FINANCE
TREASURER'S OFFICE
UNIVERSITY OF MICHIGAN

Rev 9/16/2016

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.

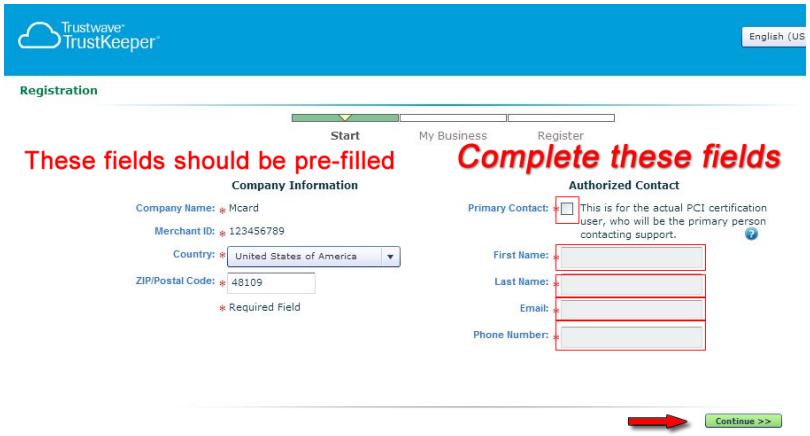
You should see one of the two screens below. If your *merchant account is new*, you should see the screen to left. If you are *renewing the SAQ* for this year, you should see the screen to the right or Screen 3 (two pages below).

Screen 1 – SAQ for a brand new merchant account

Registration

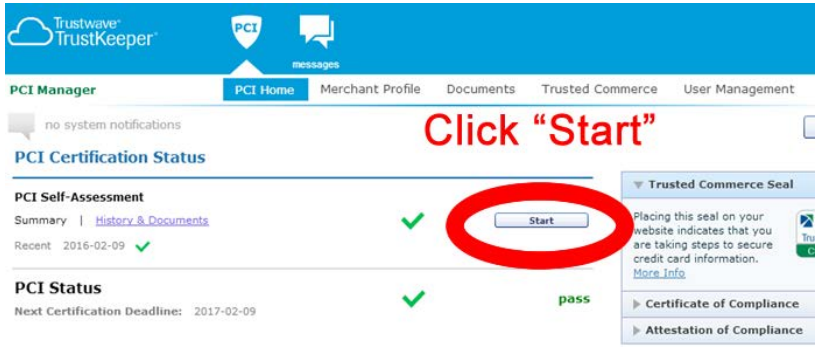
You will arrive at the Trustwave website from the Trustwave email invitation link. Registration is a one-time occurrence for the merchant account. Look for **red text** for UM Treasury guidance. **Red** outlined boxes require entry.

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



Screen 1 – Renewing the annual SAQ

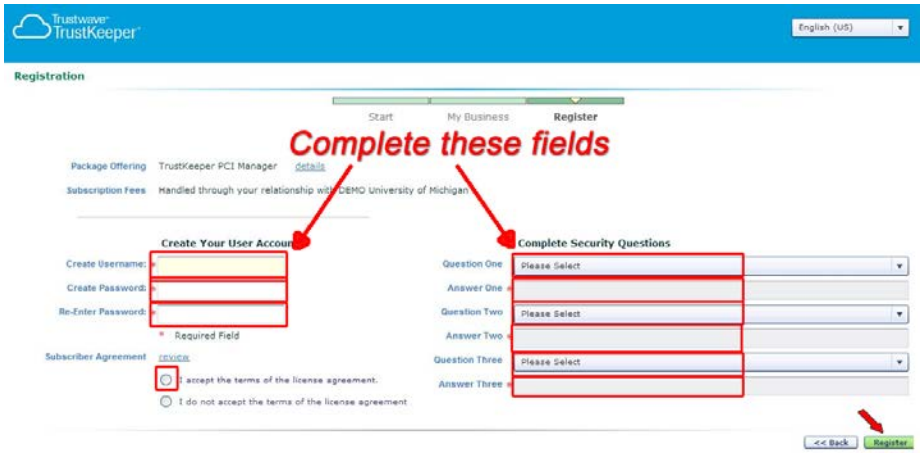
After logging in, you'll see the "PCI Home" screen. Simply click "Start" to begin.



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"



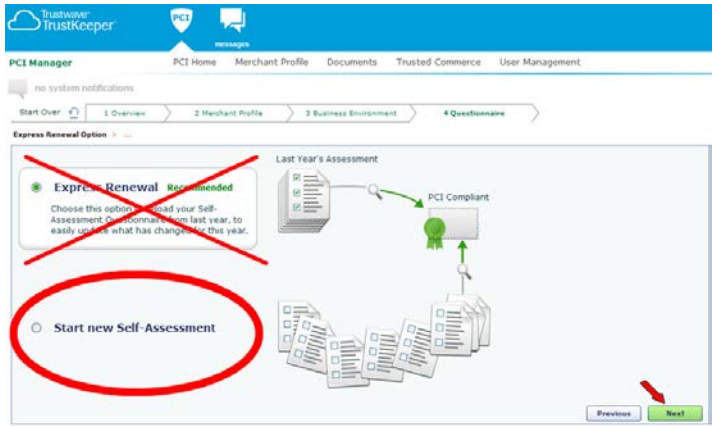
Screen 2 – Renewing the annual SAQ

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

If you see the screen just below,

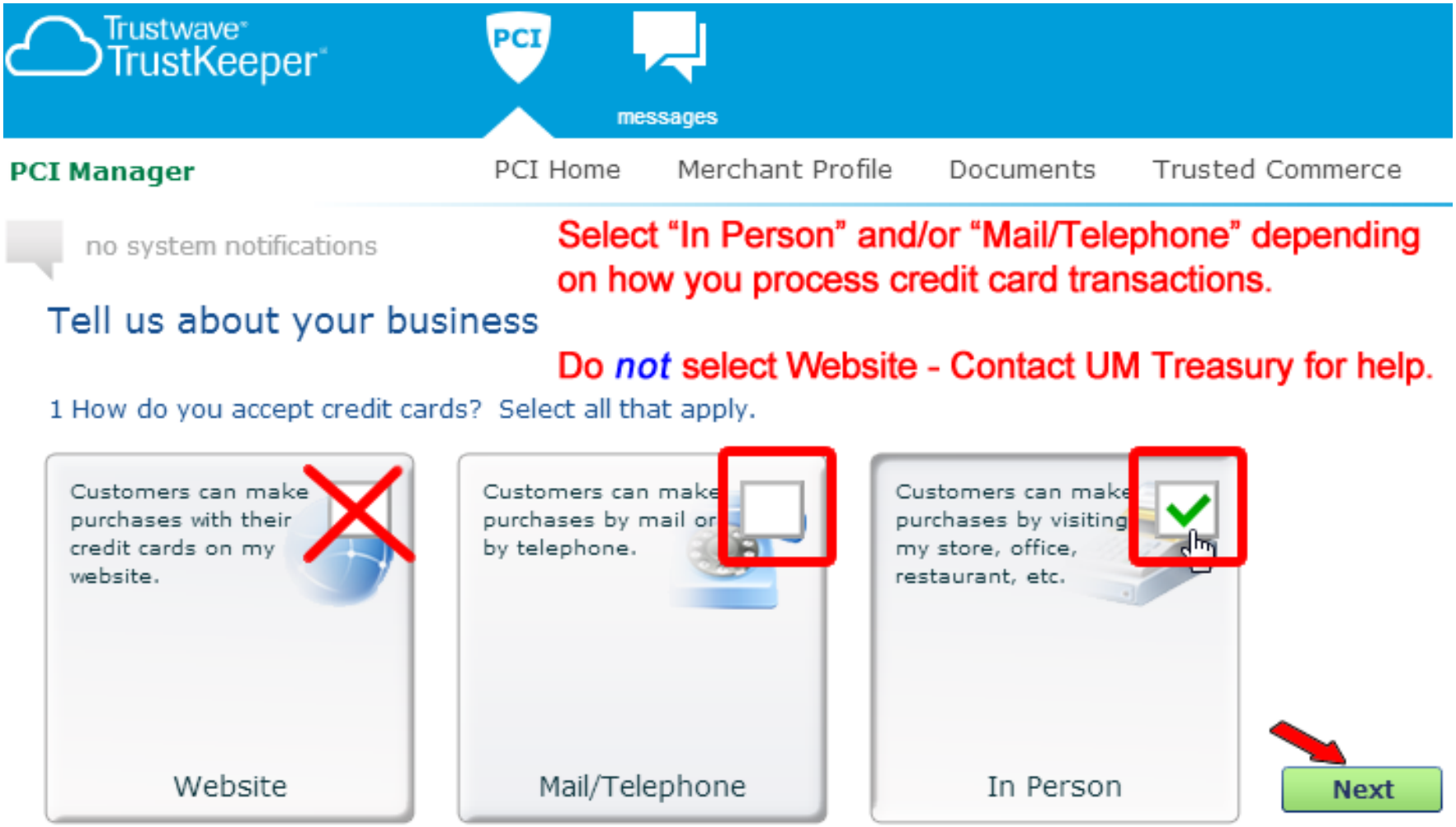
Do ***NOT*** select "Express Renewal."*
Select "Start new Self-Assessment."
Then click "Next" to begin.

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

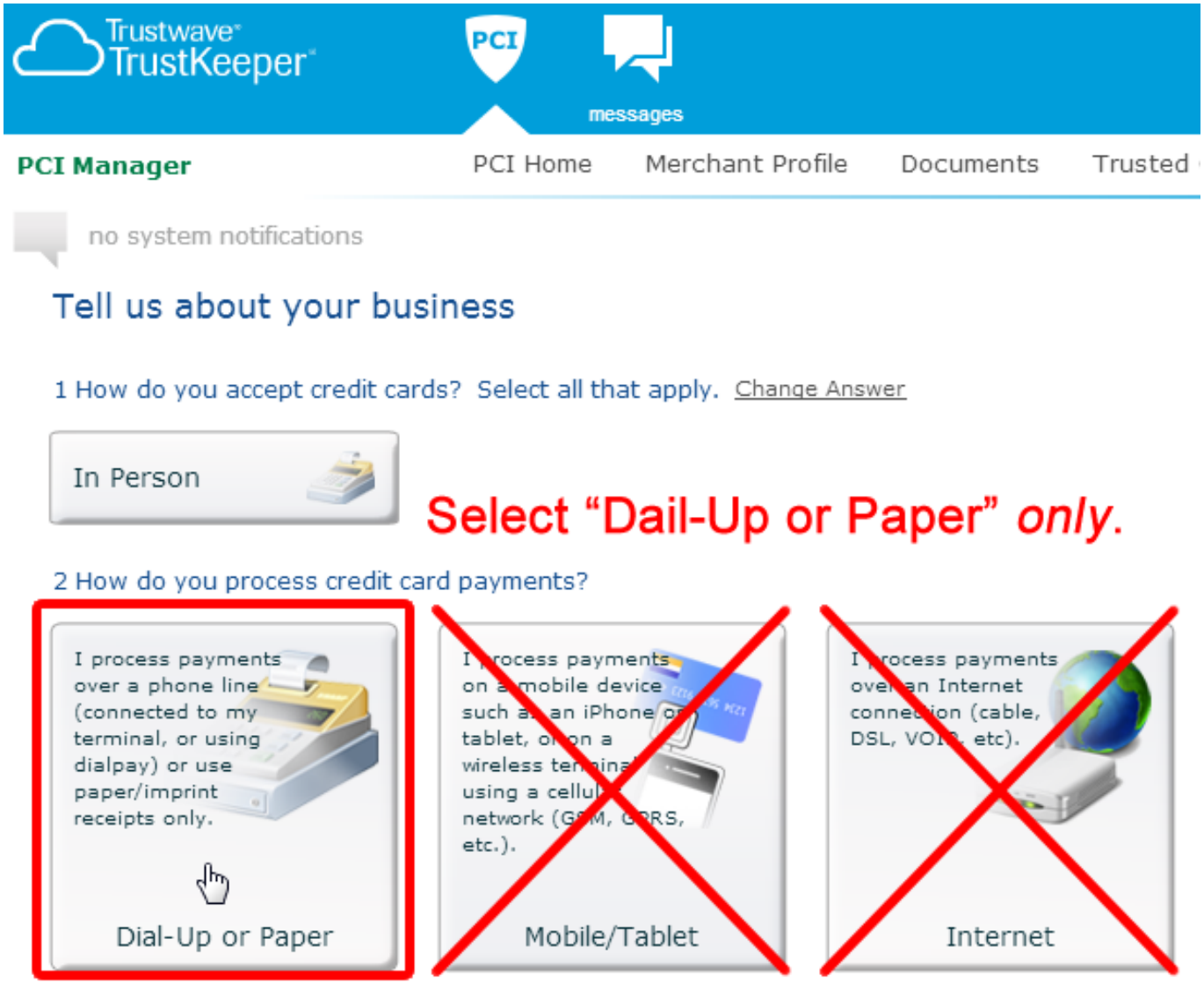


Account Profile

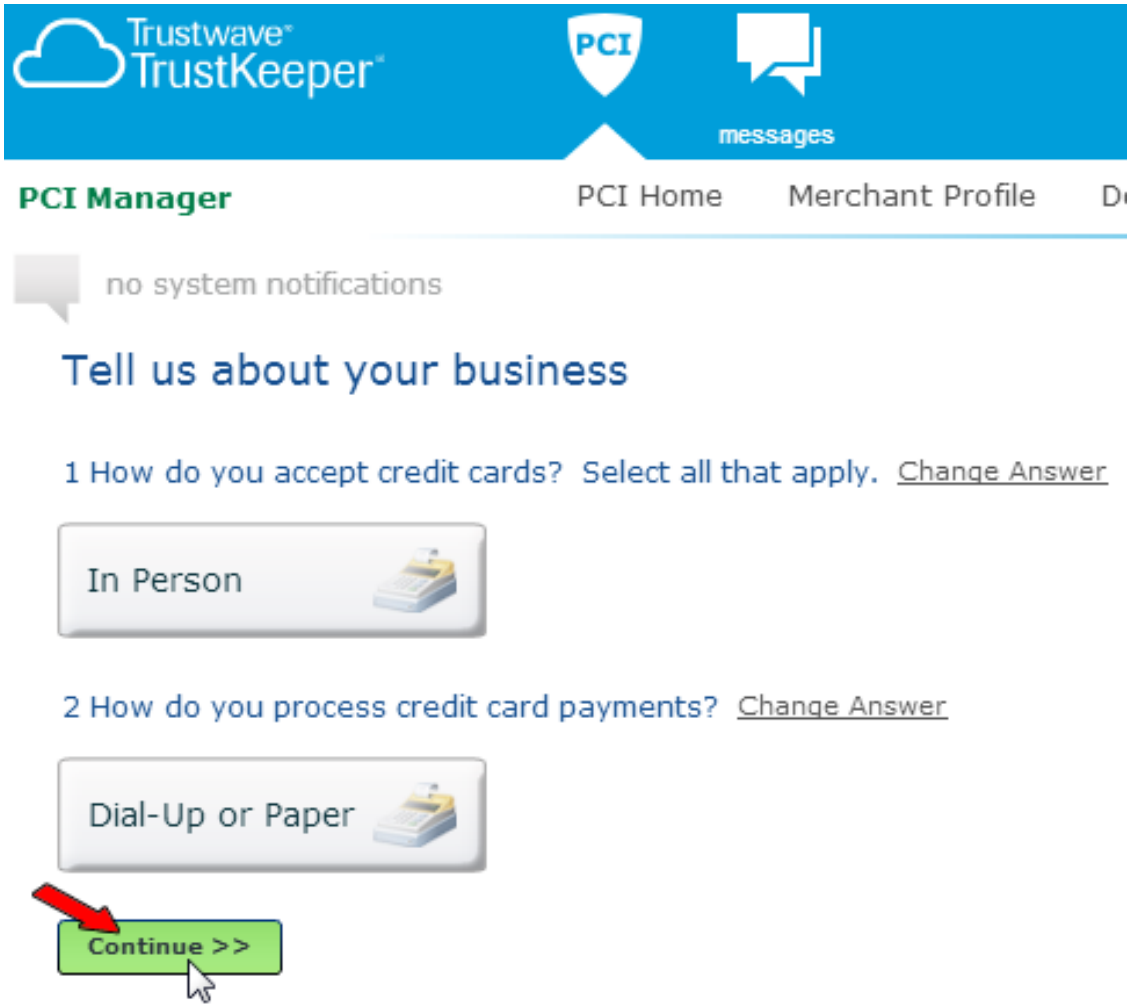
Screen 3



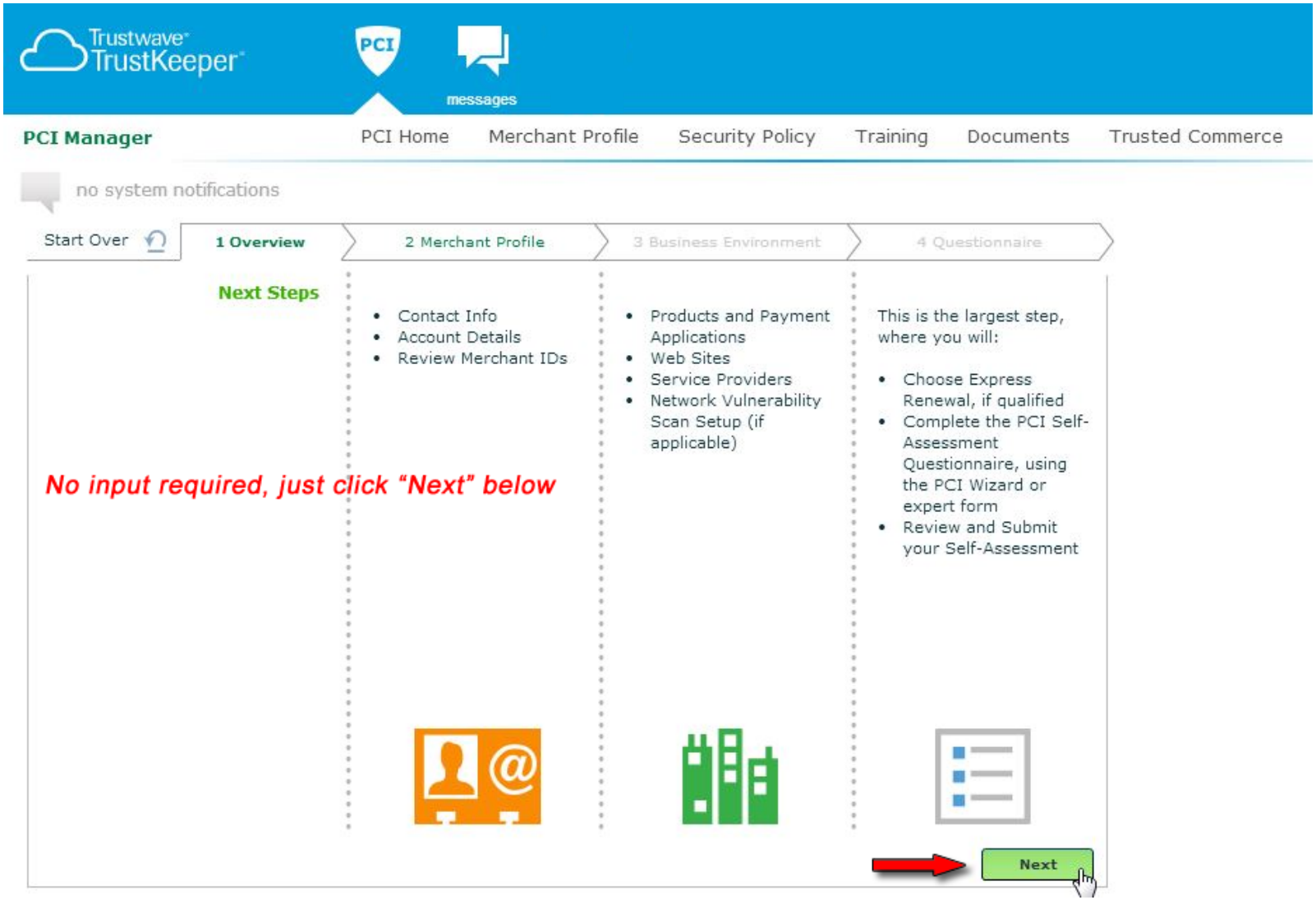
Screen 4


Trustwave TrustKeeper
PCI
messages
PCI Manager
PCI Home
Merchant Profile
Documents
Trusted
no system notifications
Tell us about your business
1 How do you accept credit cards? Select all that apply. Change Answer
In Person
Select "Dail-Up or Paper" only.
2 How do you process credit card payments?
I process payments over a phone line (connected to my terminal, or using dialpay) or use paper/imprint receipts only.
Dial-Up or Paper
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.).
Mobile/Tablet
I process payments over an Internet connection (cable, DSL, VOIP, etc).
Internet

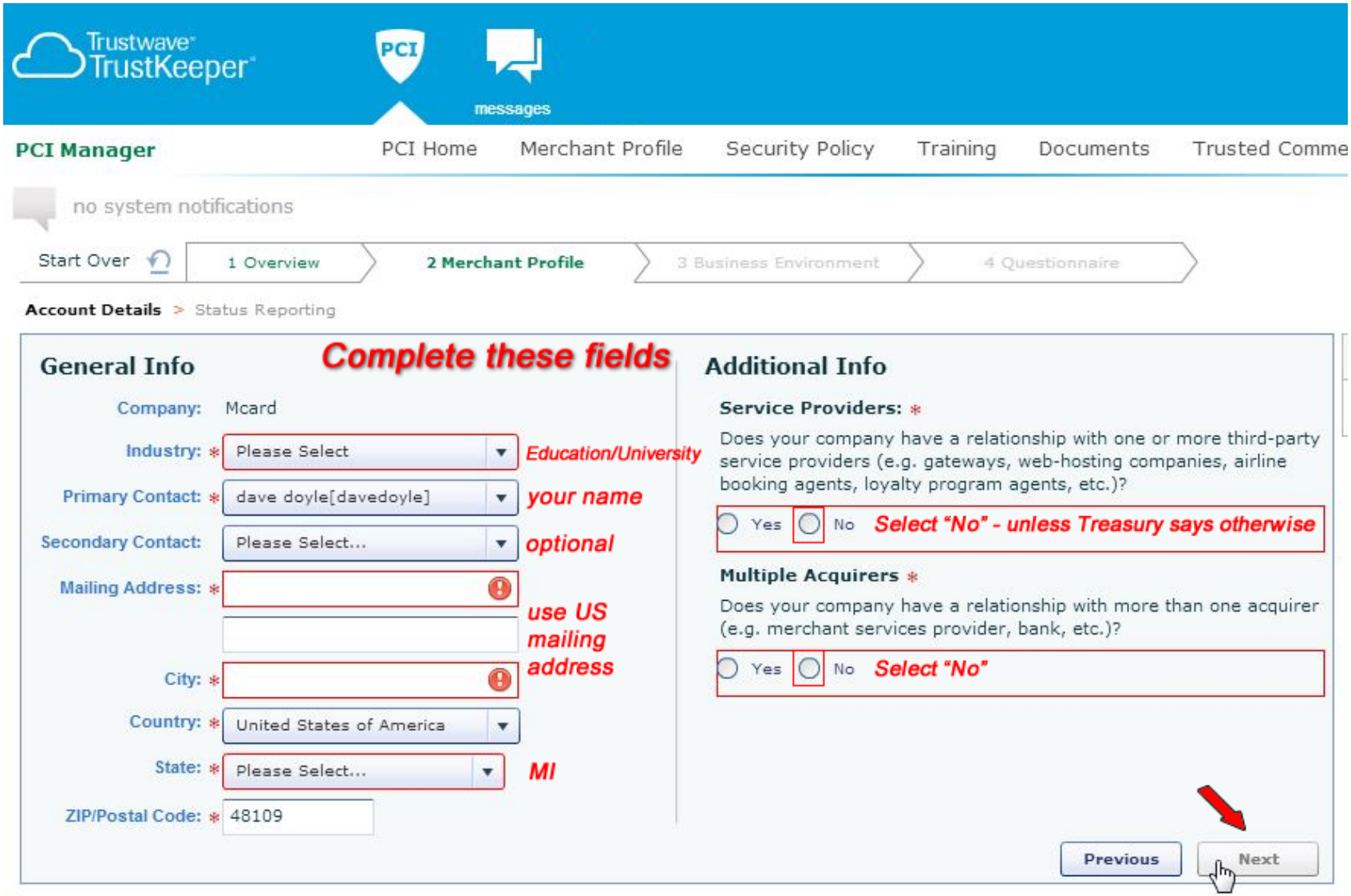
Screen 5


Trustwave
TrustKeeper
PCI
messages
PCI Manager
PCI Home
Merchant Profile
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 >>

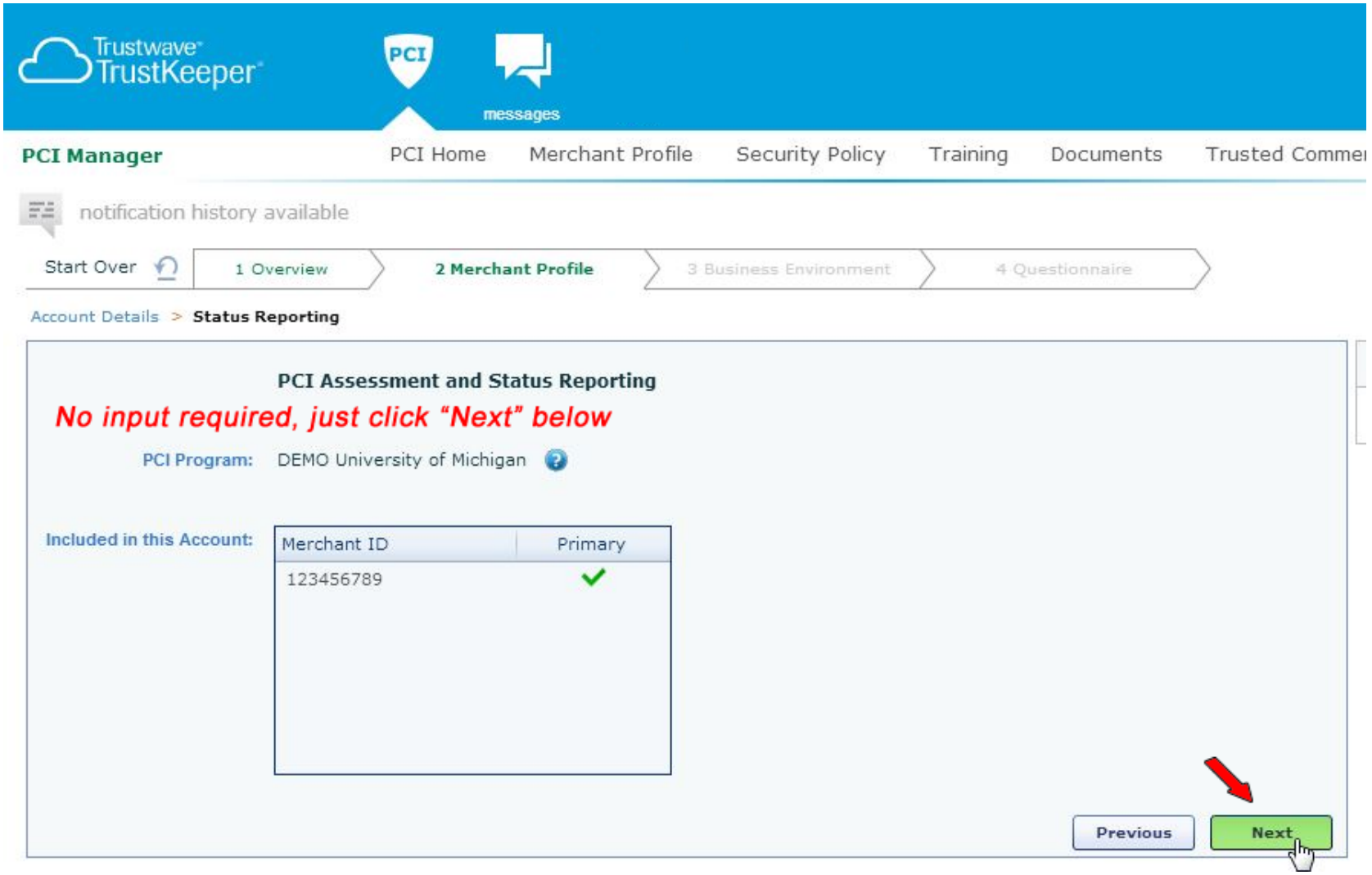
Screen 6


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
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
No input required, just click "Next" below
Next

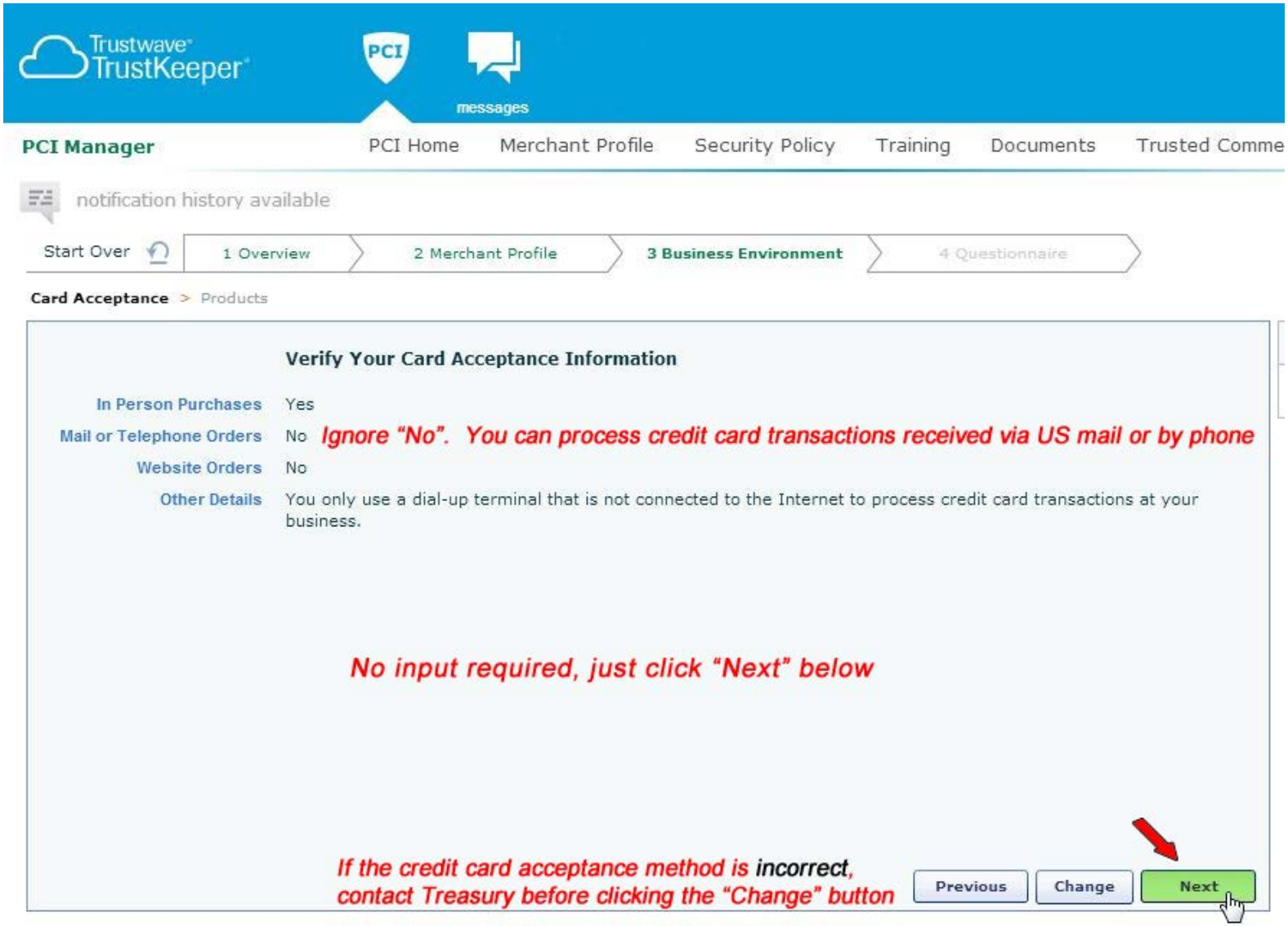
Screen 7


Trustwave TrustKeeper
PCI
messages
PCI Manager
PCI Home
Merchant Profile
Security Policy
Training
Documents
Trusted Comme
no system notifications
Start Over
1 Overview
2 Merchant Profile
3 Business Environment
4 Questionnaire
Account Details > Status Reporting
General Info
Complete these fields
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: *
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"
Previous
Next

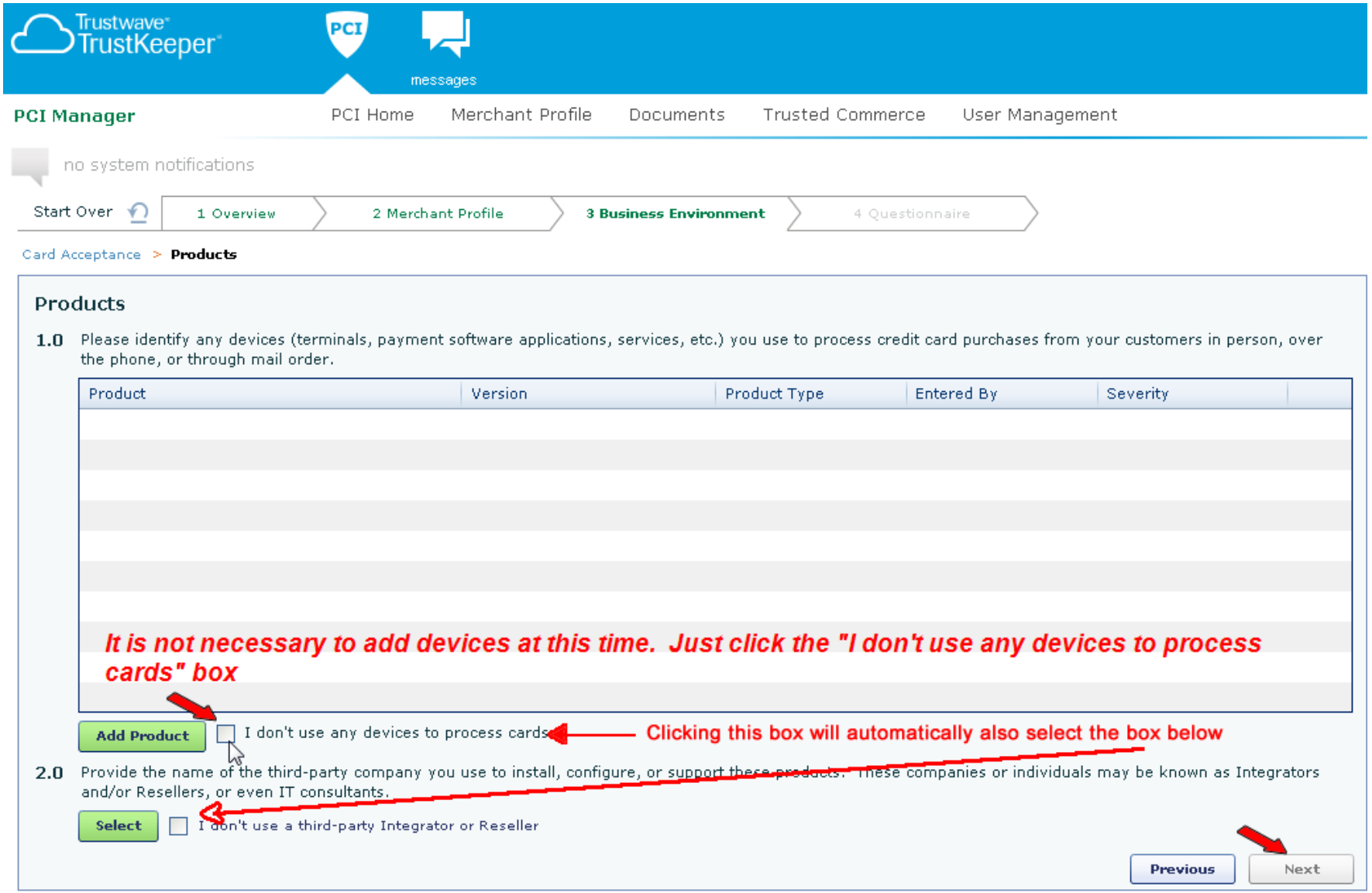
Screen 8


Trustwave TrustKeeper
PCI
messages
PCI Manager
PCI Home
Merchant Profile
Security Policy
Training
Documents
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

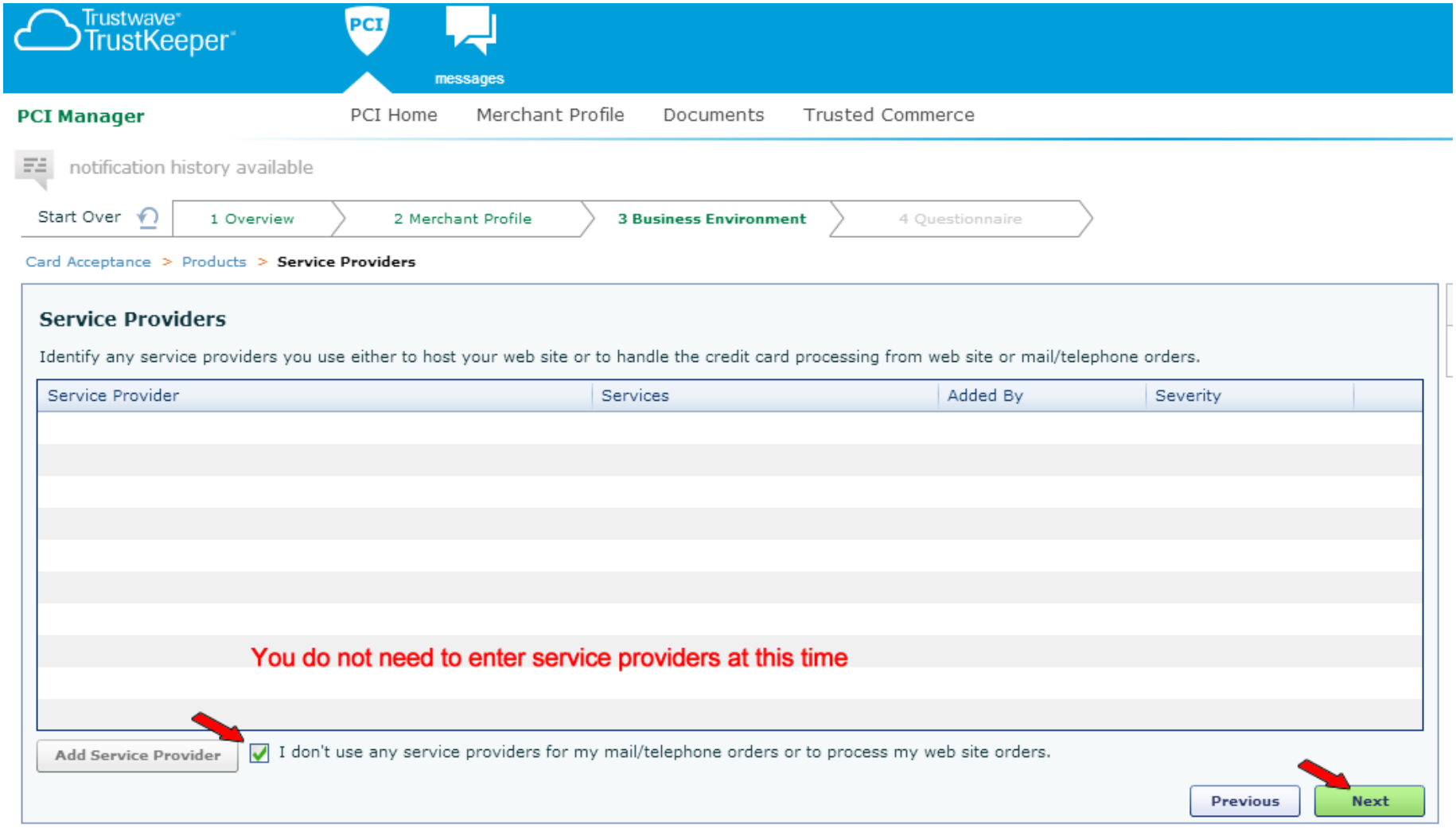

Trustwave TrustKeeper
PCI
messages
PCI Manager
PCI Home
Merchant Profile
Security Policy
Training
Documents
Trusted Comme
notification history available
Start Over
1 Overview
2 Merchant Profile
3 Business Environment
4 Questionnaire
Card Acceptance > Products
Verify Your Card Acceptance Information
In Person Purchases
Yes
Mail or Telephone Orders
No
Ignore "No". You can process credit card transactions received via US mail or by phone
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 TrustKeeper
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
Clicking this box will automatically also select the box below
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

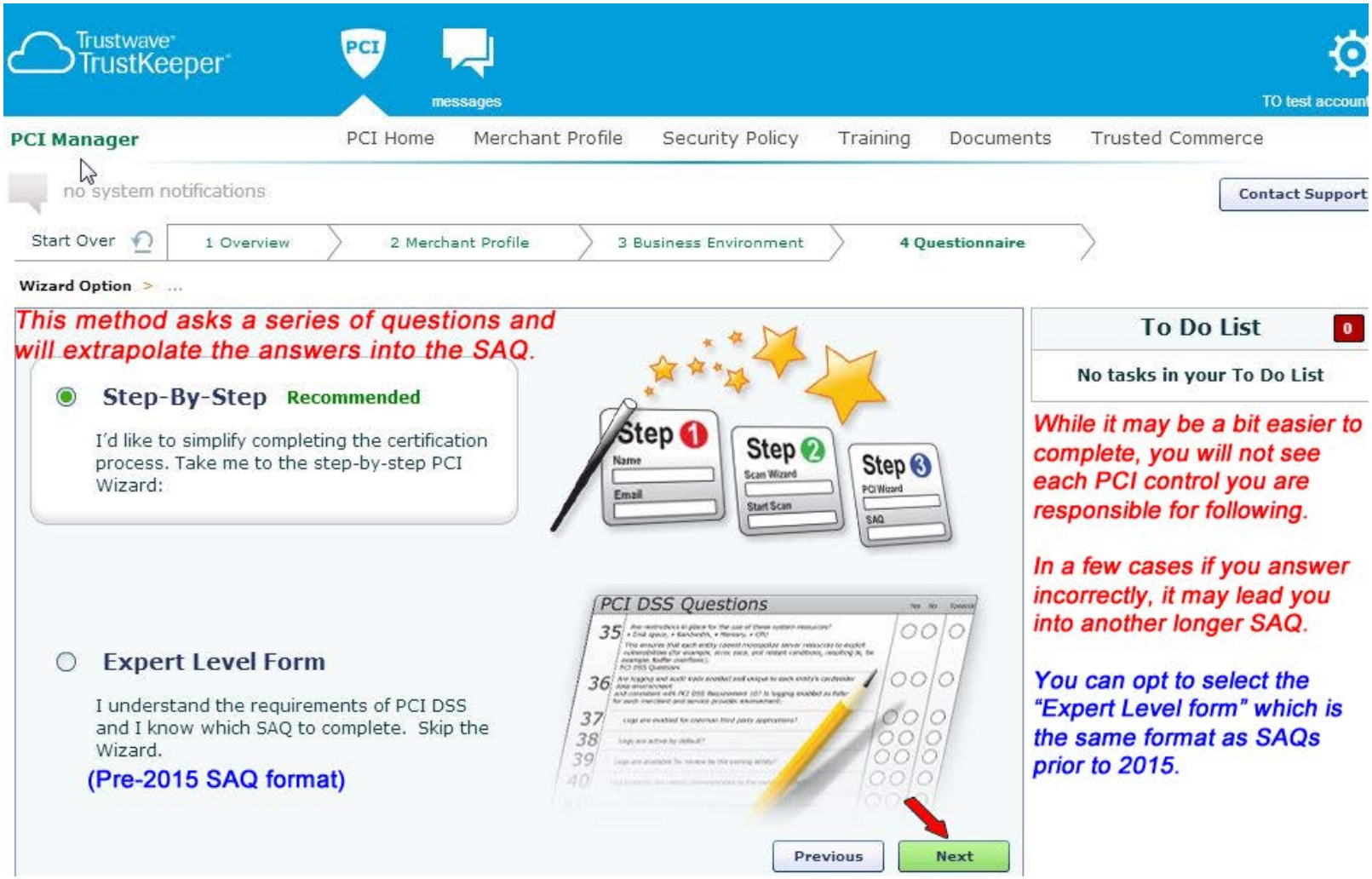
This screen may appear if you previously had indicated that you process Mail Order/Telephone Order credit card transactions.

Screen 11



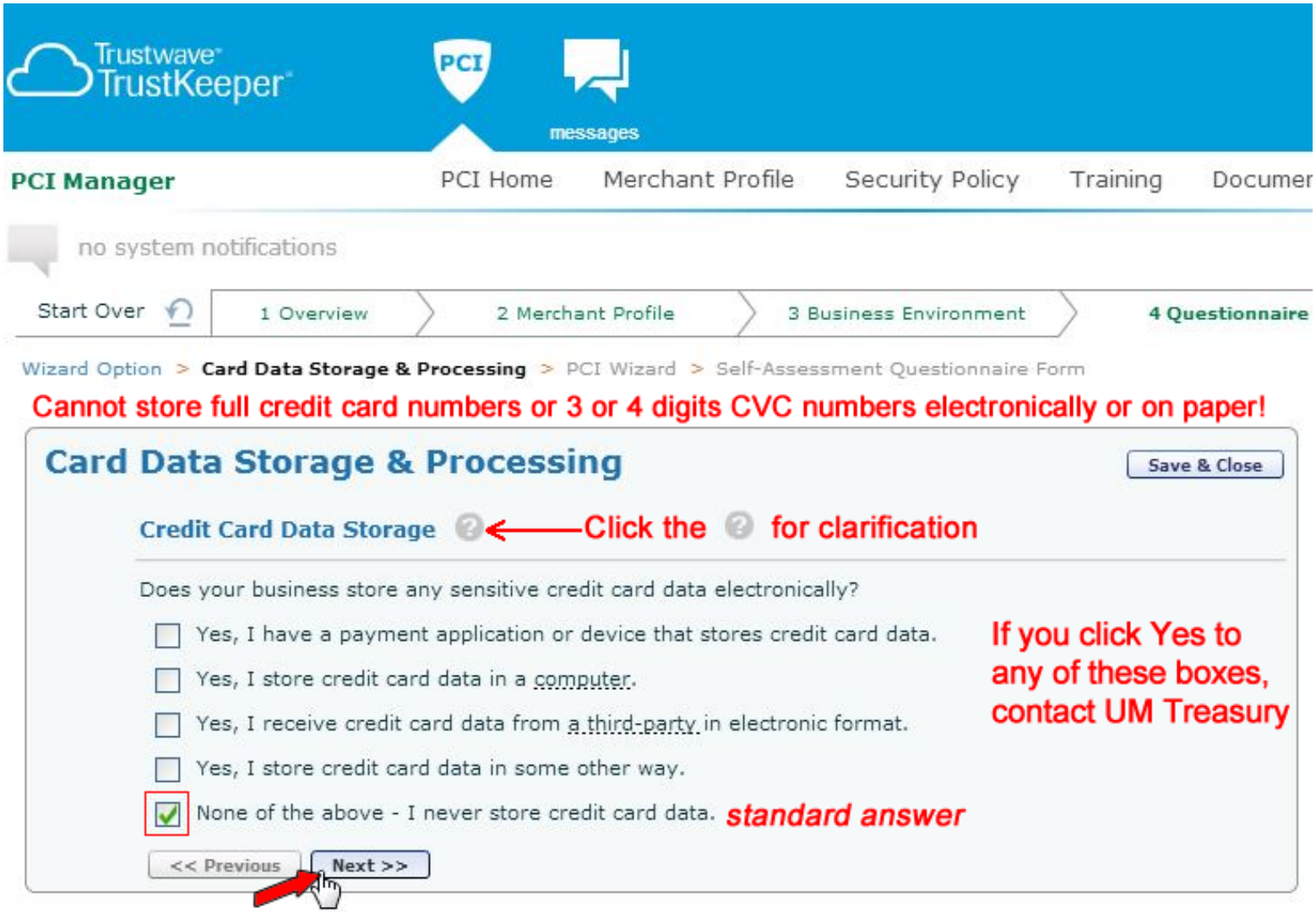
SAQ Completion Selection (It's possible that a different screen appears regarding '***Express Renewal***,' instead select '***Start a new Self-Assessment***' – see page 2 right column)

Screen 12

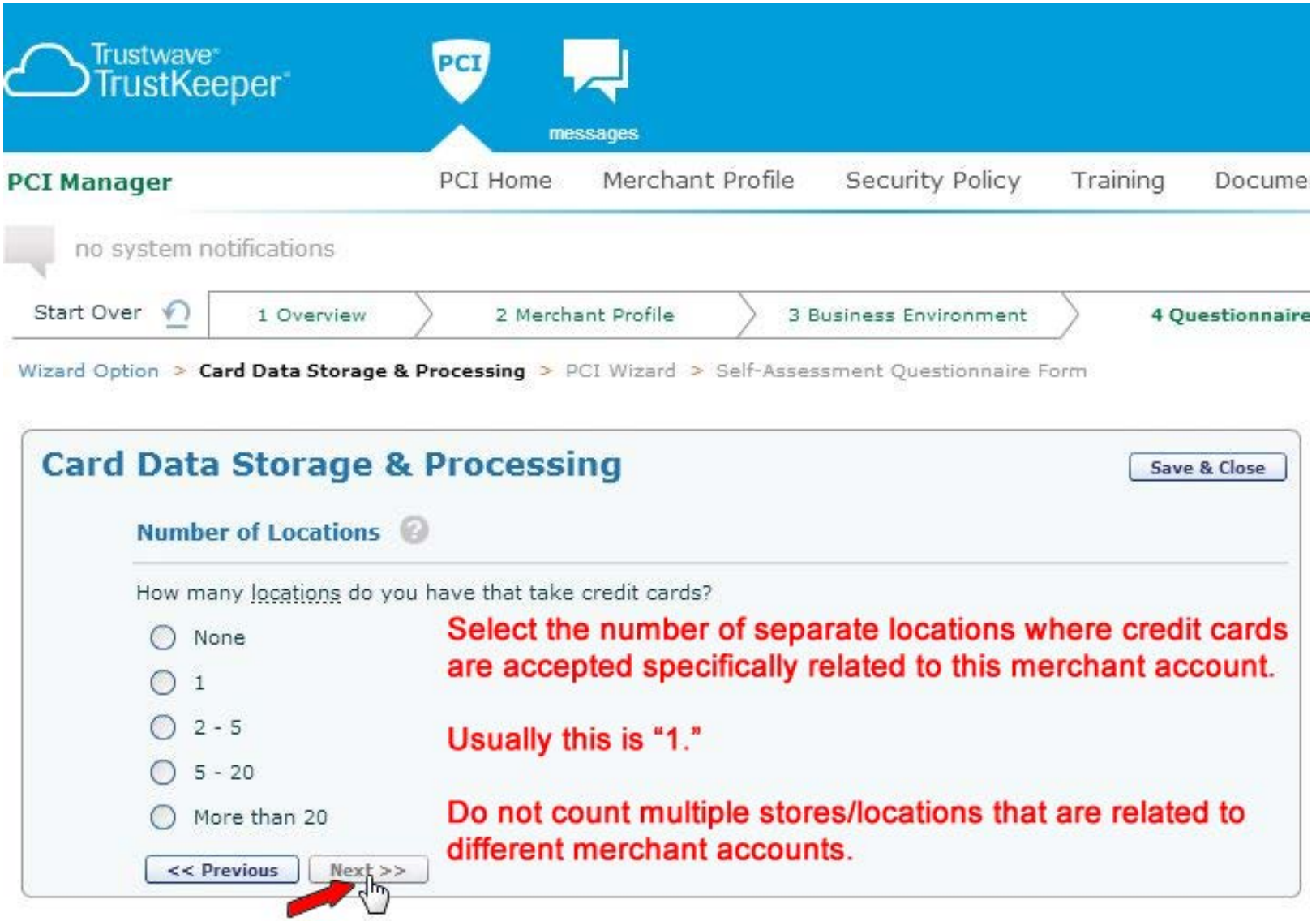


Screen 13

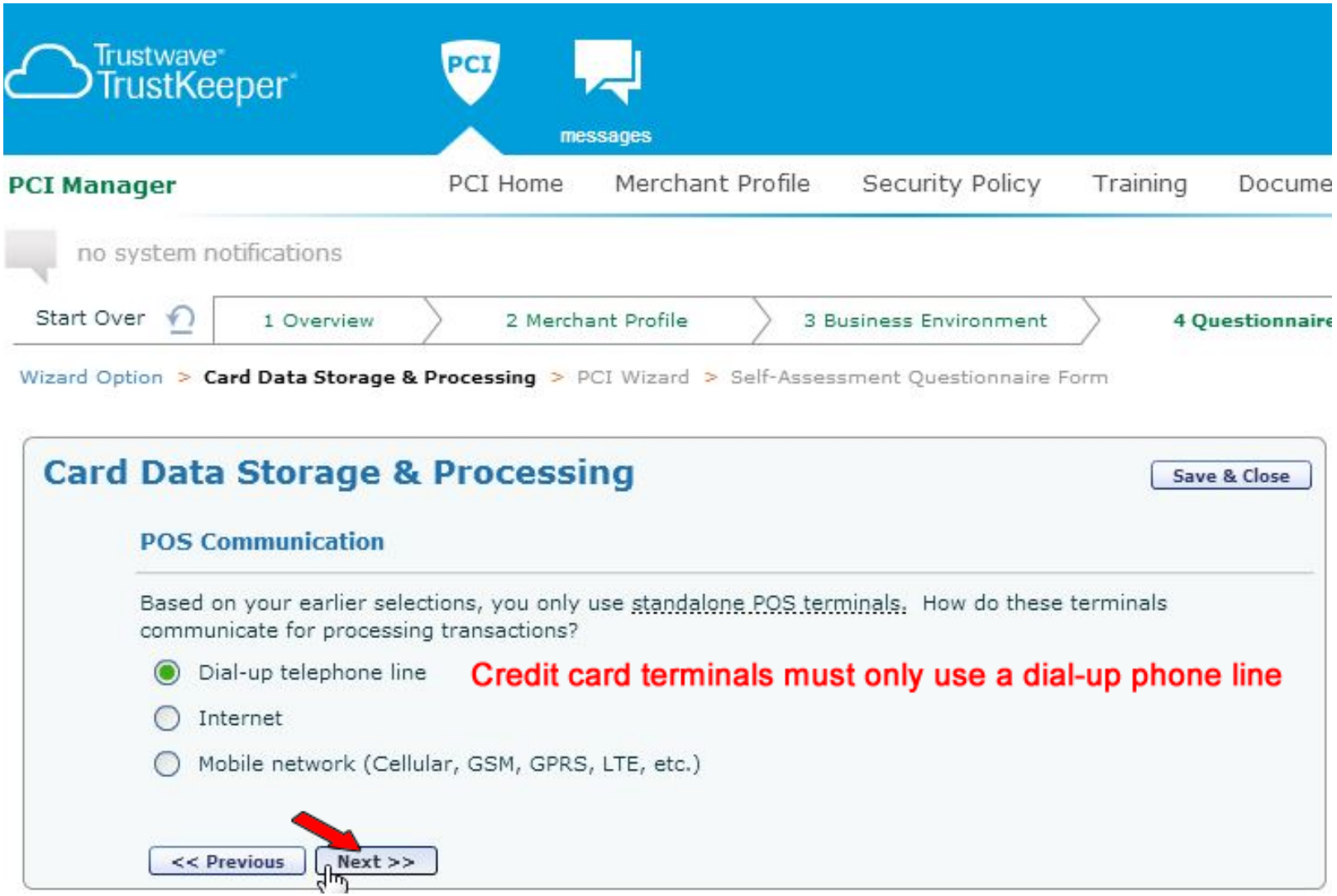
Note: you can click on the circled question mark or "i" for additional info/clarification.



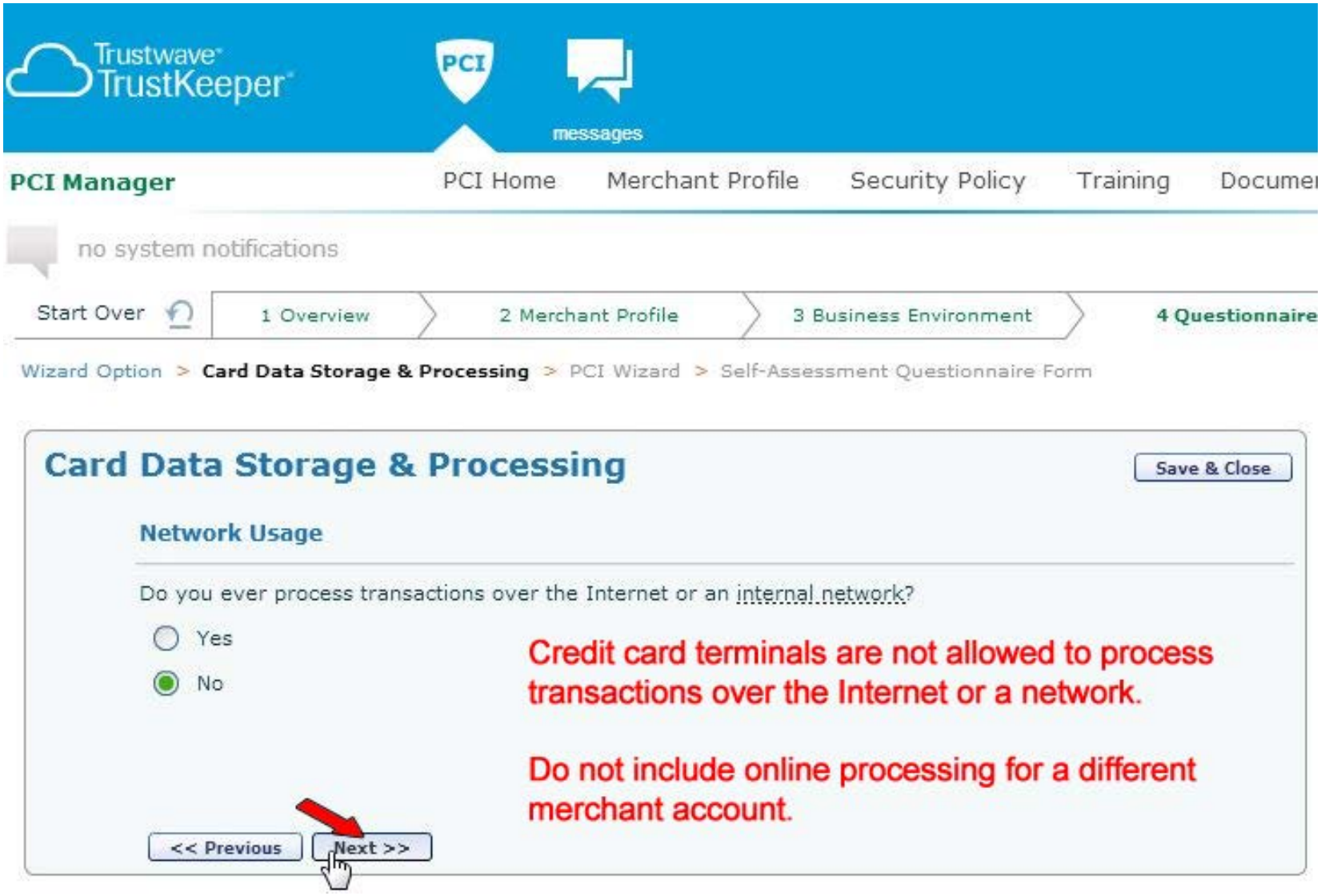
Screen 14


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
Card Data Storage & Processing
Save & Close
Number of Locations
How many locations do you have that take credit cards?
None
1
2 - 5
5 - 20
More than 20
<< Previous
Next >>
Select the number of separate locations where credit cards are accepted specifically related to this merchant account.
Usually this is "1."
Do not count multiple stores/locations that are related to different merchant accounts.

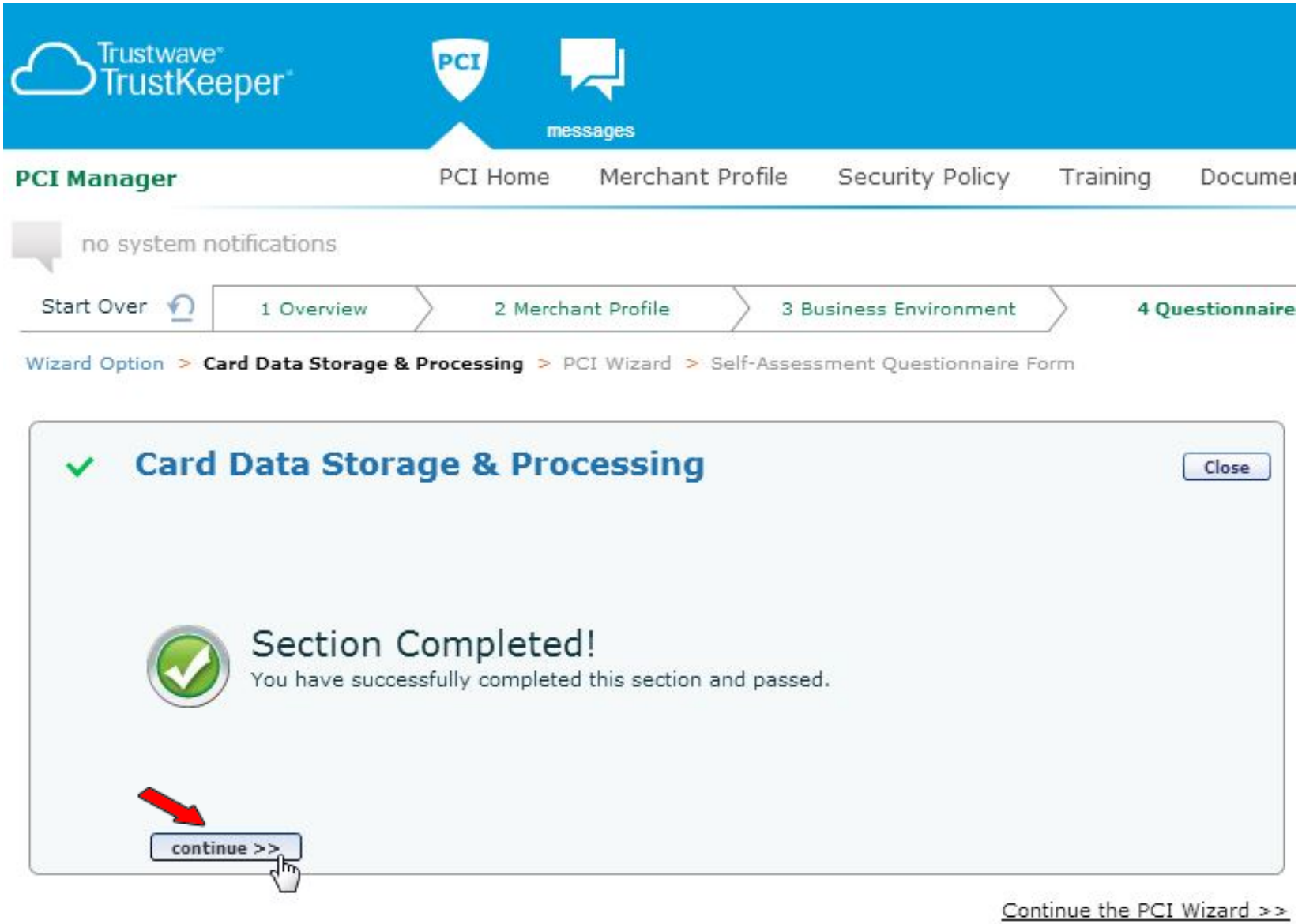
Screen 15


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
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


Trustwave TrustKeeper
PCI
messages
PCI Manager
PCI Home
Merchant Profile
Security Policy
Training
Documer
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
Card Data Storage & Processing
Save & Close
Network Usage
Do you ever process transactions over the Internet or an internal network?
Yes
No
Credit card terminals are not allowed to process transactions over the Internet or a network.
Do not include online processing for a different merchant account.
<< Previous
Next >>

Screen 17

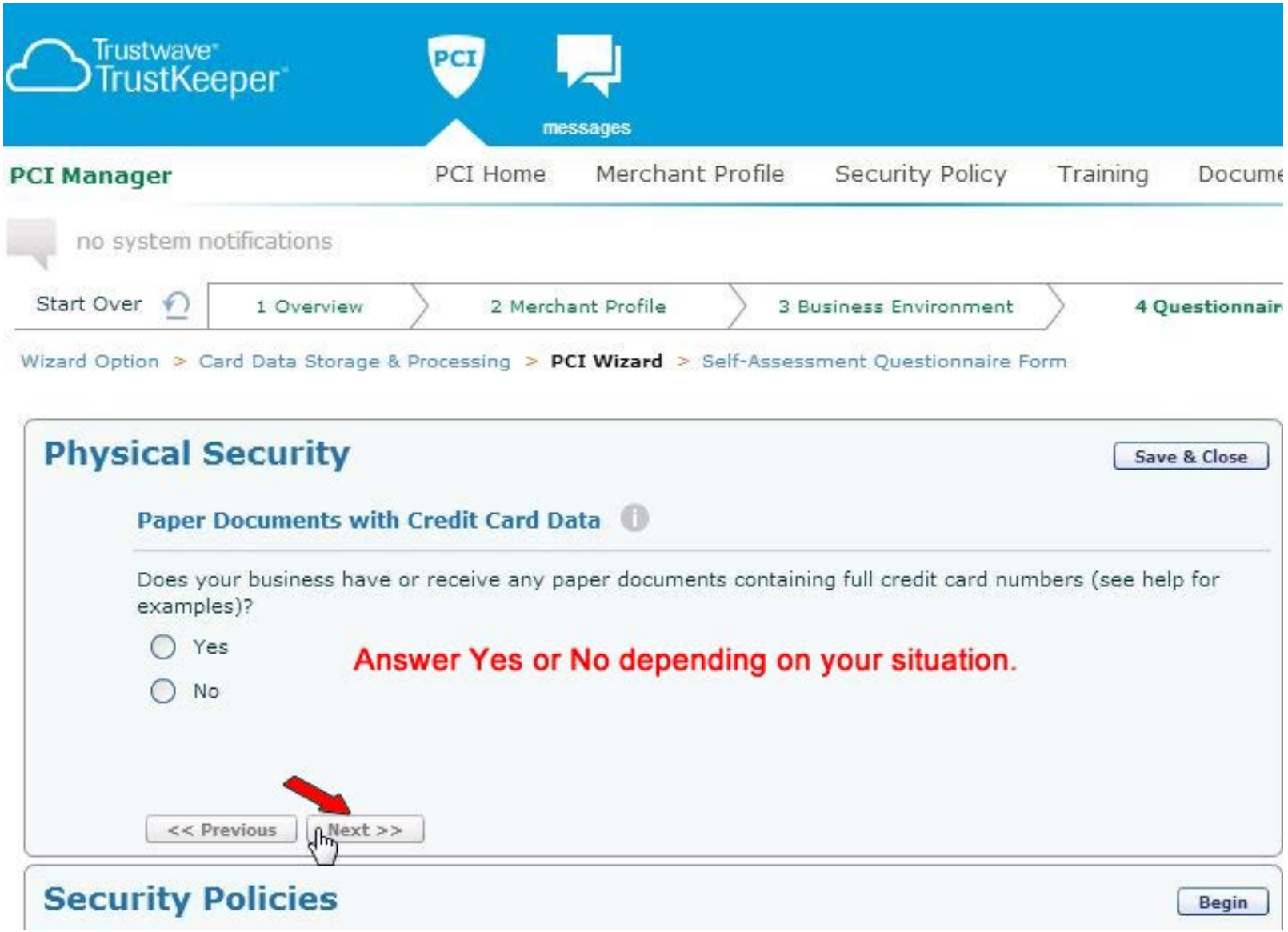


Continue the PCI Wizard >>

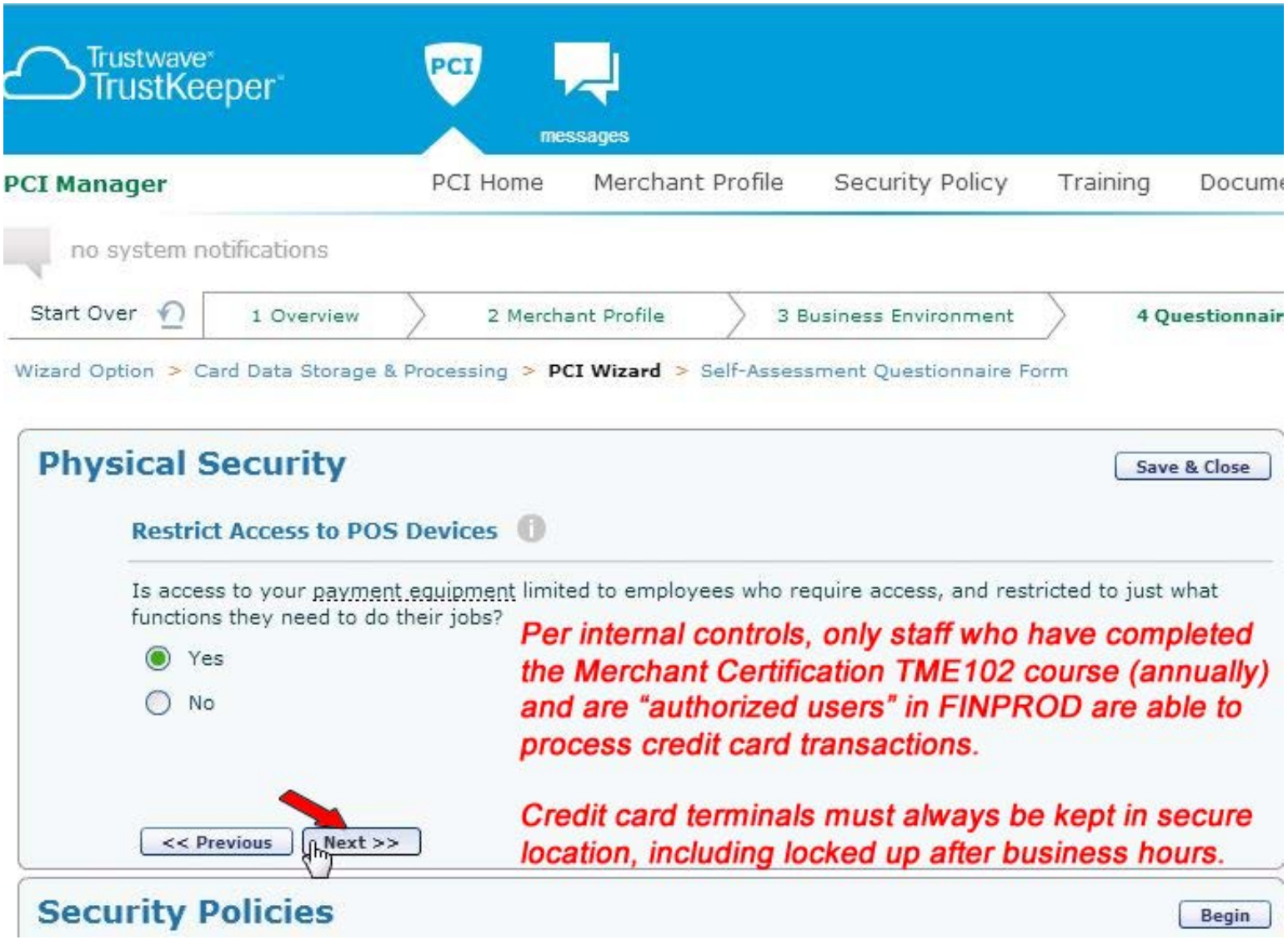
Screen 18


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
Begin
Security Policies
Begin

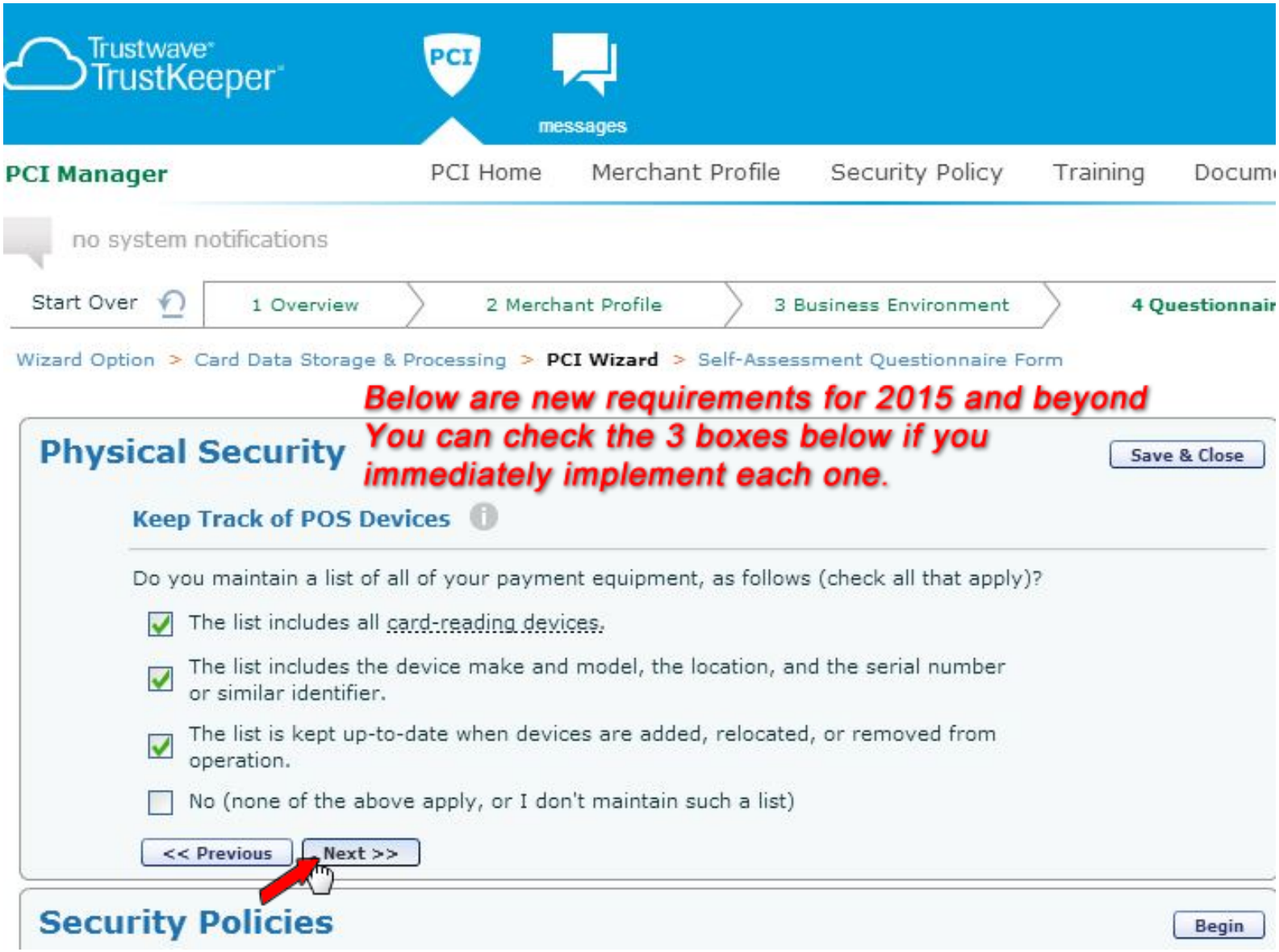
Screen 19


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 Questionnair
Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form
Physical Security
Save & Close
Paper Documents with Credit Card Data
Does your business have or receive any paper documents containing full credit card numbers (see help for examples)?
Yes
No
Answer Yes or No depending on your situation.
<< Previous
Next >>
Security Policies
Begin

Screen 20


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 Questionnair
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 >>
Security Policies
Begin

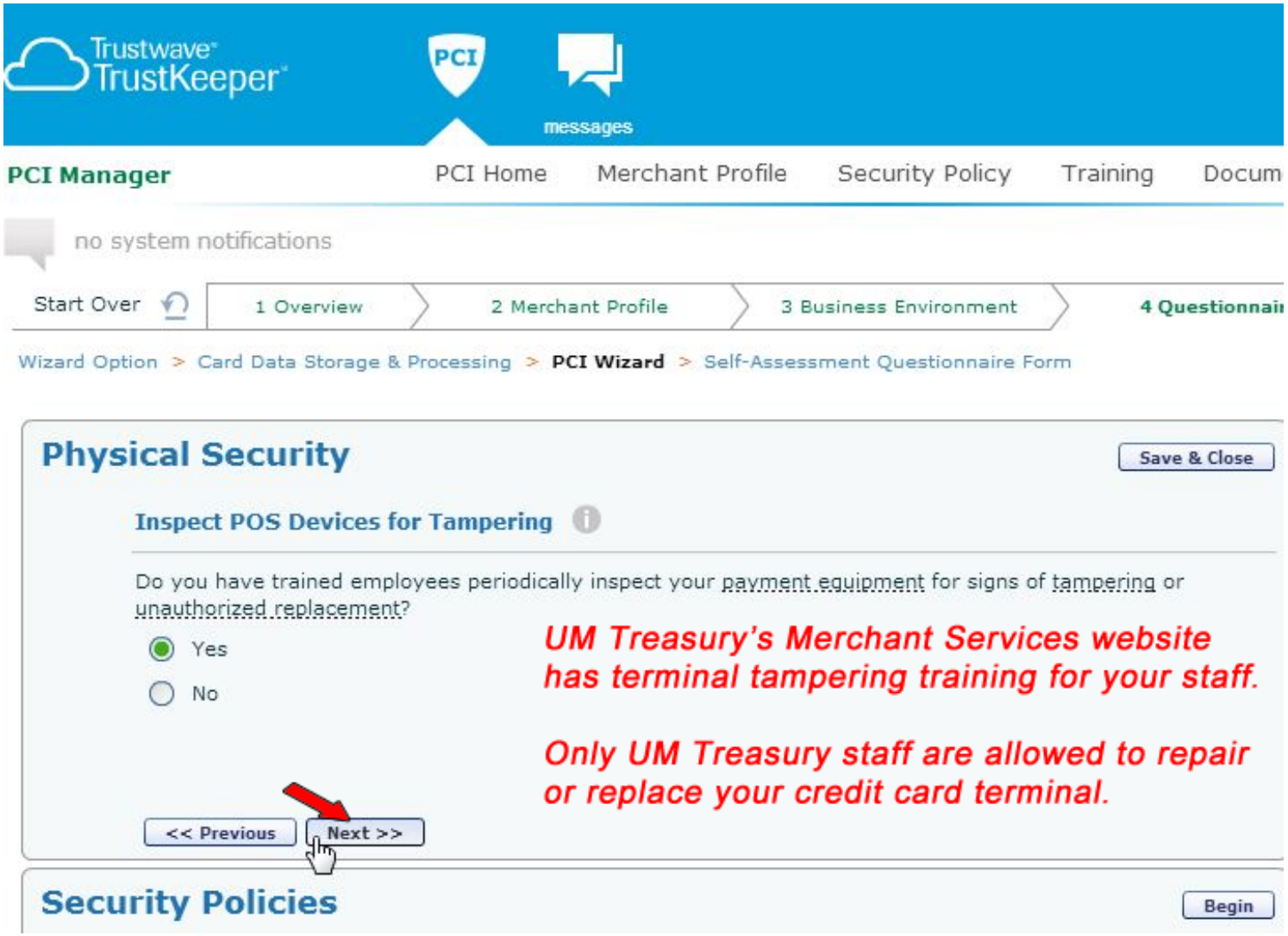
Screen 21


Trustwave TrustKeeper
PCI
messages
PCI Manager
PCI Home
Merchant Profile
Security Policy
Training
Docum
no system notifications
Start Over
1 Overview
2 Merchant Profile
3 Business Environment
4 Questionnair
Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form
Below are new requirements for 2015 and beyond
You can check the 3 boxes below if you immediately implement each one.
Physical Security
Save & Close
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

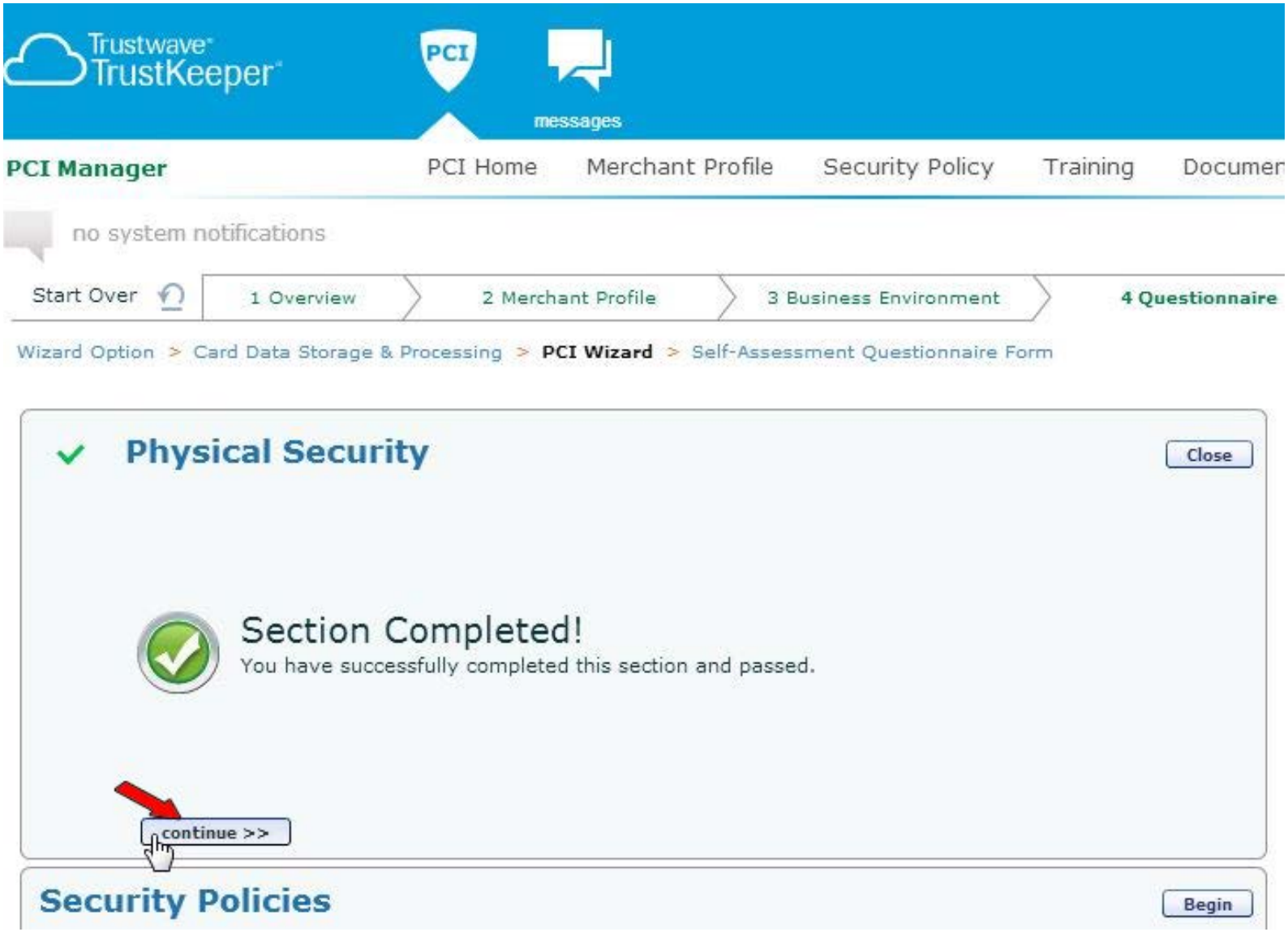
Screen 22

Remember that credit card terminals must be secured from unauthorized individuals, which includes locking up the device after business hours.

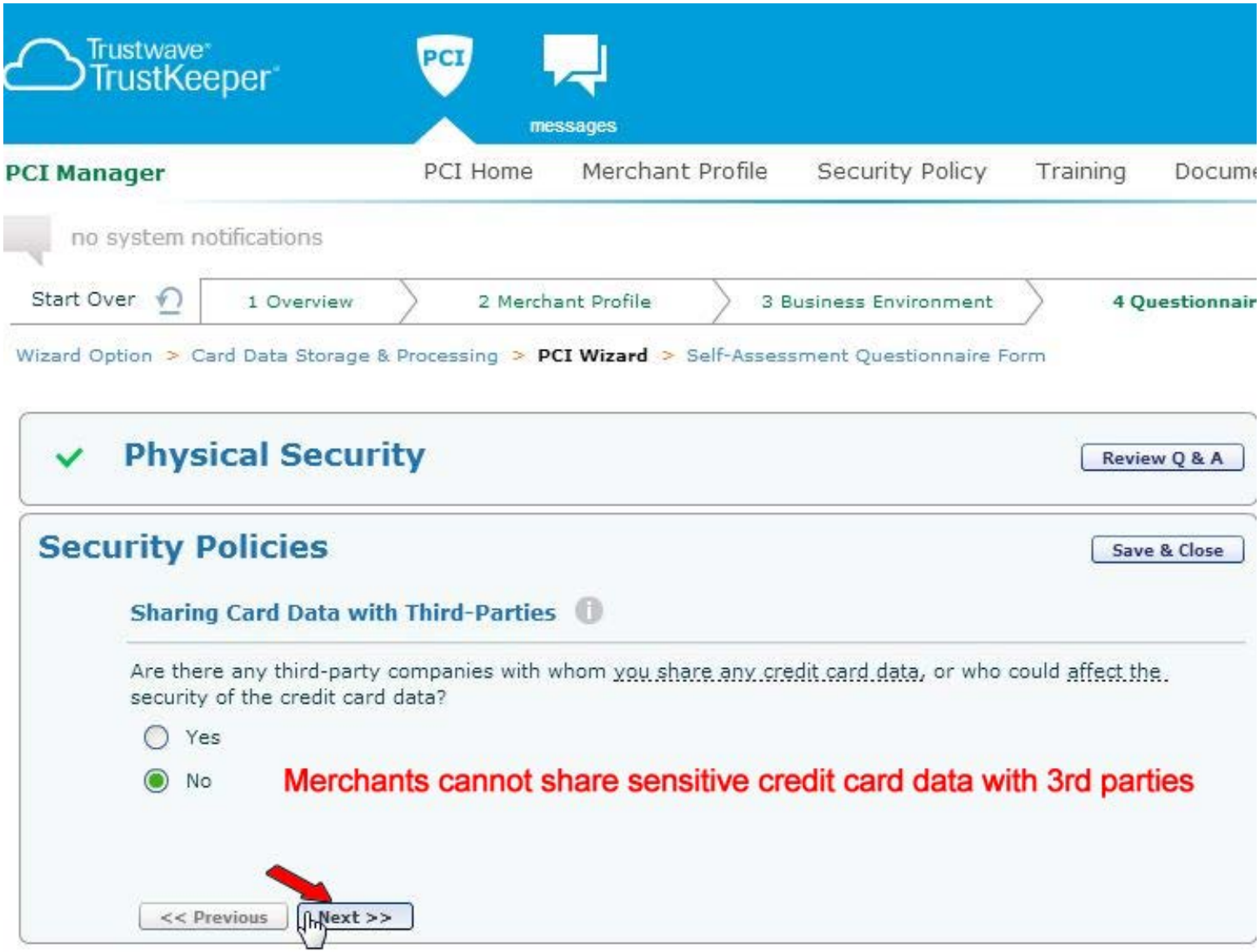
PCI version 3.0 effective for 2015 and beyond requires all merchants to frequently (daily) inspect their credit card terminals for tampering.



Screen 23


Trustwave TrustKeeper
PCI
messages
PCI Manager
PCI Home
Merchant Profile
Security Policy
Training
Documer
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
Close
Section Completed!
You have successfully completed this section and passed.
continue >>
Security Policies
Begin

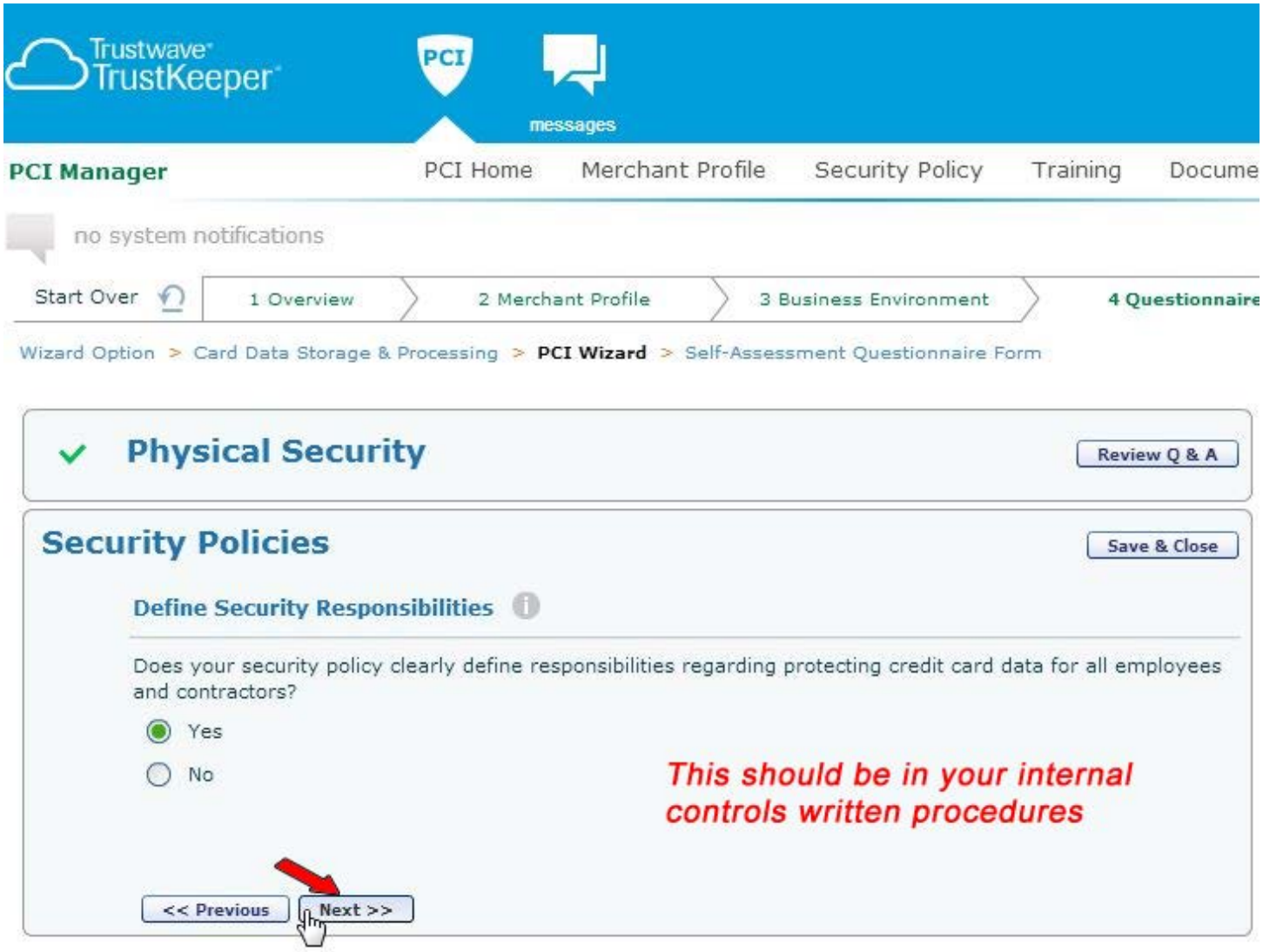
Screen 24


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 Questionnair
Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form
Physical Security
Review Q & A
Security Policies
Save & Close
Sharing Card Data with Third-Parties
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?
Yes
No
Merchants cannot share sensitive credit card data with 3rd parties
<< Previous
Next >>

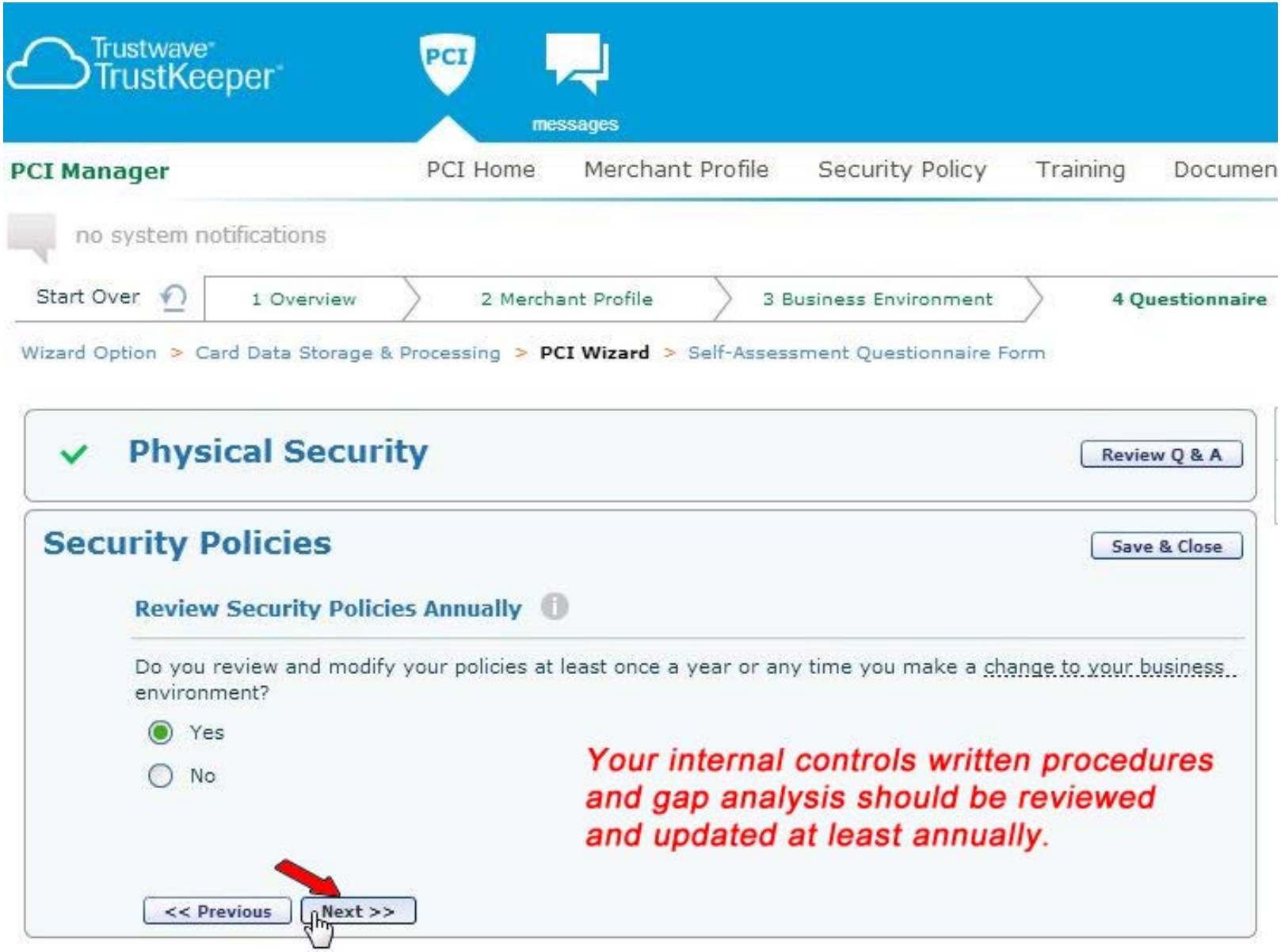
Screen 25


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 >>

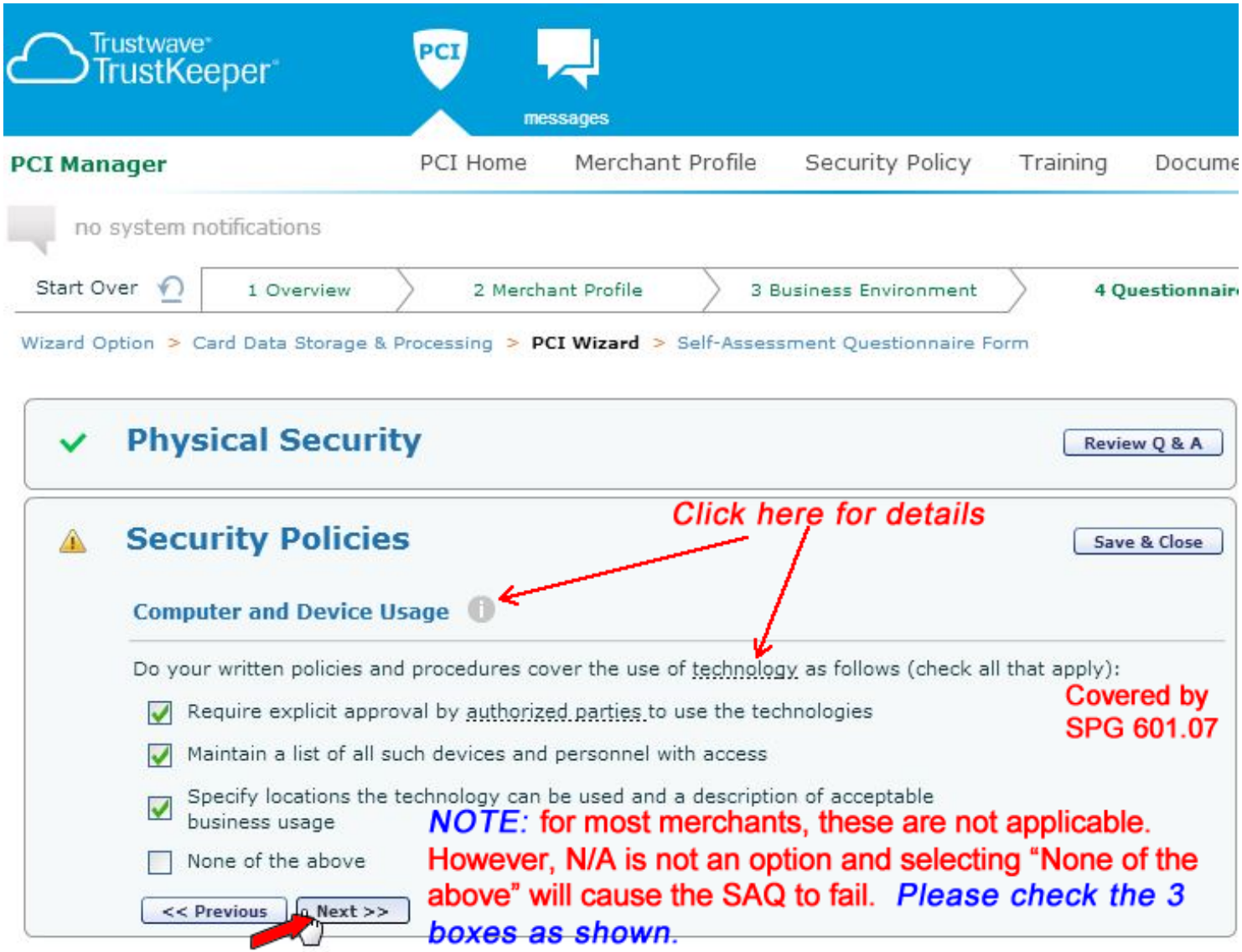
Screen 26


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 >>

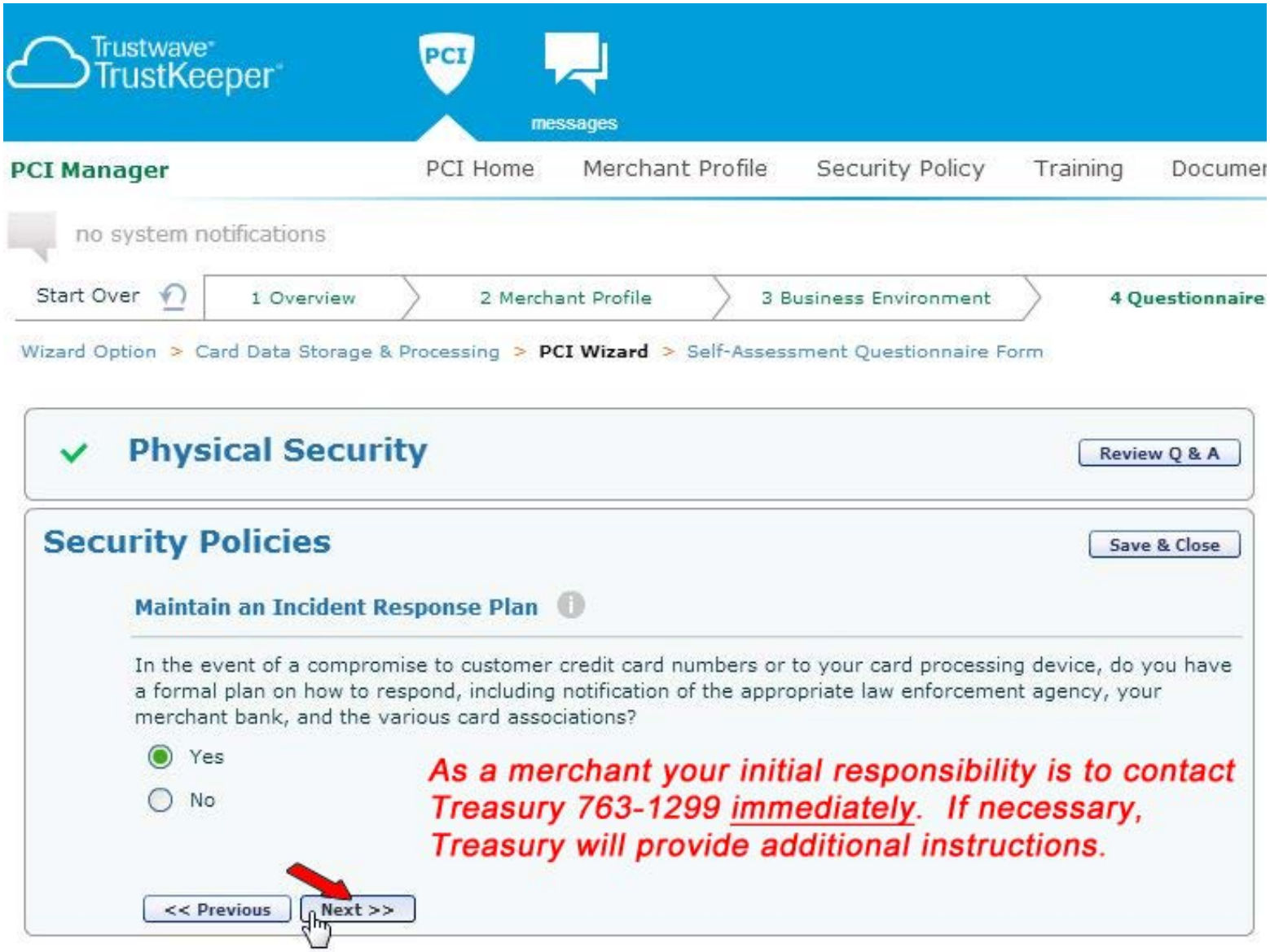
Screen 27


Trustwave TrustKeeper
PCI
messages
PCI Manager
PCI Home
Merchant Profile
Security Policy
Training
Documen
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 >>

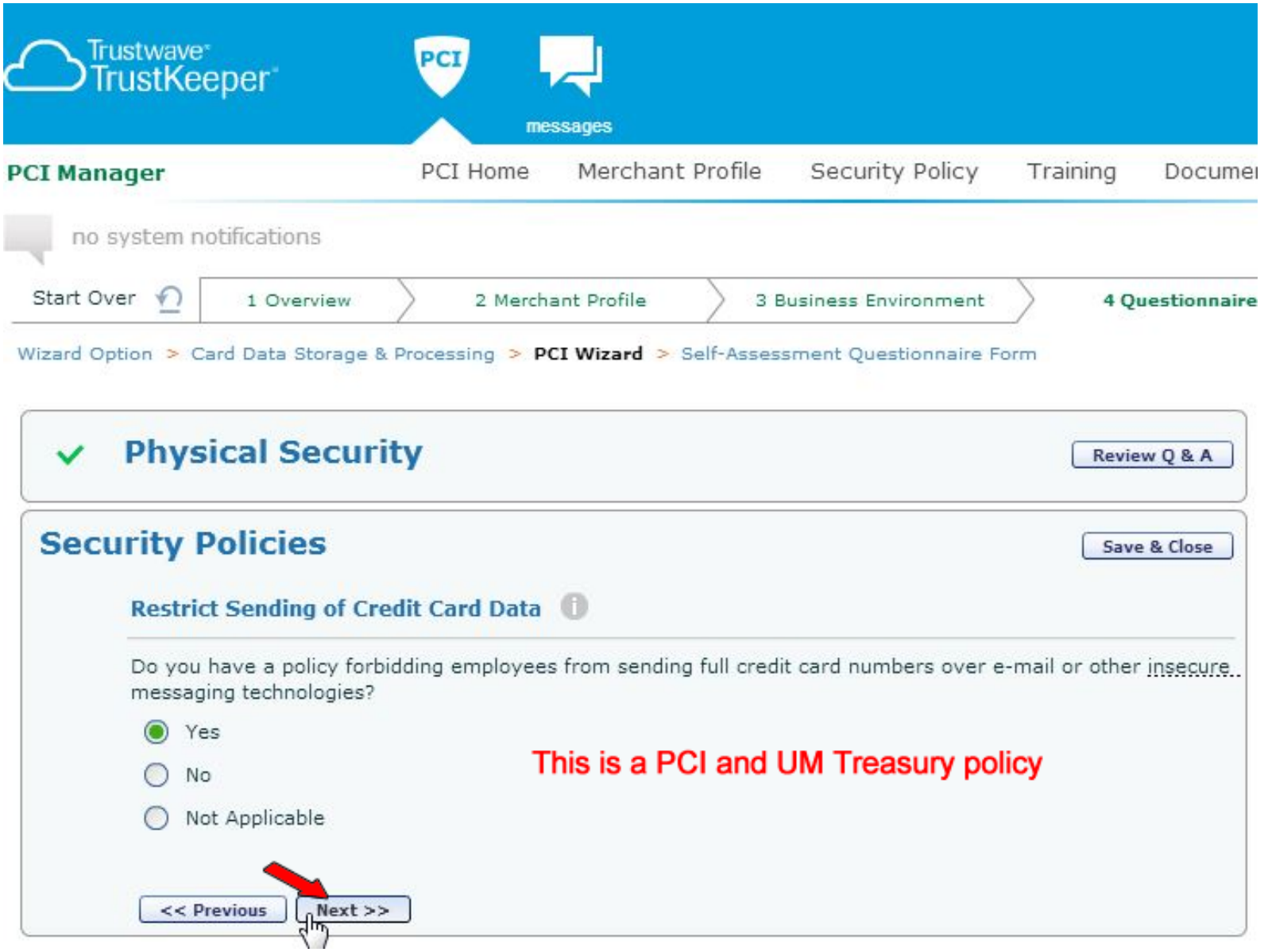
Screen 28


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 Questionnair
Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form
Physical Security
Review Q & A
Security Policies
Save & Close
Click here for details
Computer and Device Usage
Do your written policies and procedures cover the use of technology as follows (check all that apply):
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
<< Previous
Next >>
Covered by SPG 601.07
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.

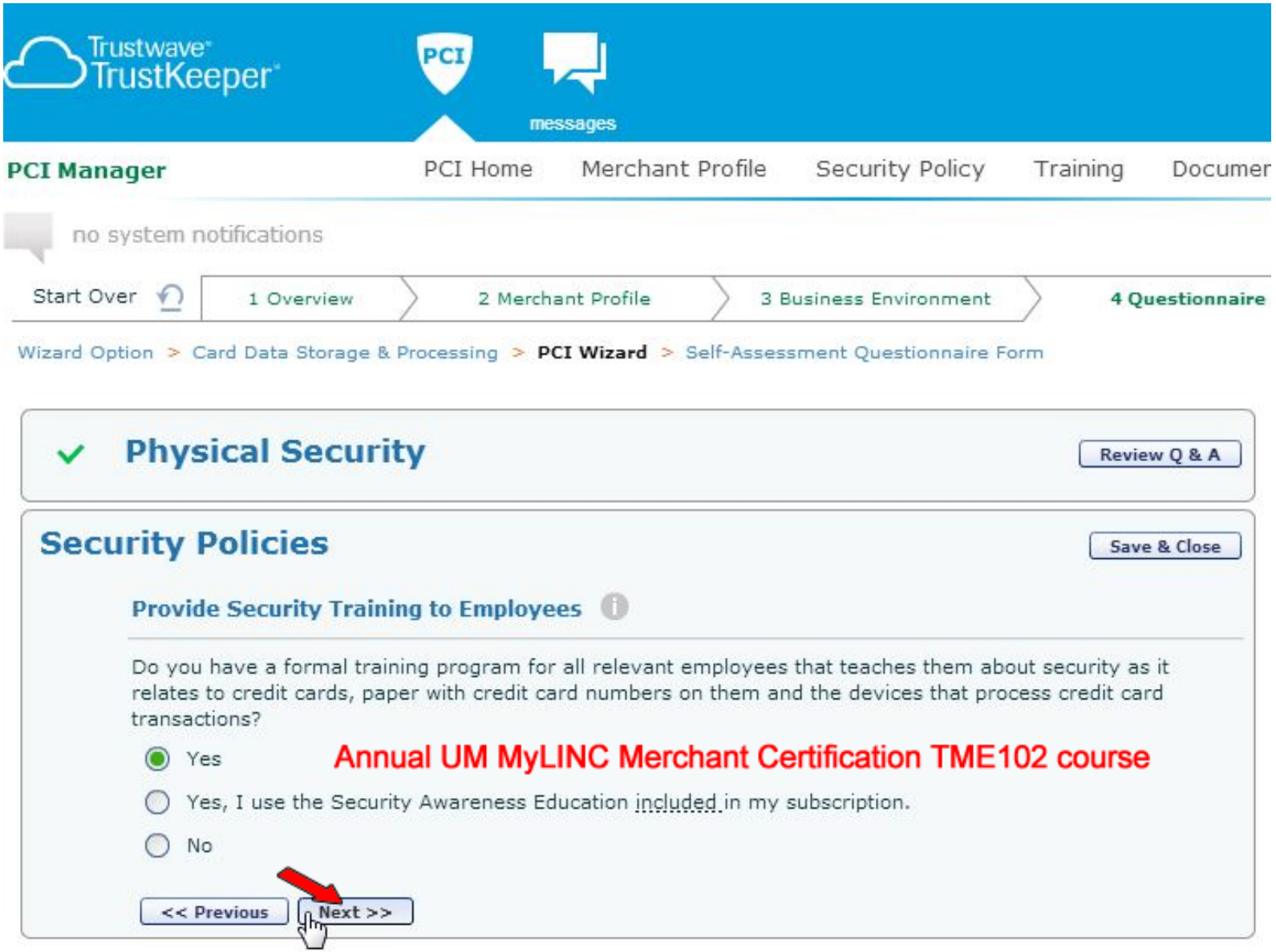
Screen 29


Trustwave TrustKeeper
PCI
messages
PCI Manager
PCI Home
Merchant Profile
Security Policy
Training
Documer
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 >>

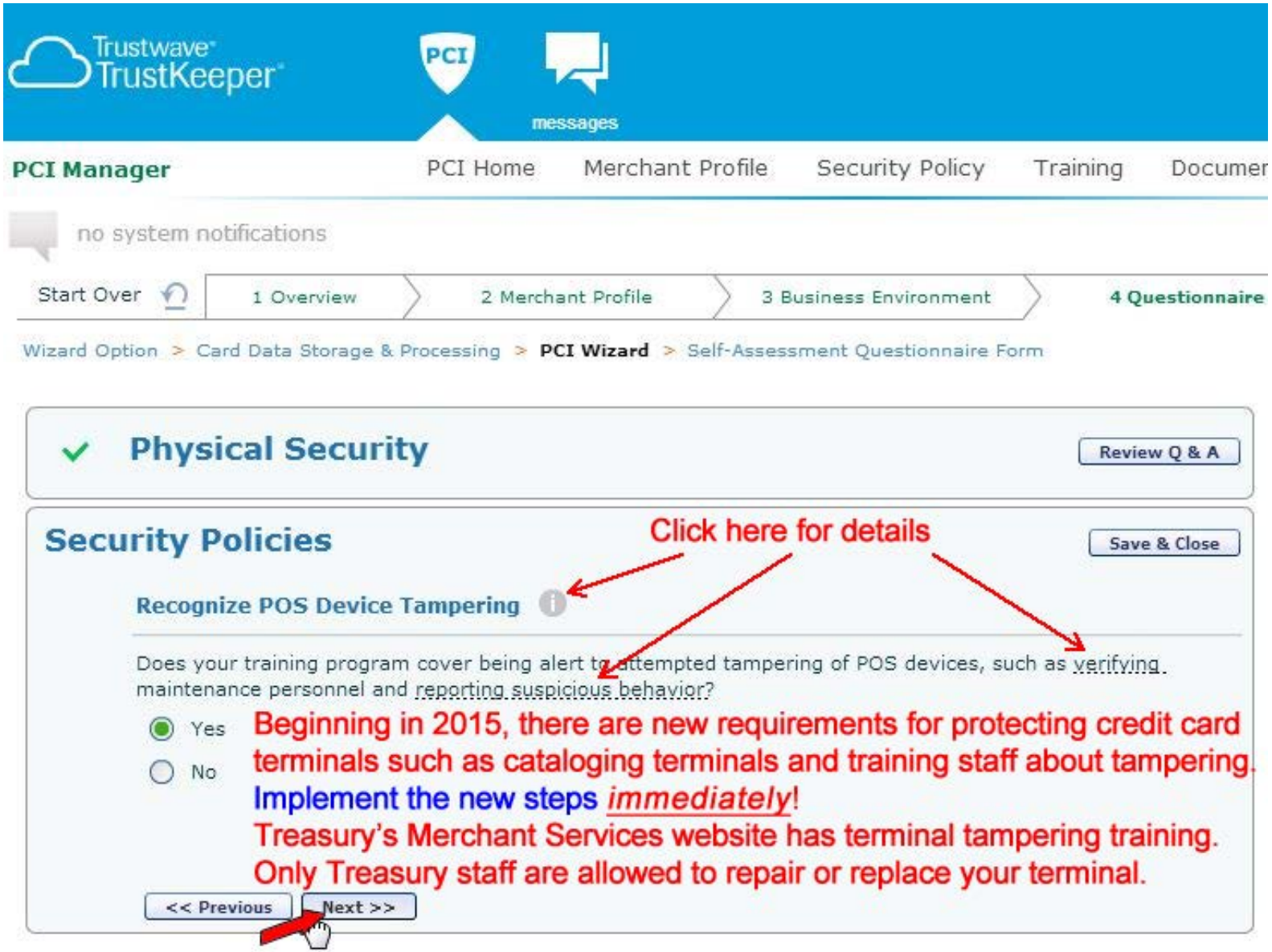
Screen 30


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
Restrict Sending of Credit Card Data
Do you have a policy forbidding employees from sending full credit card numbers over e-mail or other insecure messaging technologies?
Yes
No
Not Applicable
This is a PCI and UM Treasury policy
<< Previous
Next >>

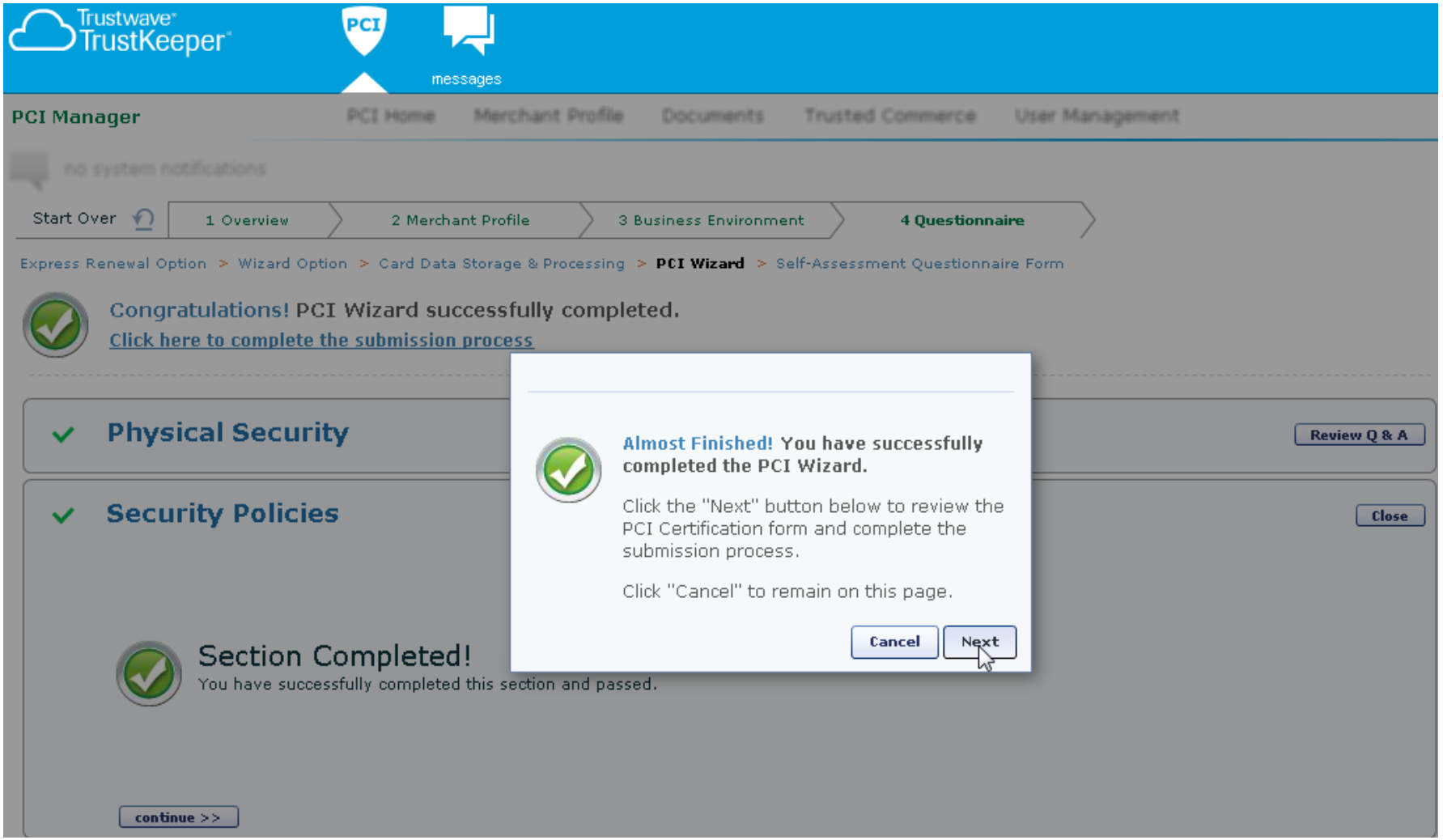
Screen 31


Trustwave TrustKeeper
PCI
messages
PCI Manager
PCI Home
Merchant Profile
Security Policy
Training
Documer
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
Provide Security Training to Employees
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?
Yes
Annual UM MyLINC Merchant Certification TME102 course
Yes, I use the Security Awareness Education included in my subscription.
No
<< Previous
Next >>

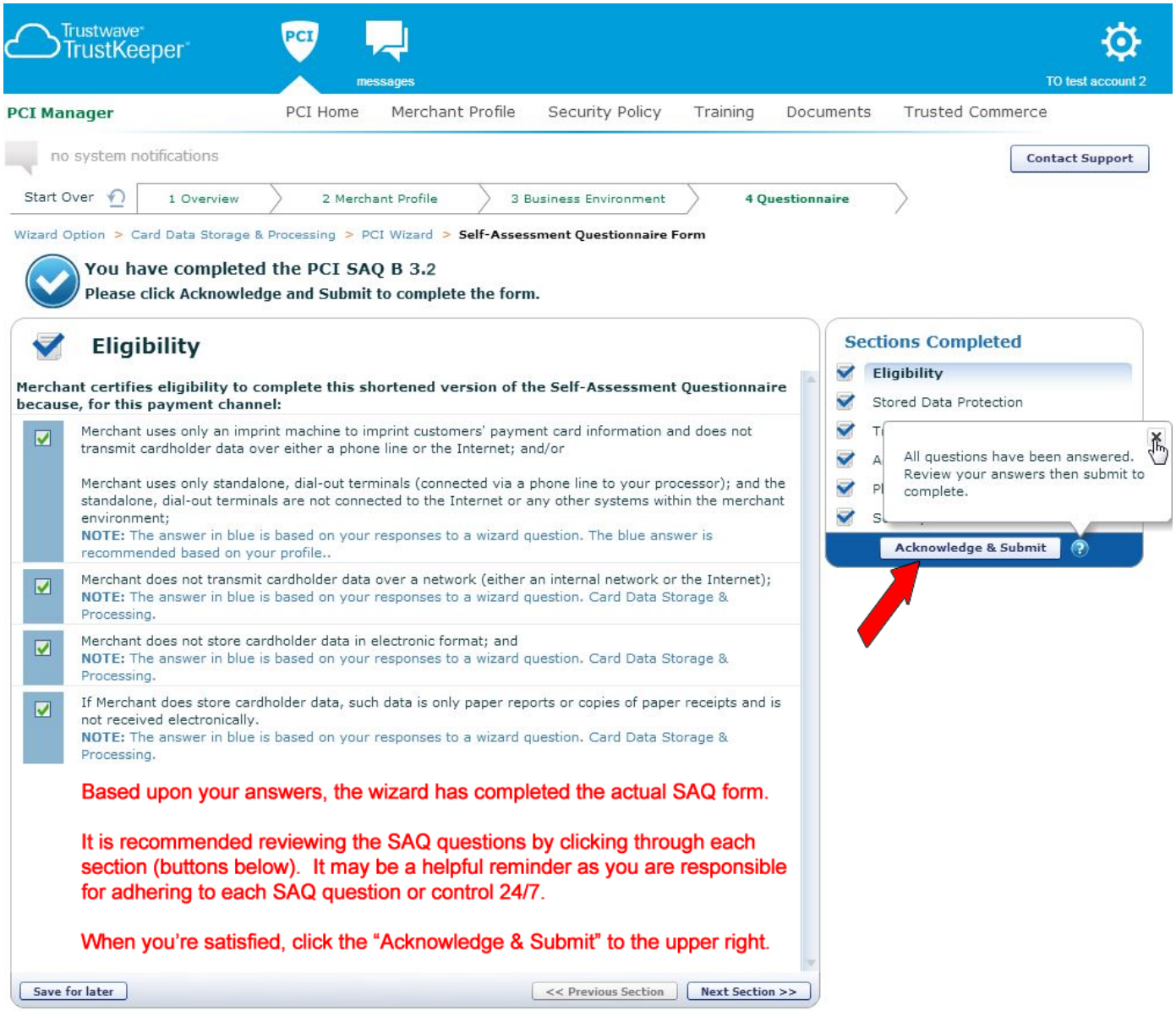
Screen 32


Trustwave TrustKeeper
PCI
messages
PCI Manager
PCI Home
Merchant Profile
Security Policy
Training
Documer
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
Click here for details
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 >>

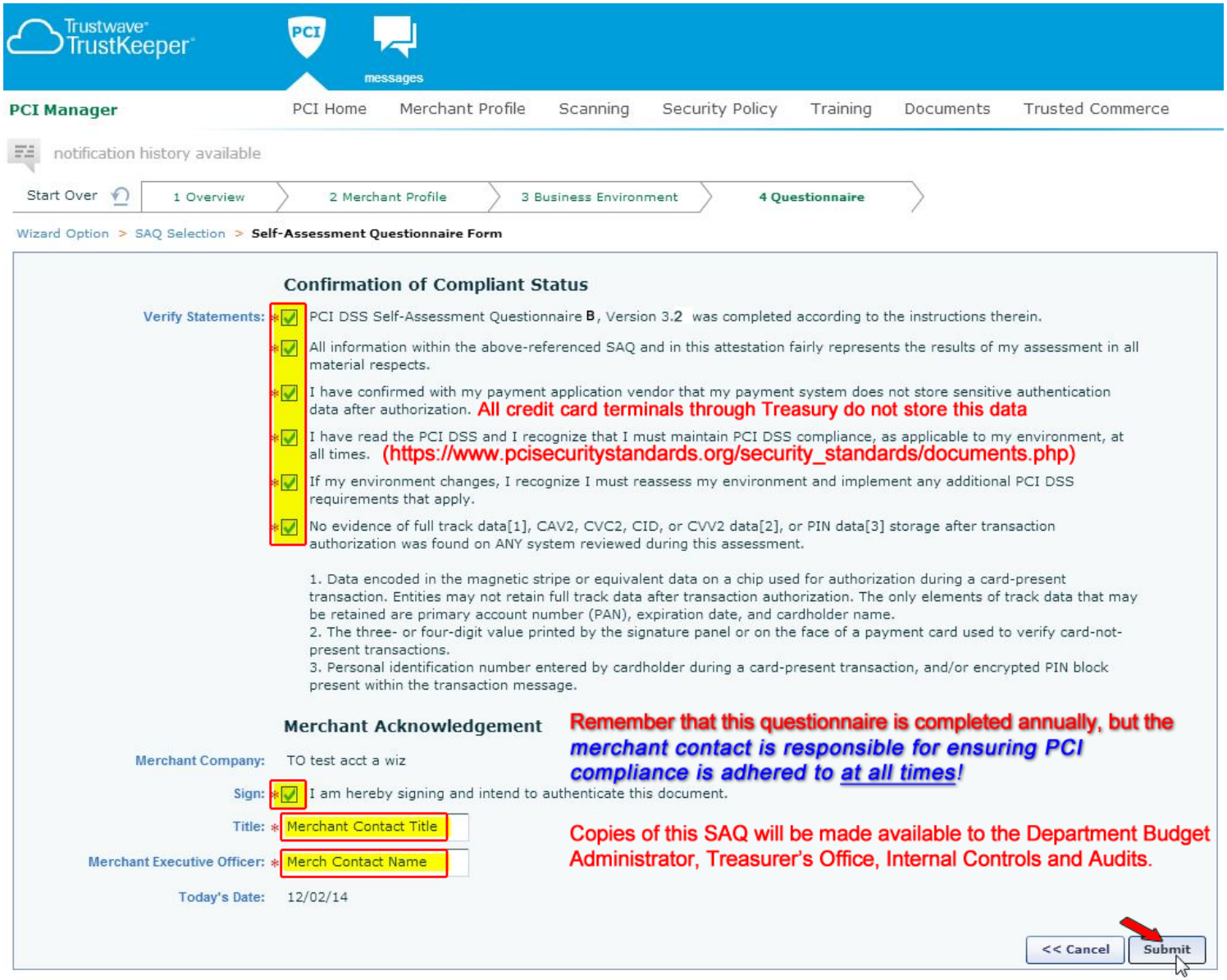
Screen 33


Trustwave TrustKeeper
PCI
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
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

Screen 34

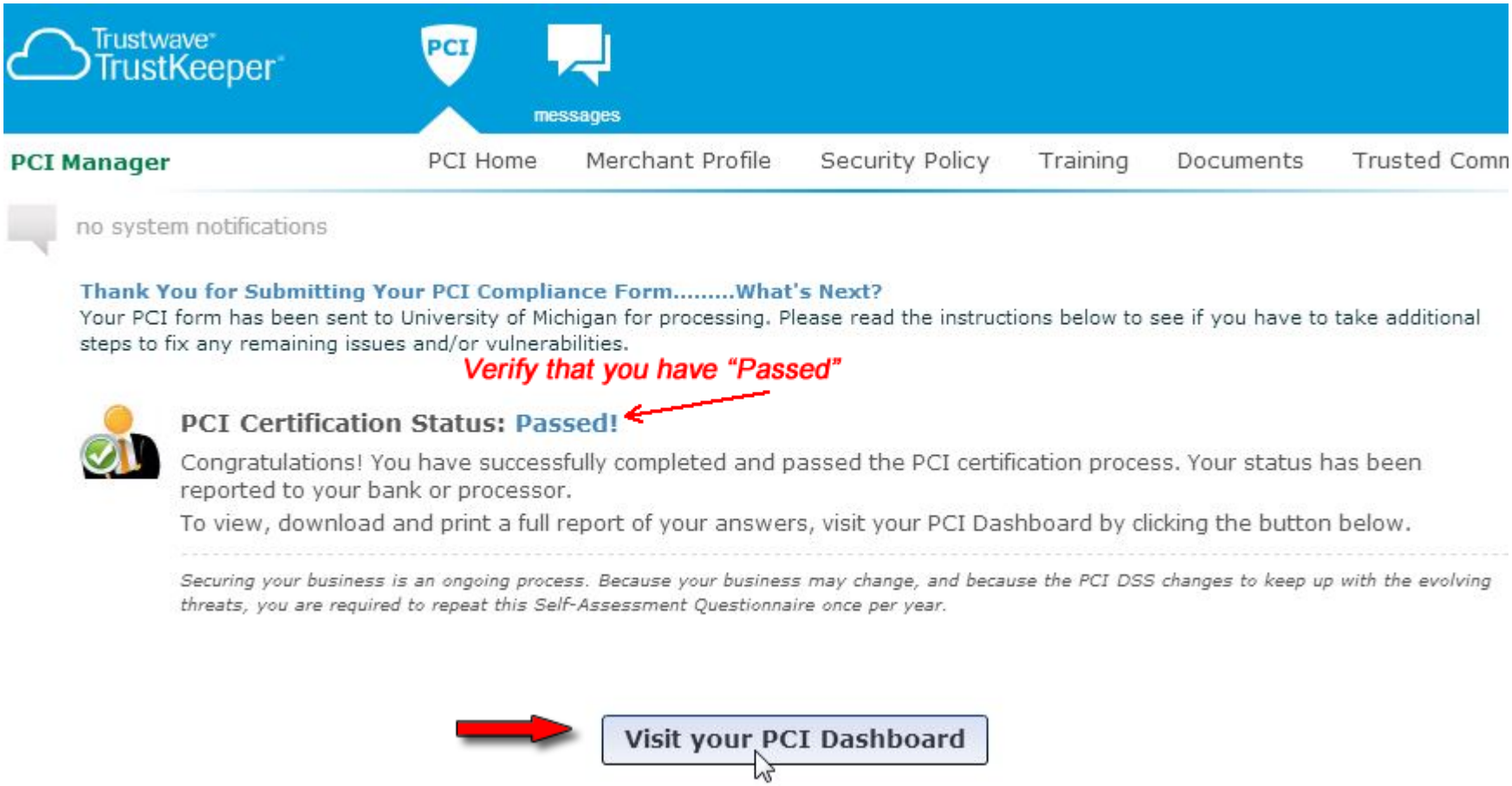

Trustwave TrustKeeper
PCI
messages
TO test account 2
PCI Manager
PCI Home
Merchant Profile
Security Policy
Training
Documents
Trusted Commerce
no system notifications
Contact Support
Start Over
1 Overview
2 Merchant Profile
3 Business Environment
4 Questionnaire
Wizard Option > Card Data Storage & Processing > 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
All questions have been answered. Review your answers then submit to complete.
Acknowledge & Submit

Screen 35

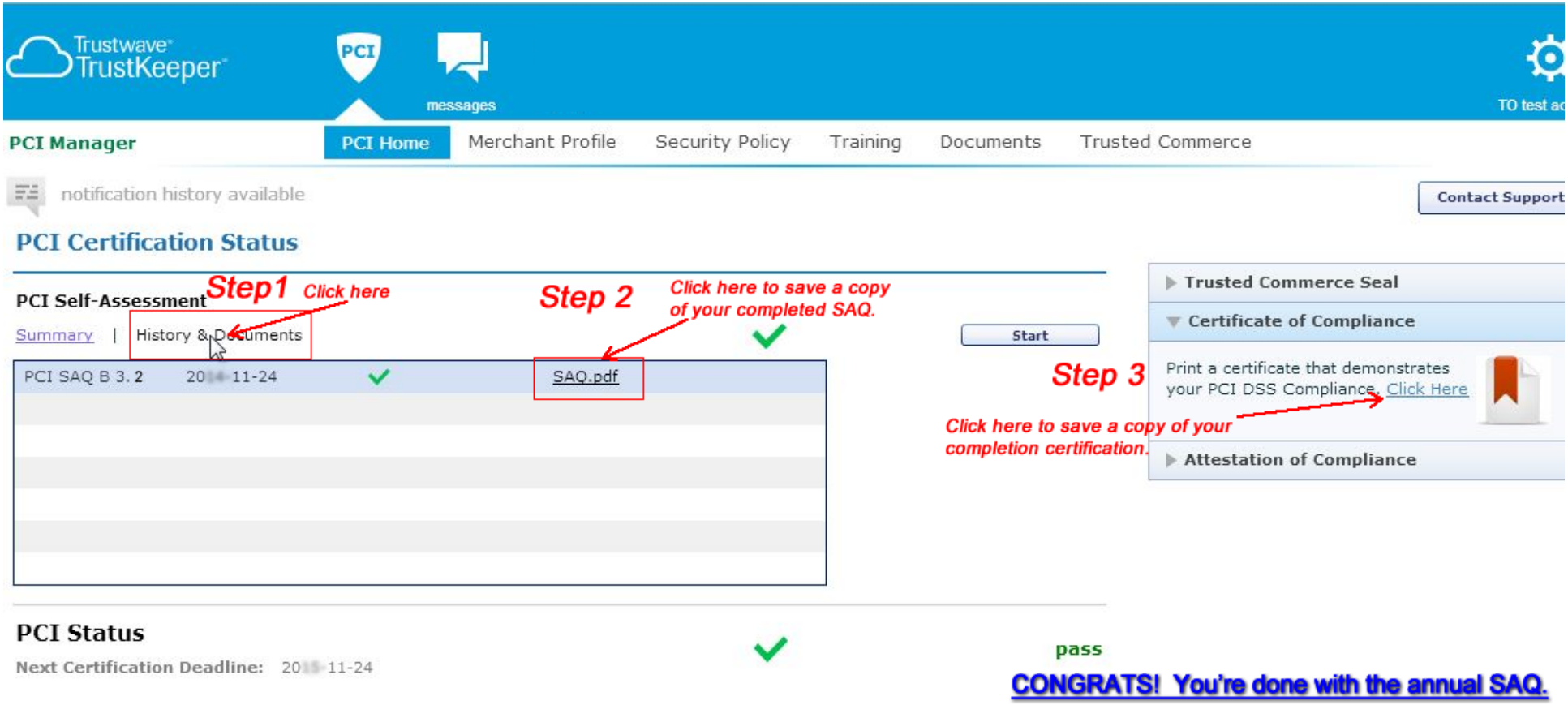

Trustwave TrustKeeper
PCI
messages
PCI Manager
PCI Home
Merchant Profile
Scanning
Security Policy
Training
Documents
Trusted Commerce
notification history available
Start Over
1 Overview
2 Merchant Profile
3 Business Environment
4 Questionnaire
Wizard Option > SAQ Selection > Self-Assessment Questionnaire 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)
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 Contact Title
Merchant Executive Officer:
Merch Contact Name
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.



Screen 37



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

Contact UM Treasury merchantservices@umich.edu with any questions.