

GETTING STARTED WITH THE WELLS FARGO PCI DSS PROGRAM

James Zou, Systems Engineer, QSA, PCIP



AGENDA

- 1 Wells Fargo Program
- 2 About Trustwave
- 3 PCI Basics
- 4 The Risk of Non-Compliance
- 5 Using TrustKeeper PCI Manager



WHO WE ARE

Company facts and figures

SERVING

over **3 MILLION** subscribers

GROWING

with over **1,300 EMPLOYEES**

GLOBAL

employees in **26** countries

INNOVATING

over **56** patents granted / pending



THREAT MANAGEMENT

Integrated portfolio of technologies delivering comprehensive protection



VULNERABILITY MANAGEMENT

Global Threat Database feeding Big Data back-end

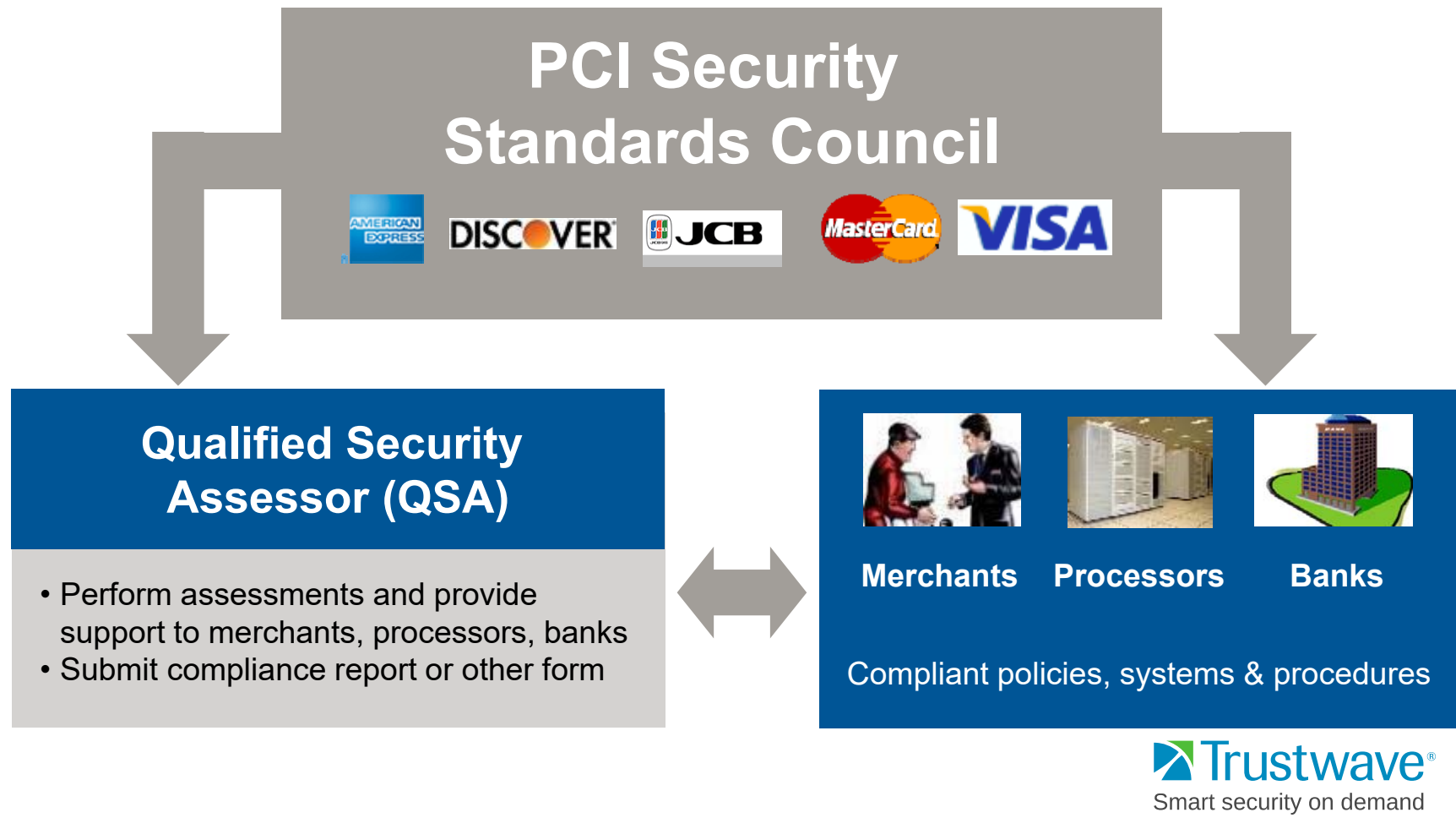


COMPLIANCE MANAGEMENT

Leading provider of cloud delivered IT-GRC services

WHO'S RESPONSIBLE FOR WHAT

Oversight, Responsibility, Enforcement



PCI BASICS

PCI DSS defined

- Cardholder data is any personally identifiable data including:
 - Primary Account Number
 - Expiry Date
 - Name
- Sensitive Authentication Data must also be protected:
 - Full Track Data (magnetic strip)
 - CAV2/CVC2/CVV2/CID (3 or 4 digit code)
 - PIN/PIN Block
- All merchants accepting debit/credit cards must comply with the PCI DSS at all times.

PCI BASICS

PCI DSS defined



- The Payment Card Industry Data Security Standard (PCI DSS) is a set of 12 requirements designed to protect cardholder data
- Applies to all merchants, systems, networks and applications that process, store, and/or transmit card numbers
 - Build and Maintain a Secure Network and Systems (2)
 - Protect Cardholder Data (2)
 - Maintain a Vulnerability Management Program (2)
 - Implement Strong Access Control Measures (3)
 - Regularly Monitor and Test Networks (2)
 - Maintain an Information Security Policy (1)

PCI DSS

Key terms

- **Self-Assessment Questionnaire (SAQ)**
 - A questionnaire designed to assist organizations in self-evaluating their IT and payment processing environment
- **Vulnerability Scanning**
 - Helps secure your business by identifying weaknesses in your network and applications
- **Qualified Security Assessor (QSA)**
 - Certified to validate that a company is compliant with the PCI DSS
- **Approved Scanning Vendor (ASV)**
 - Certified to perform vulnerability scanning

VALIDATION ACTIONS DEPEND ON LEVEL

Merchant Level		Validation Actions	Validated By	Deadline
3	Any merchant that processes 20,000 to 1 million e-commerce transactions annually	Annual Self-Assessment Questionnaire	Merchant	6/30/05
		Quarterly Network Scan	Approved Scanning Vendor	
4	Any merchant that processes up to 1 million brick-and-mortar Visa transactions, or less than 20,000 Visa/e-commerce transactions annually	Annual Self-Assessment Questionnaire	Merchant	Validation requirements and dates are determined by the merchant's acquirer
		Quarterly Network Scan	Approved Scanning Vendor	

THE RISK OF NON-COMPLIANCE

- Large corporations that have been breached make it to the evening news
- What doesn't make the news is that **SMALL MERCHANTS** are at the greatest risk of a data breach

Trustwave found that 90% of merchants that have data stolen are small businesses.

PCI DSS COMPLIANCE

Sound business practice

- Fundamental security best practices
 - Avoid fraud
 - Helps to understand own system better
 - Clarifies where data is stored
- Upholds brand name
 - Adds value to name
 - Increases consumer confidence
- Non-compliant or compromised business could expect:
 - Damage to their brand/reputation
 - Investigation costs
 - Remediation costs
 - Fines and fees








GETTING STARTED WITH TRUSTKEEPER PCI MANAGER



GETTING STARTED





Getting Started with TrustKeeper® is easy.
Register your business today.

[Get Started](#)

Already Registered? [Login](#)


Welcome to the Trustwave PCI Compliance Service Program. This program is designed to help you understand and respond to the data security needs of your business - especially if you accept credit cards for payment.

To get started, you [simply need to register](#). The PCI wizard will walk you through the self-assessment process.

What is PCI DSS?	Become Compliant	About Trustwave	Support
----------------------------------	----------------------------------	---------------------------------	-------------------------

REGISTRATION – THREE EASY STEPS

Step 1: Enter merchant information

English (US) ▼

Registration

Start

My Business

Register

Company Information

Company Name: * ?

Merchant ID: * ?

Country: * United States of America ▼

ZIP/Postal Code: *

* Required Field

Authorized Contact

Primary Contact: * ☒ This is for the actual PCI certification user, who will be the primary person contacting support. ?

First Name: *

Last Name: *

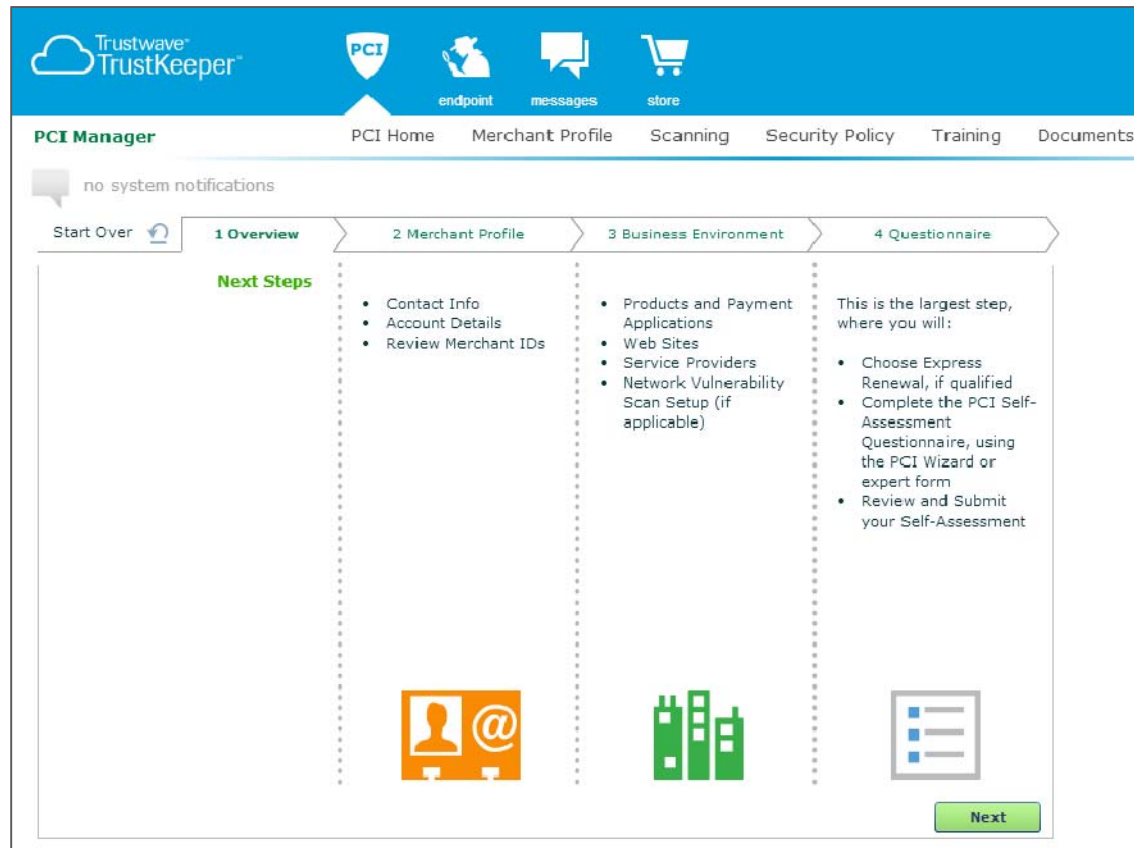
Email: *

Phone Number: *

Continue >>

ASSESSMENT OVERVIEW

Customized step-by-step workflow



BUSINESS ENVIRONMENT

Guidance for scanning and tuning the workflow

The screenshot displays the Trustwave TrustKeeper PCI Manager interface. The top navigation bar includes the TrustKeeper logo and icons for PCI, endpoint, messages, and store. Below this, the 'PCI Manager' section contains links for PCI Home, Merchant Profile, Scanning, Security Policy, Training, Documents, and Tru. A notification area indicates 'no system notifications'. A progress bar shows four steps: 1 Overview, 2 Merchant Profile, 3 Business Environment (current), and 4 Questionnaire. The breadcrumb trail reads 'Card Acceptance > Products > Scan Setup'. The main content area is titled 'Products' and includes a text prompt: '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.' Below this is a table with columns: Product, Version, Product Type, Entered By, and Severity. The table contains one entry: 'Micros 3700' with version '5.0.0003.0416' and product type 'Payment Application'. At the bottom, there is an 'Add Product' button, a checkbox labeled 'I don't use any devices to process cards.', and 'Previous' and 'Next' buttons.

Trustwave® TrustKeeper™

PCI endpoint messages store

PCI Manager PCI Home Merchant Profile Scanning Security Policy Training Documents Tru

no system notifications

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

Card Acceptance > Products > Scan Setup

Products

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.

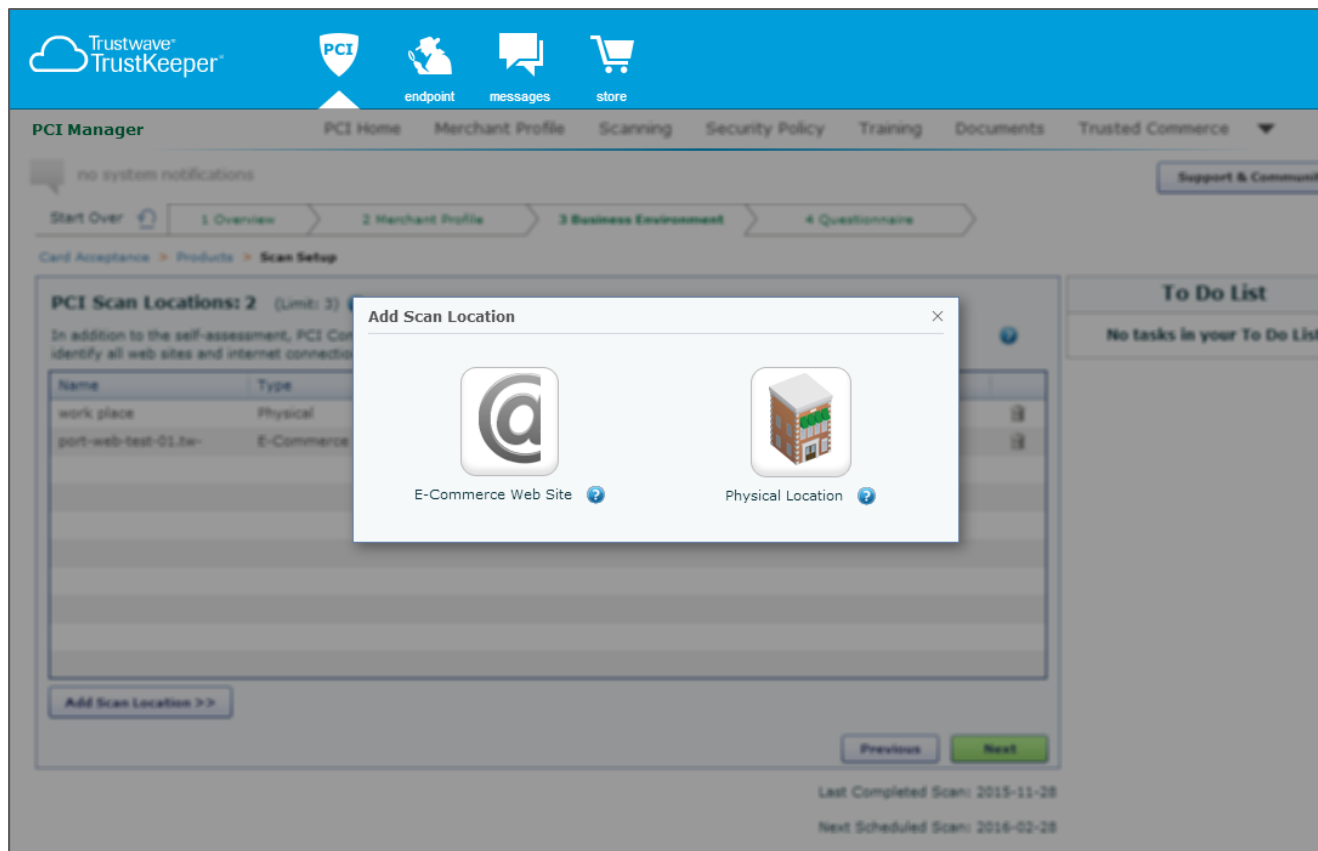
Product	Version	Product Type	Entered By	Severity
Micros 3700	5.0.0003.0416	Payment Application		

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

Previous Next

SCAN SETUP

E-commerce website or physical location?



EXPERT FORM OR PCI WIZARD

Simplify completion by selecting the Step-By-Step Wizard

The screenshot displays the Trustwave TrustKeeper PCI Manager interface. At the top, there's a blue header with the TrustKeeper logo and navigation icons for PCI, messages, and store. Below this is a navigation bar with links: PCI Home, Merchant Profile, Security Policy, Training, Documents, and Trusted Commerce. A notification says "notification history available". A progress bar shows four steps: 1 Overview, 2 Merchant Profile, 3 Business Environment, and 4 Questionnaire. The "Wizard Option" section offers two choices:

- ☒ **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.

Illustrations include a wizard path with stars, three step cards (Step 1: Name/Email, Step 2: Scan Wizard/Start Scan, Step 3: PCI Wizard/SAQ), and a "PCI DSS Questions" form with a pencil.

Navigation buttons at the bottom right: Previous, Next.

PCI WIZARD

The screenshot displays the Trustwave TrustKeeper PCI Manager interface. At the top, there's a blue header with the Trustwave TrustKeeper logo and navigation icons for PCI, endpoint, messages, and store. Below the header, a navigation bar includes links for PCI Home, Merchant Profile, Scanning, Security Policy, Training, Documents, and Tru. 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.

Card Data Storage & Processing Save & Close

Credit Card Data Storage ?

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.

<< Previous Next >>

Contextual help and tips throughout + 24/7/365 helpdesk



Card Data Sensitive

Sensitive credit card data includes the full credit card number, the 3- or 4-digit card validation code, PIN data, or full magnetic stripe data (track data) from a credit card.

Credit Card Data

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.

Internet and Network Security

Secure Communications

Secure Communication for Payment Data

For your payment applications and point-of-sale (POS) terminals, is strong encryption ALWAYS used to transmit data during both authorization and settlement?


☐ Yes

☐ No

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

Encryption is a method to protect data by rendering it unreadable without a mathematical "key". "Strong encryption" (as opposed to "weak encryption") is encryption based on industry-tested and accepted techniques that hold up better at any attempts to break them and read the data.

GUIDANCE TOWARDS COMPLIANCE

**Action Required! You have PCI issues to resolve.**
[Click here to submit results without resolving issues](#)

**Internet and Network Security**

Review Q & A

**Secure Communications**

Review Q & A

**Device & Computer Security**

Save & Close


**Action Required**

- Change default settings for all computers and devices.


These have been added to your To Do list to help you track them.

Review Issues Now

continue >>

**Secure Management and Monitoring**

Review Q & A

**Physical Security**

Review Q & A

**Security Policies**

Review Q & A


To Do List 

Use A Firewall to protect your business from hackers.

Securely destroy documents with credit card numbers.

Keep paper receipts locked and protected at all times.

Change default settings for all computers and devices.

 **Trustwave**[®]
Smart security on demand

© 2016 Trustwave Holdings, Inc.

SCAN RESULTS

Online and offline (PDF) scan results

PCI Manager

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

no system notifications

Support & Community

Scan Results Scan Setup

Scan Report: 06/06/2015 12:39 AM

Dispute Finding Ask Support PDF Report

Status	IP	Domain	Protocol	Port	Severity	PC	CVE	Vulnerability Name
			tcp	443	■■■■	⓪		SSL Weak Encryption Algorithms
			tcp	443	■■■		CVE-2000-0649	Private IP Address Leaked through HTTP Headers
			tcp	80	■■■		CVE-2000-0649	Private IP Address Leaked through HTTP Headers
			tcp	443	■■■			HTTP TRACE
			tcp	80	■■■			HTTP TRACE
			tcp	0	■■■			System Responds to SYN+FIN TCP Packets
			tcp	443	■■■		CVE-2002-0419	IIS Authentication Method ID
			tcp	80	■■■		CVE-2002-0419	IIS Authentication Method ID
			tcp	443	■■■		CVE-2002-0422	WebDAV Reveals Internal IP
			tcp	80	■■■		CVE-2002-0422	WebDAV Reveals Internal IP
			tcp	443	■■■			IIS Failure To Log Undocumented TRACK Requests
			tcp	80	■■■			IIS Failure To Log Undocumented TRACK Requests
			tcp	80	■■			Discovered HTTP Methods
			tcp	443	■■			Discovered HTTP Methods

Displaying 1 to 23 of 23

Page 1 of 1

Trustwave®

Report Date: 2016-02-04

Vulnerability Scan Report: Attestation of Compliance

Scan Customer Information	Approved Scanning Vendor Information
Company Name: James Jelly Bean Store #28 Contact: Jk Telephone: 121212123 Business Address: 70 W Madison St City: Chicago ZIP/Postal Code: 60602	Company Name: Trustwave Holdings, Inc. Contact: Trustwave Support Telephone: 1-800-363-1621 Business Address: 70 West Madison St., Ste 1050 City: Chicago ZIP/Postal Code: 60602
Title: j. com E-mail: j. com State/Province: Illinois Country: US	URL: www.trustwave.com E-mail: support@trustwave.com State/Province: IL Country: US

Scan Status

Fail Scan Compliance Status

- 2 Number of unique components scanned that are in scope
- 1 Number of identified failing vulnerabilities
- 0 Number of components scanned by TrustKeeper but confirmed by the customer not to be in scope

2015-10-28 Date Scan Completed
N/A Scan Expiration Date (3 months from Date Scan Completed)

Scan Customer Attestation	Approved Scanning Vendor Attestation
James Jelly Bean Store #28 attests that: This scan includes all components which should be in scope for PCI DSS, any component considered out-of-scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions is accurate and complete. James Jelly Bean Store #28 also acknowledges the following: 1) proper scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of the PCI DSS. This scan does not represent James Jelly Bean Store #28's overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.	This scan and report were prepared and conducted by Trustwave under certificate number 3702-01-10 (2016), 3702-01-08 (2014), 3702-01-08 (2013), 3702-01-07 (2012), 3702-01-06 (2011), according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide. Trustwave attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, and 3) active interference. This report and any exceptions were reviewed by the Trustwave Quality Assurance Process.
Signature	Printed Name
Title	Date

Confidential Information: This document may contain information that is privileged, confidential or otherwise protected from disclosure. Dissemination, distribution or copying of this document or the information herein is prohibited without prior permission of Trustwave and James Jelly Bean Store #28.

Copyright © 2016 Trustwave Holdings, Inc. All rights reserved. Page 1 of 9

CERTIFICATION DOCUMENTS

**PCI DSS**
Certificate of Compliance A9E9-E42F-7233-A043

Self-Assessment Questionnaire

Status: **Pass** 2015-01-12 16:33:40, valid through 2016-01-12

Version: SAQ B


Attested By: Test Test, Owner

Awarded To: Demo_Company 27

Client Authorization: _____
Sign Name _____ Print Name _____
This signed contact at Demo_Company 27 agrees to the accuracy of all information provided within Trustwave PCI Manager

To maintain compliance, the above named client referred to below as "CLIENT" must be aware of and validate against their individual requirements as set by the Payment Card Industry Security Standards Council and the payment card brands. For information on requirements, please visit [www.pcisecuritystandards.org](#). In addition, CLIENT must continually identify and provide to Trustwave information regarding any new systems that store, process, or transmit cardholder data, so that this system can be included in the scope of the validation process. This certificate is valid through the expiration date stated above. It is the client's sole responsibility to maintain compliance with the card association security requirements and obtain validation on at least a quarterly basis. Trustwave makes no representation or warranty as to whether CLIENT systems are secure from either an internal or external attack or whether cardholder data is at risk of being compromised. This certificate is for the sole purpose of identifying compliance and attestation for said compliance by CLIENT and cannot be used for any other purpose without express written consent of Trustwave's legal counsel.

Participating organizations: Visa® Europe, Visa® Inc., MasterCard® Worldwide, American Express®, Discover® Financial Services, JCB Co., Ltd.




**Payment Card Industry (PCI)
Data Security Standard**

**Attestation of Compliance for
Self-Assessment Questionnaire B**
Version 3.1
April 2015

TRUSTED COMMERCE SEAL


Display a “seal of approval”


 Languages: English ▼

Your credit card and identity information are secure.

COMPLIANCE: VALIDATED

Organization: James Jelly Bean Store #28 **Valid:** 2/4/2016


Click to Validate



Based upon information provided by James Jelly Bean Store #28 regarding its policies, procedures, and technical systems that store, process and/or transmit cardholder data, James Jelly Bean Store #28 has performed the required procedures to validate compliance with the PCI DSS.

[Buy Trusted Commerce](#) [Refer a Website](#) [Report Seal Misuse](#)

Disclaimer: Trustwave Holdings, Inc. makes no representation or warranty as to whether James Jelly Bean Store #28 systems are secure from either an internal or external attack or whether cardholder data is at risk of being compromised. Trustwave Holdings, Inc. makes no representations or warranties regarding this company's business activities or operations. Please contact the company displaying the seal if you have questions about their products, services or customer support.

© 2016 Trustwave • Ph: 877-262-4766 • (312-873-7500 outside U.S. or Canada) • info@trustwave.com






Click to Validate

[Terms of Use](#) | [Privacy Policy](#)

 **Trustwave®**
Smart security on demand

SECURITY POLICY ADVISOR

Sample security policies and supporting documents




messagesstore

PCI ManagerPCI HomeMerchant ProfileSecurity PolicyTrainingDocumentsTrusted Commerce

notification history available

Your Security Policy

**Security Policy Document**

Download .docDownload .rtf

Instructions: A security policy template has been drafted for your business. Please print out this document and review it carefully, filling in the blanks as applies to your specific business.

[Sample Security Policies](#) >>

*.DOC - Microsoft Word format / .RTF - Rich Text Format (WordPad, TextEdit, etc.)

Note: These are policy templates and may need modification to fit your specific business environment. These documents are intended as an aid to assist you in developing policies and procedures for your business and systems that adhere to the Payment Card Industry Data Security Standard. Adopting these policies does not guarantee that you will become PCI compliant or that your systems are secure. Trustwave makes no representations or warranties and specially disclaims any and all representation and warranties regarding these policies.

Supporting Documents

These supplemental documents are available if needed to help you implement the security policy you adopt.

Documents	Download
Security Awareness and Acceptable Use Policy	.doc .rtf
Authorization Request Form	.doc .rtf
Media Inventory Log	.doc .rtf
Periodic Operational Security Procedures	.doc .rtf

SECURITY AWARENESS EDUCATION

Online training based on different industries and roles

The screenshot shows the Trustwave TrustKeeper PCI Manager interface. The top navigation bar includes the TrustKeeper logo, a PCI shield icon, and links for messages and store. The main menu has tabs for PCI Home, Merchant Profile, Security Policy, and Training (which is selected). Below the menu, a notification area states 'no system notifications'. The 'Security Awareness Education' section is active, showing a three-step process: 1. Select Your Industry (with a 'Retail' button), 2. Select Your Training Options (with a 'Basic' button and a 'Your training options' link), and 3. Take a Course. Under 'Take a Course', there are two columns of links: 'Managers' and 'Associates'. The 'Managers' column includes links for Payment Card Industry Overview, Information Security, Security Awareness, Sensitive Information, Social Engineering, Physical Security, PC Security, Email Security, Password Security, Web browsing Security, and Security Awareness for Retail Managers. The 'Associates' column includes links for Information Security, Security Awareness Overview, Sensitive Information, and Secure Practices for Retail Associates.

This screenshot shows the 'E-mail Security' lesson overview screen. It features a large '@' symbol on the left. The title 'E-mail Security' is at the top right. Below it, the 'Lesson Overview' section states: 'This lesson defines e-mail security and describes common threats and security best practices. You will learn about three major topics:'. A list follows: 1. What is e-mail security? 2. How information is stolen 3. Using e-mail securely. At the bottom, there is a progress bar showing '1 / 16' and 'BACK' and 'NEXT' buttons.

This screenshot shows the 'Security Awareness' lesson overview screen. It features an image of a safe on the left. The title 'Security Awareness' is at the top right. Below it, the 'Lesson Overview' section states: 'This lesson provides an introduction to security awareness and the importance of following security awareness best practices. You will learn about three main topics:'. A list follows: 1. Security Awareness Defined 2. Threats to Security 3. Importance of Awareness. At the bottom, there is a progress bar showing '1 / 5' and 'BACK' and 'NEXT' buttons.


 **Trustwave®**
Smart security on demand

USER MANAGEMENT

Create additional users to work as a team

The screenshot displays the Trustwave TrustKeeper PCI Manager interface. The top navigation bar includes the Trustwave TrustKeeper logo, a PCI shield icon, and icons for endpoint, messages, and store. The main navigation menu shows options like PCI Home, Merchant Profile, Scanning, Security Policy, Training, and User Management (which is highlighted). A 'Support & Community' link is also visible. The background shows a table of users with columns for Username, First Name, and Last Name. Overlaid on this is a 'New User' form. The form contains the following fields: Customer Name (pre-filled with 'James Jelly Bean Store #28'), Username (with a red asterisk and error icon), Email (with a red asterisk), First Name (with a red asterisk), Last Name (with a red asterisk), Address 1, Address 2, Country/Region (a dropdown menu showing 'Please Select...'), State/Province, City, Postal Code, Phone, Fax, Mobile Phone, Mobile Email, Language (a dropdown menu showing 'English (US)'), and Two Factor (a checkbox). At the bottom right of the form are 'Cancel' and 'Save' buttons.

EMAIL NOTIFICATIONS



SECURE YOUR BUSINESS AND YOUR CUSTOMERS' DATA.

Get started today!

Through your relationship with Acquire Acquiring Bank, you have been pre-registered in TrustKeeper PCI Manager - the industry's leading data security and compliance certification program. TrustKeeper PCI Manager will guide you through the [PCI DSS compliance process](#), and provide information and resources so you can get secure.

GET STARTED!


Company Name
Acquire Daily Drive (Inc)
(S)

Merchant ID
N-HKJVI331338-v111

PCI Status
INCOMPLETE

Need help?
Please contact Compliance Support, available to help 24/7x365.

1-800-363-1621 | support@trustwave.com



COMPLIANCE STATUS: INCOMPLETE

Your annual PCI certification requires attention.

According to our records, your annual PCI Self Assessment Questionnaire, or SAQ, has been started but is incomplete.

We'd like to help you get certified today. Please [log into your account](#) to address your status. If needed, you can retrieve your username or password on this page.

Helpful Tips to Complete the Process:

- Once logged in, your dashboard will display a continue button for items that you have not started yet.
- Get help along the way - click the question mark or "?" icon next to each question for more information.

LOGIN TODAY!


Company Name
test welcome 1

Merchant ID
C387JF387H439

Username
j.smith

Have you logged in and need additional help?
Please contact Compliance Support.

1-800-363-1621 | support@trustwave.com



EXPIRING SOON!

Your annual PCI certification is due soon.

The PCI Self Assessment Questionnaire for test welcome 1 will expire on **11/15/2016**.

Please [log into TrustKeeper PCI Manager](#) to review your certification. Renewing your certification today can give you peace of mind knowing that you're keeping your customer's data - and your business - secure.

LOGIN TODAY!


Company Name
test welcome 1

Merchant ID
C387JF387H439

Username
j.smith

Have you logged in and need additional help?
Please contact Compliance Support.

1-800-363-1621 | support@trustwave.com



SUCCESS!

You have completed the PCI certification for test welcome 1.

What's next?

- If your service includes vulnerability scans, please return monthly to check the status of the scan. You will receive emails when the scans are completed.
- The SAQ you submitted is valid for one year, until 11/15/2016. You will receive email reminders to renew your compliance next year.
- Your PCI status is reported to ASB Payment Solutions on your behalf.
- Please take two minutes to tell us how we're doing. Click [here](#).

Remember, securing your business is an ongoing everyday activity - not just an annual requirement. Take advantage of the education and policy tools - available within TrustKeeper PCI Manager - by logging in regularly and making changes if needed.

LOGIN TODAY!


Company Name
test welcome 1

Merchant ID
C387JF387H439

Username
j.smith

Have you logged in and need additional help?
Please contact Compliance Support.

1-800-363-1621 | support@trustwave.com



SCAN STATUS: FAILING

The vulnerability scan of test welcome 1 completed and vulnerabilities have been found.

During the scan, TrustKeeper PCI Manager identified that your network is at risk (this happens from time to time).

What's next?

- TrustKeeper PCI Manager is generating a vulnerability scan report that includes remediation advice. [Log in to your account](#) to view the scan report.
- If you have questions about the scan findings or the remediation advice, click the [Ask Support](#) button, or view the [Scanning FAQ's](#).
- Your next vulnerability scan is currently scheduled for 11/15/2016.

LOGIN TODAY!


Company Name
test welcome 1

Merchant ID
C387JF387H439

Username
j.smith

Have you logged in and need additional help?
Please contact Compliance Support.

1-800-363-1621 | support@trustwave.com



COMPLIANCE STATUS: EXPIRED

Your annual PCI certification has expired.

The PCI Self-Assessment Questionnaire for test welcome 1 expired on **11/15/2016**.

Please [log into TrustKeeper PCI Manager](#) to renew your certification. Renewing your certification today can give you peace of mind knowing that you're keeping your customer's data - and your business - secure.

LOGIN TODAY!

Company Name
test welcome 1

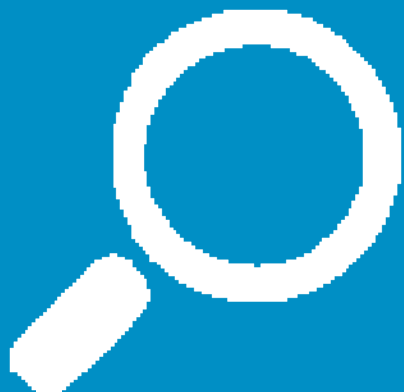
Merchant ID
C387JF387H439

Username
j.smith

Have you logged in and need additional help?
Please contact Compliance Support.

1-800-363-1621 | support@trustwave.com

 **Trustwave®**
Smart security on demand



GETTING STARTED WITH ENDPOINT PROTECTION



TRUSTWAVE ENDPOINT PROTECTION

Before you begin

- Trustwave Endpoint Protection Suite software works on a wide range of operating systems including but not limited to the below:
 - Microsoft Windows XP, Windows Vista, Windows 7, Windows 8/8.1, and Windows 10
 - Microsoft Windows Sever 2003, Windows Server 2008, and Windows Server 2012
- Like installing any software on your system, system administrator privileges are required in order to install Trustwave Endpoint Protection.
- Active internet connection is required to download components for installation and integration with your TrustKeeper cloud account.



WHERE TO DOWNLOAD ENDPOINT PROTECTION

Download Installer and the browser will save to your computer

The screenshot shows the Trustwave TrustKeeper Endpoint Protection dashboard. The top navigation bar includes links for PCI, messages, and store. The main content area displays a list of services and their status, along with a 'Download Installer' link. A red arrow points to the download bar at the bottom, indicating where to click to run the installer.

Services	Status	Devices	Status
Security Health Check	?	Download Installer	
Point-of-Sale Software Compliance	?		
Credit Card Data Storage	?		
Security Configuration	?		
Unauthorized Devices	?		
File Integrity Monitoring			
Security Log Monitoring			
Anti-virus Protection			
Mobile Device Security			

Total Alerts: 0

Note this example is from the Google Chrome web browser

Trustwave
Smart security on demand

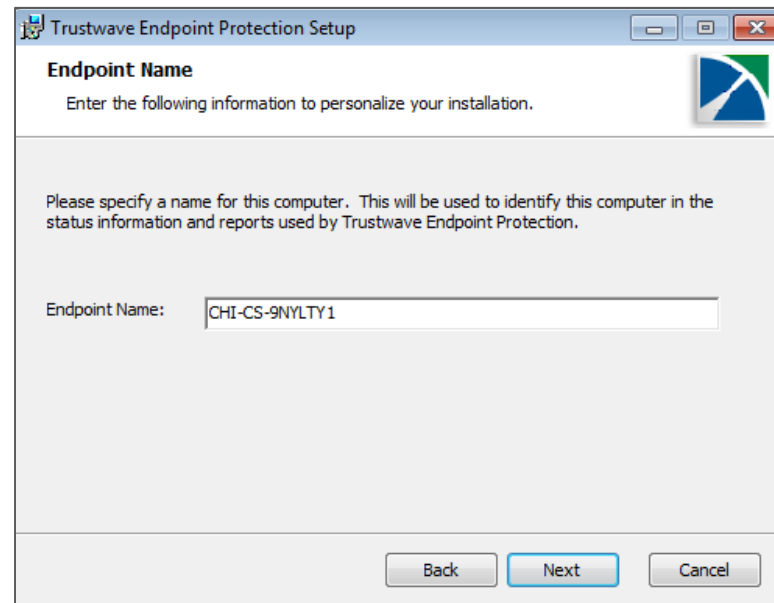
ASSIGN A NAME TO THE ENDPOINT

Give a meaningful name to this computer for easy tracking

Note:

If you have multiple payment processing locations or devices we suggest installing Endpoint Protection to each system.

For tracking purposes we advise a naming convention such as:
“Store1-POS1”, “Store1-POS2”,
“Store2-BackOfficeServer1”, etc.

A screenshot of the 'Trustwave Endpoint Protection Setup' window. The window has a title bar with the text 'Trustwave Endpoint Protection Setup' and standard Windows window controls. The main content area is titled 'Endpoint Name' and includes the instruction 'Enter the following information to personalize your installation.' Below this, a message states: 'Please specify a name for this computer. This will be used to identify this computer in the status information and reports used by Trustwave Endpoint Protection.' There is a text input field labeled 'Endpoint Name:' containing the text 'CHI-CS-9NYLTY1'. At the bottom right of the window are three buttons: 'Back', 'Next', and 'Cancel'.

ENDPOINT INTEGRATION WITH PCI MANAGER

Automatic IP target updates so you don't have to

PCI Manager

PCI Home Merchant Profile Scanning Security Policy Training Documents Trust

no system notifications

Scan Results Scan Setup

Last Completed Next Scheduled Scan Location

Add Scan Location

Name

work place

port-web-test-01

Add Scan Location

1. Please specify a name for this location (Store, etc.).

2. TrustKeeper offers three ways to identify a physical location for scanning:

☐ I am currently at this location. Use the IP address of the computer I am using ().

☒ I have one or more TrustKeeper Agents installed at this location.

Agent Selection: backOffice_Winsrvr2

☐ I will specify the IP address.

3. James Jelly Bean Store #28 has full authority to allow TrustKeeper to scan for vulnerabilities on the above location.

☐ I agree

☐ I disagree

Cancel Submit

RESOURCES

- PCI Security Standards Council:
 - www.pcisecuritystandards.org
 - List of validated payment applications, services providers, and more
 - Full version of the PCI DSS
- VISA CISP:
 - <http://www.visa.com/cisp>
- MasterCard SDP:
 - <http://www.mastercard.com/sdp>



QUESTIONS? WE ARE HERE TO HELP.

Wells Fargo Getting Started Page:

- <https://pci.trustwave.com/wellsfargo>
- Have your Merchant ID handy

Customer Support Number – TrustKeeper

- 1-800-443-9825
- WellsFargoSupport@trustwave.com



THANK YOU