just click "Next" below*

- Contact Info
- Account Details
- Review Merchant IDs

- Products and Payment Applications
- Web Sites
- Service Providers
- Network Vulnerability Scan Setup (if applicable)

This is the largest step, where you will:

- Choose Express Renewal, if qualified
- Complete the PCI Self-Assessment Questionnaire, using the PCI Wizard or expert form
- Review and Submit your Self-Assessment

Next

Screen 7

The screenshot shows the PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header, the navigation bar includes "PCI Manager", "PCI Home", "Merchant Profile", "Security Policy", "Training", "Documents", and "Trusted Comme". A notification bubble indicates "no system notifications". A progress bar shows four steps: "1 Overview", "2 Merchant Profile" (current), "3 Business Environment", and "4 Questionnaire". The breadcrumb trail is "Account Details > Status Reporting".

The main form is titled "General Info" and "Additional Info". The "General Info" section includes fields for Company (Mcard), Industry (Please Select), Primary Contact (dave doyle[davedoyle]), Secondary Contact (Please Select...), Mailing Address, City, Country (United States of America), State (Please Select...), and ZIP/Postal Code (48109). Red annotations highlight several fields: "Education/University" for Industry, "your name" for Primary Contact, "optional" for Secondary Contact, "use US mailing address" for Mailing Address and City, and "MI" for State. A red arrow points to the "Next" button.

**Complete these fields**

**General Info**

Company: Mcard

Industry: \* Please Select *Education/University*

Primary Contact: \* dave doyle[davedoyle] *your name*

Secondary Contact: Please Select... *optional*

Mailing Address: \* *use US mailing address*

City: \* *use US mailing address*

Country: \* United States of America

State: \* Please Select... *MI*

ZIP/Postal Code: \* 48109

**Additional Info**

**Service Providers: \***  
Does your company have a relationship with one or more third-party service providers (e.g. gateways, web-hosting companies, airline booking agents, loyalty program agents, etc.)?  
 Yes  No *Select "No" - unless Treasury says otherwise*

**Multiple Acquirers \***  
Does your company have a relationship with more than one acquirer (e.g. merchant services provider, bank, etc.)?  
 Yes  No *Select "No"*

Screen 8

Trustwave TrustKeeper

PCI messages

PCI Manager

PCI Home Merchant Profile Security Policy Training Documents Trusted Commer

notification history available

Start Over 1 Overview 2 Merchant Profile 3 Business Environment 4 Questionnaire

Account Details > Status Reporting

**PCI Assessment and Status Reporting**

*No input required, just click "Next" below*

PCI Program: DEMO University of Michigan ?

Included in this Account:

Merchant ID	Primary
123456789	✓

Previous Next

Screen 9

Trustwave® TrustKeeper®

PCI messages

PCI Manager    PCI Home    Merchant Profile    Security Policy    Training    Documents    Trusted Comme

notification history available

Start Over    1 Overview    2 Merchant Profile    3 Business Environment    4 Questionnaire

Card Acceptance > Products

**Verify Your Card Acceptance Information**

In Person Purchases	Yes
Mail or Telephone Orders	No <b>Ignore "No". You can process credit card transactions received via US mail or by phone</b>
Website Orders	No
Other Details	You only use a dial-up terminal that is not connected to the Internet to process credit card transactions at your business.

**No input required, just click "Next" below**

**If the credit card acceptance method is incorrect, contact Treasury before clicking the "Change" button**

Previous    Change    **Next**

Screen 10

Trustwave<sup>™</sup>  
TrustKeeper<sup>™</sup>

PCI

messages

PCI Manager    PCI Home    Merchant Profile    Documents    Trusted Commerce    User Management

no system notifications

Start Over    1 Overview    2 Merchant Profile    3 Business Environment    4 Questionnaire

Card Acceptance > Products

### Products

1.0 Please identify any devices (terminals, payment software applications, services, etc.) you use to process credit card purchases from your customers in person, over the phone, or through mail order.

Product	Version	Product Type	Entered By	Severity

*It is not necessary to add devices at this time. Just click the "I don't use any devices to process cards" box*

**Add Product**     I don't use any devices to process cards

2.0 Provide the name of the third-party company you use to install, configure, or support these products. These companies or individuals may be known as Integrators and/or Resellers, or even IT consultants.

**Select**     I don't use a third-party Integrator or Reseller

Previous    Next

This screen may appear if you previously had indicated that you process Mail Order/Telephone Order credit card transactions.

Screen 11

Trustwave TrustKeeper

PCI messages

PCI Manager PCI Home Merchant Profile Documents Trusted Commerce

notification history available

Start Over 1 Overview 2 Merchant Profile 3 Business Environment 4 Questionnaire

Card Acceptance > Products > Service Providers

### Service Providers

Identify any service providers you use either to host your web site or to handle the credit card processing from web site or mail/telephone orders.

Service Provider	Services	Added By	Severity
<b>You do not need to enter service providers at this time</b>			

Add Service Provider  I don't use any service providers for my mail/telephone orders or to process my web site orders.

Previous Next

**SAQ Completion Selection** (It's possible that a different screen appears regarding *'Express Renewal,'* instead select *'Start a new Self-Assessment'* – see page 2 right column)

Screen 12

**Trustwave® TrustKeeper™** PCI messages TO test account

**PCI Manager** PCI Home Merchant Profile Security Policy Training Documents Trusted Commerce

no system notifications **Contact Support**

Start Over 1 Overview 2 Merchant Profile 3 Business Environment 4 Questionnaire

Wizard Option > ...

**This method asks a series of questions and will extrapolate the answers into the SAQ.**

**Step-By-Step Recommended**

I'd like to simplify completing the certification process. Take me to the step-by-step PCI Wizard:

**Expert Level Form**

I understand the requirements of PCI DSS and I know which SAQ to complete. Skip the Wizard.  
**(Pre-2015 SAQ format)**

**To Do List** 0  
No tasks in your To Do List

*While it may be a bit easier to complete, you will not see each PCI control you are responsible for following.*

*In a few cases if you answer incorrectly, it may lead you into another longer SAQ.*

*You can opt to select the "Expert Level form" which is the same format as SAQs prior to 2015.*

Step 1 Step 2 Step 3

PCI DSS Questions	Yes	No	Special
35. Are web browsers in place for the use of these system resources? - Card apps, e-commerce, e-mail, e-DB	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
36. Are logging and audit trails enabled and unique to each entity's cardholder data environment? - PCI DSS Requirement 10.7 is logging enabled as follows for each merchant and service provider environment.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
37. Logs are enabled for external third party applications?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
38. Logs are active by default?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
39. Logs are available for review by the owning entity?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
40. Log content is stored in tamper-resistant storage?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Previous Next

Screen 13

Note: you can click on the circled question mark or "i" for additional info/clarification.

The screenshot shows the Trustwave TrustKeeper PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header, there is a navigation bar with links for PCI Home, Merchant Profile, Security Policy, Training, and Documents. A notification area shows "no system notifications". A progress bar indicates the current step is "4 Questionnaire", with previous steps being "1 Overview", "2 Merchant Profile", and "3 Business Environment". The breadcrumb trail reads: Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form. The main content area is titled "Card Data Storage & Processing" and contains a "Save & Close" button. The section is titled "Credit Card Data Storage" with a circled question mark icon and a red arrow pointing to it with the text "Click the ? for clarification". The question is "Does your business store any sensitive credit card data electronically?". There are five radio button options: "Yes, I have a payment application or device that stores credit card data.", "Yes, I store credit card data in a computer.", "Yes, I receive credit card data from a third-party in electronic format.", "Yes, I store credit card data in some other way.", and "None of the above - I never store credit card data. *standard answer*". A red box highlights the "None of the above" option. To the right of the options, there is a red warning: "If you click Yes to any of these boxes, contact UM Treasury". At the bottom, there are "Previous" and "Next" buttons, with a red arrow pointing to the "Next" button.

Trustwave®  
TrustKeeper™

PCI

messages

PCI Manager

PCI Home Merchant Profile Security Policy Training Documents

no system notifications

Start Over 1 Overview 2 Merchant Profile 3 Business Environment 4 Questionnaire

Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form

**Cannot store full credit card numbers or 3 or 4 digits CVC numbers electronically or on paper!**

### Card Data Storage & Processing

Save & Close

Credit Card Data Storage ? ← Click the ? for clarification

Does your business store any sensitive credit card data electronically?

- Yes, I have a payment application or device that stores credit card data.
- Yes, I store credit card data in a computer.
- Yes, I receive credit card data from a third-party in electronic format.
- Yes, I store credit card data in some other way.
- None of the above - I never store credit card data. *standard answer*

If you click Yes to any of these boxes, contact UM Treasury

<< Previous Next >>

Screen 14

The screenshot shows the Trustwave PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation bar with links for PCI Home, Merchant Profile, Security Policy, Training, and Documents. A notification area shows 'no system notifications'. A progress bar indicates the current step is '4 Questionnaire', with previous steps being '1 Overview', '2 Merchant Profile', and '3 Business Environment'. A breadcrumb trail shows the path: Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form.

The main content area is titled 'Card Data Storage & Processing' and includes a 'Save & Close' button. The question is 'Number of Locations' with a help icon. The question text is 'How many locations do you have that take credit cards?'. There are five radio button options: None, 1, 2 - 5, 5 - 20, and More than 20. To the right of the options, there are three red text annotations: 'Select the number of separate locations where credit cards are accepted specifically related to this merchant account.', 'Usually this is "1."', and 'Do not count multiple stores/locations that are related to different merchant accounts.' At the bottom, there are 'Previous' and 'Next' buttons, with a red arrow pointing to the 'Next' button.

Screen 15

The screenshot shows the Trustwave PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation bar with links for PCI Home, Merchant Profile, Security Policy, Training, and Documents. A notification bubble indicates "no system notifications". A progress bar shows four steps: 1 Overview, 2 Merchant Profile, 3 Business Environment, and 4 Questionnaire. The current step is "Card Data Storage & Processing" under the "Self-Assessment Questionnaire Form".

### Card Data Storage & Processing

Save & Close

#### POS Communication

Based on your earlier selections, you only use standalone POS terminals. How do these terminals communicate for processing transactions?

- Dial-up telephone line **Credit card terminals must only use a dial-up phone line**
- Internet
- Mobile network (Cellular, GSM, GPRS, LTE, etc.)

<< Previous    Next >>

Screen 16

The screenshot shows the Trustwave TrustKeeper PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header, the main navigation bar includes "PCI Manager" and several menu items: "PCI Home", "Merchant Profile", "Security Policy", "Training", and "Documents". A notification area below the navigation bar shows "no system notifications". A progress bar indicates the current step is "4 Questionnaire", with previous steps being "1 Overview", "2 Merchant Profile", and "3 Business Environment". A breadcrumb trail shows the path: "Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form".

The main content area is titled "Card Data Storage & Processing" and includes a "Save & Close" button in the top right corner. Under the "Network Usage" section, the question is "Do you ever process transactions over the Internet or an internal network?". There are two radio button options: "Yes" (unselected) and "No" (selected). To the right of the options, there are two red text warnings: "Credit card terminals are not allowed to process transactions over the Internet or a network." and "Do not include online processing for a different merchant account." At the bottom of the form, there are two buttons: "<< Previous" and "Next >>". A red arrow points to the "Next >>" button, which is being clicked by a mouse cursor.

Screen 17

The screenshot displays the Trustwave TrustKeeper PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header, the main navigation bar includes 'PCI Manager', 'PCI Home', 'Merchant Profile', 'Security Policy', 'Training', and 'Documents'. A notification area shows 'no system notifications'. A progress bar indicates four steps: '1 Overview', '2 Merchant Profile', '3 Business Environment', and '4 Questionnaire', with the current step being '4 Questionnaire'. The breadcrumb trail reads: 'Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form'. A large modal window is open, titled 'Card Data Storage & Processing', with a green checkmark icon and the text 'Section Completed! You have successfully completed this section and passed.' A 'Close' button is in the top right of the modal. A red arrow points to a 'continue >>' button at the bottom left of the modal, which is being clicked by a mouse cursor. At the bottom right of the page, there is a link: 'Continue the PCI Wizard >>'.

Screen 18

Trustwave®  
TrustKeeper®

PCI

messages

**PCI Manager**    PCI Home    Merchant Profile    Security Policy    Training    Documents

no system notifications

Start Over ↻    1 Overview    2 Merchant Profile    3 Business Environment    **4 Questionnaire**

Wizard Option > Card Data Storage & Processing > **PCI Wizard** > Self-Assessment Questionnaire Form

**Physical Security**   

**Security Policies**

Screen 19

The screenshot displays the Trustwave TrustKeeper PCI Manager interface. At the top, there is a blue header with the TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation bar with links for PCI Home, Merchant Profile, Security Policy, Training, and Documents. A notification bubble indicates "no system notifications". A progress bar shows four steps: 1 Overview, 2 Merchant Profile, 3 Business Environment, and 4 Questionnaire. The current step is "PCI Wizard" under "Self-Assessment Questionnaire Form".

The main content area is titled "Physical Security" and contains a section for "Paper Documents with Credit Card Data". The question asks: "Does your business have or receive any paper documents containing full credit card numbers (see help for examples)?" with radio button options for "Yes" and "No". A red instruction reads: "Answer Yes or No depending on your situation." At the bottom of this section are "Previous" and "Next" navigation buttons, with a red arrow pointing to the "Next" button.

Below the "Physical Security" section is a "Security Policies" section with a "Begin" button.

Screen 20

The screenshot shows the Trustwave PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation bar with links for PCI Home, Merchant Profile, Security Policy, Training, and Documents. A notification bubble indicates "no system notifications". A progress bar shows four steps: 1 Overview, 2 Merchant Profile, 3 Business Environment, and 4 Questionnaire, with the current step highlighted. The breadcrumb trail reads: Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form.

**Physical Security** Save & Close

**Restrict Access to POS Devices** ⓘ

Is access to your payment equipment limited to employees who require access, and restricted to just what functions they need to do their jobs?

Yes  
 No

*Per internal controls, only staff who have completed the Merchant Certification TME102 course (annually) and are "authorized users" in FINPROD are able to process credit card transactions.*

*Credit card terminals must always be kept in secure location, including locked up after business hours.*

<< Previous Next >> Begin

Screen 21

The screenshot shows the Trustwave PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header, a navigation bar includes "PCI Manager" and links for "PCI Home", "Merchant Profile", "Security Policy", "Training", and "Documents". A notification bubble indicates "no system notifications". A progress bar shows four steps: "1 Overview", "2 Merchant Profile", "3 Business Environment", and "4 Questionnaire", with "4 Questionnaire" being the active step. Below the progress bar, the breadcrumb trail reads "Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form".

**Physical Security** Save & Close

*Below are new requirements for 2015 and beyond  
You can check the 3 boxes below if you  
immediately implement each one.*

**Keep Track of POS Devices** ⓘ

Do you maintain a list of all of your payment equipment, as follows (check all that apply)?

- The list includes all card-reading devices.
- The list includes the device make and model, the location, and the serial number or similar identifier.
- The list is kept up-to-date when devices are added, relocated, or removed from operation.
- No (none of the above apply, or I don't maintain such a list)

<< Previous    Next >>

**Security Policies** Begin

Screen 22

Remember that credit card terminals must be secured from unauthorized individuals, which includes locking up the device after business hours. PCI version 3.0 effective for 2015 and beyond requires all merchants to frequently (daily) inspect their credit card terminals for tampering.

The screenshot shows the Trustwave PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation bar with links for PCI Manager, PCI Home, Merchant Profile, Security Policy, Training, and Documents. A notification bubble indicates 'no system notifications'. A progress bar shows four steps: 1 Overview, 2 Merchant Profile, 3 Business Environment, and 4 Questionnaire. The current step is 'Self-Assessment Questionnaire Form' under the 'PCI Wizard' section. The main content area is titled 'Physical Security' and contains a question: 'Do you have trained employees periodically inspect your payment equipment for signs of tampering or unauthorized replacement?'. There are two radio button options: 'Yes' (selected) and 'No'. To the right of the question, there are two red text annotations: 'UM Treasury's Merchant Services website has terminal tampering training for your staff.' and 'Only UM Treasury staff are allowed to repair or replace your credit card terminal.' At the bottom of the question area are 'Previous' and 'Next' buttons, with a red arrow pointing to the 'Next' button. Below the question area is a 'Security Policies' section with a 'Begin' button.

Screen 23

The screenshot displays the Trustwave TrustKeeper PCI Manager interface. At the top, there is a blue header with the TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation bar with links for PCI Home, Merchant Profile, Security Policy, Training, and Documents. A notification area shows 'no system notifications'. A progress bar indicates four steps: 1 Overview, 2 Merchant Profile, 3 Business Environment, and 4 Questionnaire. The current step is 'PCI Wizard' under 'Self-Assessment Questionnaire Form'. The main content area features a 'Physical Security' section with a green checkmark icon and the text 'Section Completed! You have successfully completed this section and passed.' A 'Close' button is in the top right of this section. A red arrow points to a 'continue >>' button at the bottom left. Below this is a 'Security Policies' section with a 'Begin' button.

Screen 24

The screenshot displays the Trustwave TrustKeeper PCI Manager interface. At the top, there is a blue header with the TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation bar with links for PCI Home, Merchant Profile, Security Policy, Training, and Documents. A notification area shows "no system notifications". A progress bar indicates the current step is "4 Questionnaire", with previous steps being "1 Overview", "2 Merchant Profile", and "3 Business Environment". A breadcrumb trail shows the path: Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form.

The main content area is titled "Physical Security" with a green checkmark icon and a "Review Q & A" button. Below this is a section for "Security Policies" with a "Save & Close" button. The current policy is "Sharing Card Data with Third-Parties" with an information icon. The question asks: "Are there any third-party companies with whom you share any credit card data, or who could affect the security of the credit card data?". Two radio buttons are present: "Yes" (unselected) and "No" (selected). A red text annotation reads: "Merchants cannot share sensitive credit card data with 3rd parties". At the bottom, there are navigation buttons: "<< Previous" and "Next >>". A red arrow points to the "Next >>" button, which has a mouse cursor over it.

Trustwave® TrustKeeper™

PCI messages

**PCI Manager** PCI Home Merchant Profile Security Policy Training Docume

no system notifications

Start Over ↻ 1 Overview 2 Merchant Profile 3 Business Environment 4 Questionnaire

Wizard Option > Card Data Storage & Processing > **PCI Wizard** > Self-Assessment Questionnaire Form

**All employees are bound by university policies including:**

- ✓ **Physical Security**
  - SPG 601.27 Info Security Policy
  - SPG 601.7 Proper Use of Info Resources, Info Tech, & Networks at UM[Review Q & A](#)

**Security Policies** [Save & Close](#)

**Maintain Written Security Policies** ⓘ *Failure to comply with these policies may result in disciplinary action including termination.*

Do you have written security policies and procedures that address the protection of paper with credit card numbers such as receipts and the physical security of your card processing devices?

- Yes ***This should be in your internal controls written procedures***
- Yes, I use the security policies included in my subscription.
- No

[<< Previous](#) [Next >>](#)

Screen 26

Trustwave  
TrustKeeper

PCI

messages

**PCI Manager**    PCI Home    Merchant Profile    Security Policy    Training    Docume

no system notifications

Start Over ↻    1 Overview    2 Merchant Profile    3 Business Environment    **4 Questionnaire**

Wizard Option > Card Data Storage & Processing > **PCI Wizard** > Self-Assessment Questionnaire Form

✓ **Physical Security**    Review Q & A

**Security Policies**    Save & Close

**Define Security Responsibilities** ⓘ

Does your security policy clearly define responsibilities regarding protecting credit card data for all employees and contractors?

Yes  
 No

*This should be in your internal controls written procedures*

<< Previous    Next >>

Trustwave®  
TrustKeeper®

PCI

messages

**PCI Manager**    PCI Home    Merchant Profile    Security Policy    Training    Document

no system notifications

Start Over    1 Overview    2 Merchant Profile    3 Business Environment    **4 Questionnaire**

Wizard Option > Card Data Storage & Processing > **PCI Wizard** > Self-Assessment Questionnaire Form

✓ **Physical Security**    Review Q & A

**Security Policies**    Save & Close

**Review Security Policies Annually** ⓘ

Do you review and modify your policies at least once a year or any time you make a change to your business environment?

Yes  
 No

**Your internal controls written procedures and gap analysis should be reviewed and updated at least annually.**

<< Previous    **Next >>**

The screenshot shows the Trustwave PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation bar with links for PCI Manager, PCI Home, Merchant Profile, Security Policy, Training, and Documents. A notification area indicates 'no system notifications'. A progress bar shows four steps: Start Over, 1 Overview, 2 Merchant Profile, 3 Business Environment, and 4 Questionnaire. The current step is 4 Questionnaire, with a breadcrumb trail: Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form.

The main content area is divided into two sections:

- Physical Security**: Indicated by a green checkmark and a 'Review Q & A' button.
- Security Policies**: Indicated by a yellow warning triangle and a 'Save & Close' button. This section contains a sub-section for **Computer and Device Usage**, which has an information icon (i) next to it. A red arrow points from the text 'Click here for details' to this information icon.

Under the 'Computer and Device Usage' section, there is a question: 'Do your written policies and procedures cover the use of technology as follows (check all that apply):'. Three checkboxes are checked, and one is unchecked:

- Require explicit approval by authorized parties to use the technologies
- Maintain a list of all such devices and personnel with access
- Specify locations the technology can be used and a description of acceptable business usage
- None of the above

Red text annotations are present:

- 'Covered by SPG 601.07' is written in red next to the first three checked items.
- 'NOTE: for most merchants, these are not applicable. However, N/A is not an option and selecting "None of the above" will cause the SAQ to fail. Please check the 3 boxes as shown.' is written in red and blue below the checkboxes.

At the bottom of the 'Security Policies' section, there are navigation buttons: '<< Previous' and 'Next >>'. A red arrow points to the 'Next >>' button.

Trustwave  
TrustKeeper

PCI

messages

PCI Manager

PCI Home Merchant Profile Security Policy Training Document

no system notifications

Start Over

1 Overview

2 Merchant Profile

3 Business Environment

4 Questionnaire

Wizard Option > Card Data Storage & Processing > **PCI Wizard** > Self-Assessment Questionnaire Form

✓ **Physical Security** [Review Q & A](#)

**Security Policies** [Save & Close](#)

**Maintain an Incident Response Plan** ⓘ

In the event of a compromise to customer credit card numbers or to your card processing device, do you have a formal plan on how to respond, including notification of the appropriate law enforcement agency, your merchant bank, and the various card associations?

Yes

No

**As a merchant your initial responsibility is to contact Treasury 763-1299 immediately. If necessary, Treasury will provide additional instructions.**

<< Previous **Next >>**

The screenshot shows the Trustwave PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation bar with links for PCI Home, Merchant Profile, Security Policy, Training, and Documents. A notification bubble indicates "no system notifications". A progress bar shows four steps: 1 Overview, 2 Merchant Profile, 3 Business Environment, and 4 Questionnaire. The current step is 4 Questionnaire, which is highlighted in green. Below the progress bar is a breadcrumb trail: Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form.

The main content area is titled "Physical Security" with a green checkmark icon and a "Review Q & A" button. Below this is a section titled "Security Policies" with a "Save & Close" button. The first policy is "Restrict Sending of Credit Card Data" with an information icon. The question is: "Do you have a policy forbidding employees from sending full credit card numbers over e-mail or other insecure messaging technologies?". There are three radio button options: "Yes" (selected), "No", and "Not Applicable". A red text annotation says "This is a PCI and UM Treasury policy". At the bottom, there are two buttons: "<< Previous" and "Next >>". A red arrow points to the "Next >>" button, and a mouse cursor is hovering over it.

Screen 31

The screenshot shows the PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation bar with links for PCI Home, Merchant Profile, Security Policy, Training, and Documents. A notification area shows 'no system notifications'. A progress bar indicates the current step is '4 Questionnaire', with previous steps being '1 Overview', '2 Merchant Profile', and '3 Business Environment'. A breadcrumb trail shows the path: Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form.

The main content area is titled 'Physical Security' with a green checkmark icon and a 'Review Q & A' button. Below this is the 'Security Policies' section, which includes a 'Save & Close' button and a sub-section titled 'Provide Security Training to Employees' with an information icon. The question asks: 'Do you have a formal training program for all relevant employees that teaches them about security as it relates to credit cards, paper with credit card numbers on them and the devices that process credit card transactions?'. There are three radio button options: 'Yes' (selected), 'Yes, I use the Security Awareness Education included in my subscription.', and 'No'. A red arrow points to the 'Next >>' button at the bottom of the form.

**Annual UM MyLINC Merchant Certification TME102 course**

Trustwave®  
TrustKeeper®

PCI

messages

**PCI Manager**    PCI Home    Merchant Profile    Security Policy    Training    Documents

no system notifications

Start Over    1 Overview    2 Merchant Profile    3 Business Environment    **4 Questionnaire**

Wizard Option > Card Data Storage & Processing > **PCI Wizard** > Self-Assessment Questionnaire Form

✓ **Physical Security**    Review Q & A

**Security Policies**    Save & Close

**Recognize POS Device Tampering** ⓘ

Does your training program cover being alert to attempted tampering of POS devices, such as verifying maintenance personnel and reporting suspicious behavior?

Yes     No

**Beginning in 2015, there are new requirements for protecting credit card terminals such as cataloging terminals and training staff about tampering. Implement the new steps immediately! Treasury's Merchant Services website has terminal tampering training. Only Treasury staff are allowed to repair or replace your terminal.**

<< Previous    Next >>

Screen 33

Trustwave  
TrustKeeper

PCI Home Merchant Profile Documents Trusted Commerce User Management

no system notifications

Start Over 1 Overview 2 Merchant Profile 3 Business Environment 4 Questionnaire

Express Renewal Option > Wizard Option > Card Data Storage & Processing > **PCI Wizard** > Self-Assessment Questionnaire Form

Congratulations! PCI Wizard successfully completed.  
[Click here to complete the submission process](#)

**Physical Security** Review Q & A

**Security Policies** Close

**Section Completed!**  
You have successfully completed this section and passed.

continue >>

**Almost Finished! You have successfully completed the PCI Wizard.**

Click the "Next" button below to review the PCI Certification form and complete the submission process.

Click "Cancel" to remain on this page.

Cancel Next

Trustwave®  
TrustKeeper™

PCI

messages

TO test account 2

**PCI Manager**    PCI Home    Merchant Profile    Security Policy    Training    Documents    Trusted Commerce

no system notifications    [Contact Support](#)

Start Over    1 Overview    2 Merchant Profile    3 Business Environment    4 Questionnaire

Wizard Option > Card Data Storage & Processing > PCI Wizard > **Self-Assessment Questionnaire Form**

**You have completed the PCI SAQ B 3.2**  
Please click Acknowledge and Submit to complete the form.

### Eligibility

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:

- Merchant uses only an imprint machine to imprint customers' payment card information and does not transmit cardholder data over either a phone line or the Internet; and/or
- Merchant uses only standalone, dial-out terminals (connected via a phone line to your processor); and the standalone, dial-out terminals are not connected to the Internet or any other systems within the merchant environment;  
**NOTE:** The answer in blue is based on your responses to a wizard question. The blue answer is recommended based on your profile..
- Merchant does not transmit cardholder data over a network (either an internal network or the Internet);  
**NOTE:** The answer in blue is based on your responses to a wizard question. Card Data Storage & Processing.
- Merchant does not store cardholder data in electronic format; and  
**NOTE:** The answer in blue is based on your responses to a wizard question. Card Data Storage & Processing.
- If Merchant does store cardholder data, such data is only paper reports or copies of paper receipts and is not received electronically.  
**NOTE:** The answer in blue is based on your responses to a wizard question. Card Data Storage & Processing.

**Based upon your answers, the wizard has completed the actual SAQ form.**

**It is recommended reviewing the SAQ questions by clicking through each section (buttons below). It may be a helpful reminder as you are responsible for adhering to each SAQ question or control 24/7.**

**When you're satisfied, click the "Acknowledge & Submit" to the upper right.**

Save for later    << Previous Section    Next Section >>

### Sections Completed

- Eligibility
- Stored Data Protection
- T
- A
- P
- S

**Acknowledge & Submit** ?

All questions have been answered. Review your answers then submit to complete.

Trustwave TrustKeeper

PCI messages

PCI Manager    PCI Home    Merchant Profile    Scanning    Security Policy    Training    Documents    Trusted Commerce

notification history available

Start Over    1 Overview    2 Merchant Profile    3 Business Environment    4 Questionnaire

Wizard Option > SAQ Selection > Self-Assessment Questionnaire Form

### Confirmation of Compliant Status

Verify Statements:

- PCI DSS Self-Assessment Questionnaire B, Version 3.2 was completed according to the instructions therein.
- All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
- I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization. **All credit card terminals through Treasury do not store this data**
- I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times. ([https://www.pcisecuritystandards.org/security\\_standards/documents.php](https://www.pcisecuritystandards.org/security_standards/documents.php))
- If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.
- No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.

1. Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.  
2. The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.  
3. Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

### Merchant Acknowledgement

Remember that this questionnaire is completed annually, but the merchant contact is responsible for ensuring PCI compliance is adhered to at all times!

Merchant Company: TO test acct a wiz

Sign:  I am hereby signing and intend to authenticate this document.

Title:

Merchant Executive Officer:

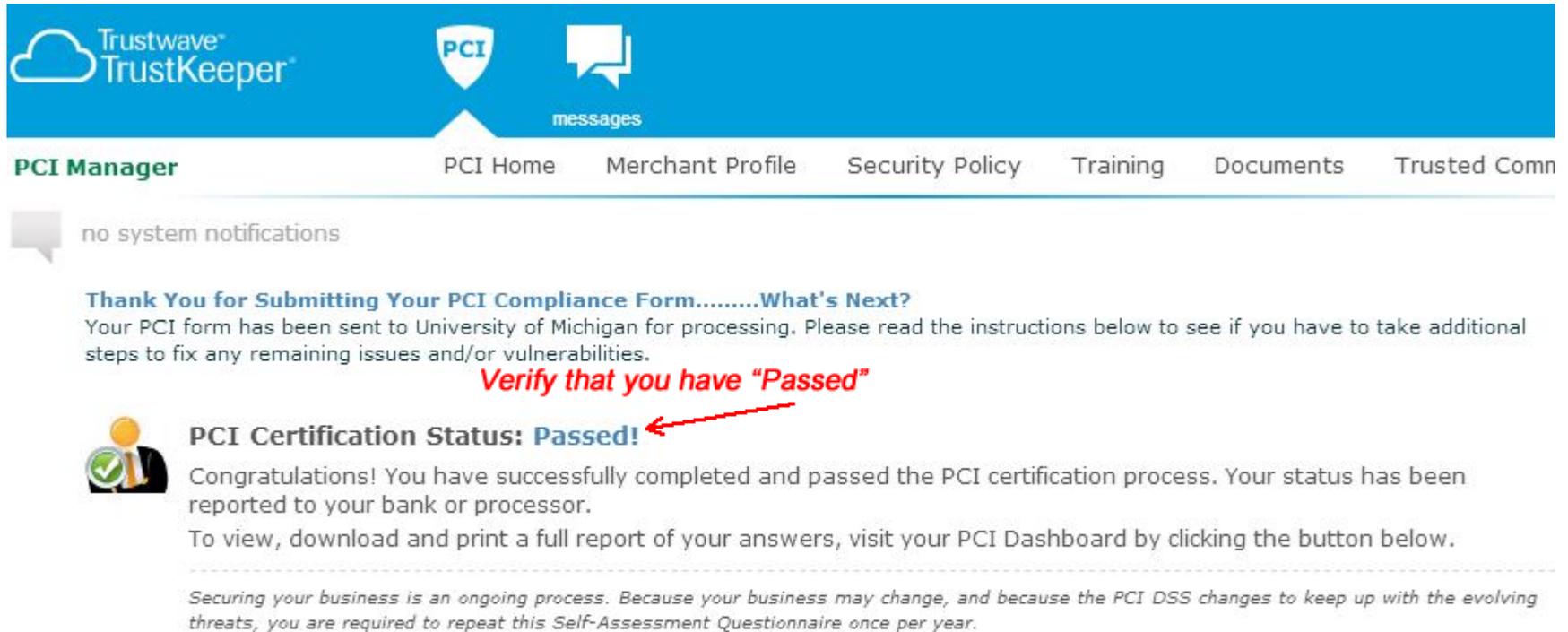
Today's Date: 12/02/14

Copies of this SAQ will be made available to the Department Budget Administrator, Treasurer's Office, Internal Controls and Audits.

<< Cancel    Submit

Screen 36

If you did not pass, the screen should indicate which question(s) were incorrect. If you simply answered incorrectly, go back and change your answer. If you answered incorrectly due to how you process credit cards, you will need to change your method(s) prior to correcting your answer.



The screenshot shows the Trustwave PCI Manager dashboard. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation bar with links for PCI Home, Merchant Profile, Security Policy, Training, Documents, and Trusted Comm. A notification area shows 'no system notifications'. The main content area features a heading 'Thank You for Submitting Your PCI Compliance Form.....What's Next?' followed by instructions. A red arrow points to the text 'Verify that you have "Passed"'. Below this, a person icon with a checkmark is next to the text 'PCI Certification Status: Passed!'. Further instructions and a disclaimer are provided at the bottom of the main content area.

Trustwave<sup>®</sup>  
TrustKeeper<sup>™</sup>

PCI

messages

**PCI Manager**      PCI Home    Merchant Profile    Security Policy    Training    Documents    Trusted Comm

no system notifications

**Thank You for Submitting Your PCI Compliance Form.....What's Next?**  
Your PCI form has been sent to University of Michigan for processing. Please read the instructions below to see if you have to take additional steps to fix any remaining issues and/or vulnerabilities.

**Verify that you have "Passed"**

**PCI Certification Status: Passed!**

Congratulations! You have successfully completed and passed the PCI certification process. Your status has been reported to your bank or processor.  
To view, download and print a full report of your answers, visit your PCI Dashboard by clicking the button below.

*Securing your business is an ongoing process. Because your business may change, and because the PCI DSS changes to keep up with the evolving threats, you are required to repeat this Self-Assessment Questionnaire once per year.*



The screenshot displays the Trustwave TrustKeeper PCI Manager interface. At the top, there is a blue navigation bar with the TrustKeeper logo, a PCI shield icon, a messages icon, and a gear icon. Below this is a secondary navigation bar with tabs for 'PCI Home', 'Merchant Profile', 'Security Policy', 'Training', 'Documents', and 'Trusted Commerce'. A notification banner indicates 'notification history available' and a 'Contact Support' button is visible on the right.

The main content area is titled 'PCI Certification Status'. Underneath, there is a section for 'PCI Self-Assessment' with two tabs: 'Summary' and 'History & Documents'. The 'History & Documents' tab is active, showing a table with one entry:

PCI SAQ B 3.2	2014-11-24	✓	SAQ.pdf

Red annotations highlight three steps: 'Step 1 Click here' points to the 'History & Documents' tab; 'Step 2 Click here to save a copy of your completed SAQ.' points to the 'SAQ.pdf' link; and 'Step 3 Click here to save a copy of your completion certification.' points to a 'Click Here' link in the 'Certificate of Compliance' section on the right. A 'Start' button is also visible.

Below the table, the 'PCI Status' section shows 'Next Certification Deadline: 2015-11-24' with a green checkmark. To the right, a 'pass' status is shown above a large blue message: **CONGRATS! You're done with the annual SAQ.**

Remember the PCI compliance SAQ is done annually but *being PCI compliance is done 24/7 365 days.*

Contact UM Treasury [merchantservices@umich.edu](mailto:merchantservices@umich.edu) with any questions.