2TouchPOS 3.03

PA-DSS 2.0 Implementation Guide

Version 1.0

6/25/2014

Document Owners

Kevin Bolton

Vice President of Client Fulfillment

Xenios LLC

Table of Contents

Notice

THE INFORMATION IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. Xenios LLC MAKES NO REPRESENTATION OR WARRANTY AS TO THE ACCURACY OR THE COMPLETENESS OF THE INFORMATION CONTAINED HEREIN. YOU ACKNOWLEDGE AND AGREE THAT THIS INFORMATION IS PROVIDED TO YOU ON THE CONDITION THAT NEITHER Xenios LLC NOR ANY OF ITS AFFILIATES OR REPRESENTATIVES WILL HAVE ANY LIABILITY IN RESPECT OF, OR AS A RESULT OF, THE USE OF THIS INFORMATION. IN ADDITION, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE SOLELY RESPONSIBLE FOR MAKING YOUR OWN DECISIONS BASED ON THE INFORMATION HEREIN.

Nothing herein shall be construed as limiting or reducing your obligations to comply with any applicable laws, regulations or industry standards relating to security or otherwise including, but not limited to, PA-DSS and DSS.

The retailer may undertake activities that may affect compliance. For this reason, Xenios LLC is required to be specific to only the standard software provided by it.

About this Document

This document describes the steps that must be followed in order for your 2TouchPOS installations to comply with Payment Application – Data Security Standards (PA-DSS). The information in this document is based on PCI Security Standards Council Payment Application Data Security Standards program (version 2.0 dated October, 2010).

Xenios LLC instructs and advises its customers to deploy Xenios LLC applications in a manner that adheres to the PCI Data Security Standard (v2.0). Subsequent to this, best practices and hardening methods, such as those referenced by the Center for Internet Security (CIS) and their various "Benchmarks", should be followed in order to enhance system logging, reduce the chance of intrusion and increase the ability to detect intrusion, as well as other general recommendations to secure networking environments. Such methods include, but are not limited to, enabling operating system auditing subsystems, system logging of individual servers to a centralized logging server, the disabling of infrequently-used or frequently vulnerable networking protocols and the implementation of certificate-based protocols for access to servers by users and vendors.

You must follow the steps outlined in this *Implementation Guide* in order for your 2TouchPOS installation to support your PCI DSS compliance efforts.

Revision Information

Name	Title	Date of Update	Summary of Changes
Kevin Bolton	VP of Client Fulfillment	2/24/2014	Document Creation
Kevin Bolton	VP of Client Fulfillment	2/24/2014	Added information to the application summary table.
Kevin Bolton	VP of Client Fulfillment	2/25/2014	Updated Versioning Methodology

Note: This PA-DSS Implementation Guide must be reviewed on a yearly basis, whenever the underlying application changes or whenever the PA-DSS requirements change. Updates should be tracked and reasonable accommodations should be made to distribute or make the updated guide available to users. Xenios LLC will distribute the IG to new customers via a downloadable document on our website.

Executive Summary

Payment Application 2TouchPOS has been PA-DSS (Payment Application Data Security Standard) certified, with PA-DSS Version 2.0. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):

Coalfire Systems, Inc. 361 Centennial Parkway Suite 150 Louisville, CO 80027	Coalfire Systems, Inc. 1633 Westlake Avenue N. Suite 100 Seattle, WA 98109

This document also explains the Payment Card Industry (PCI) initiative and the Payment Application Data Security Standard (PA-DSS) guidelines. The document then provides specific installation, configuration, and ongoing management best practices for using Payment Application as a PA-DSS validated Application operating in a PCI Compliant environment.

PCI Security Standards Council Reference Documents

The following documents provide additional detail surrounding the PCI SSC and related security programs (PA-DSS, PCI DSS, etc):

- Payment Applications Data Security Standard (PA-DSS)
  https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml
- Payment Card Industry Data Security Standard (PCI DSS)
  https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- Open Web Application Security Project (OWASP)
  http://www.owasp.org

Application Summary

Payment Application Name:	2TouchPOS
Payment Application Version:	3.03
Application Description:	The 2TouchPOS application is a POS system designed to run in a networked merchant environment in a client-server fashion. One or more POS applications are installed on a local network segment. If only a single POS system is implemented, it runs all the software including MS SQL Server. In a multi-POS system one of the POS stations is designated as the "base" system which serves system wide services such as the database. The other POS clients then access the centralized services over the local network.

	The 2TouchPOS application is integrated with both Midnite Express' Slipstream Payment Application and Mercury's DSIClient (with Mercury Payment System's back-end) for credit card processing. All credit card functionality is modularized in a single program and all transaction requests are queued in a separate queuing agent which handles the interface to the credit card processing APIs. The system is built with VB6, OCX Controls, VB.Net, and C#.Net. 2TouchPOS accepts card present and card not present payment channels. 2TouchPOS transmits and stores cardholder data using 3DES encryption. Stored cardholder data is retained for 45 days. 2TouchPOS is sold directly to the end user by Xenios LLC or one of its dealers. The end customer purchases licenses to run 2TouchPOS. 2TouchPOS is comprised of core functionality and add-on modules. The customer must purchase the credit card integration module to accept credit card payments. 2TouchPOS is a standalone system and not part of an application suite.
Typical Role of Application:	The 2Touch POS application is targeted at the hospitality market and is typically implemented in restaurants, bars, and nightclubs. Payments from guests are processed through 2TouchPOS. Credit cards are typically swiped through the mag reader at the time of payment. Credit card information can be swiped earlier and affiliated with a tab. 2TouchPOS uses either Slipstream Batch Manager or DataCap DSIClientX depending on the customer's credit card processor. One of these two payment applications is required to process credit cards. In both cases, 2TouchPOS makes payment requests to and receives confirmation from the appropriate payment application.
Components of Application Suite (i.e. POS, Back Office, etc.)	• 2TouchPOS.exe: Primary POS application, deployed on all POS terminals • SQL Server: Base Station only • Slipstream Batch Manager as needed • DataCap DSIClientX as needed
Required Third Party Payment Application Software:	• Midnite Express' Slipstream Payment Application version 4.5 • Mercury's DSIClient version 2.50.3862
Database Software Supported:	Microsoft SQL Server 2008 R2
Other Required Third Party Software:	Microsoft .Net Framework v4
Operating System(s) Supported:	The latest supported versions of: • Windows Server 2008 64-bit • Windows 7 Pro 64-bit

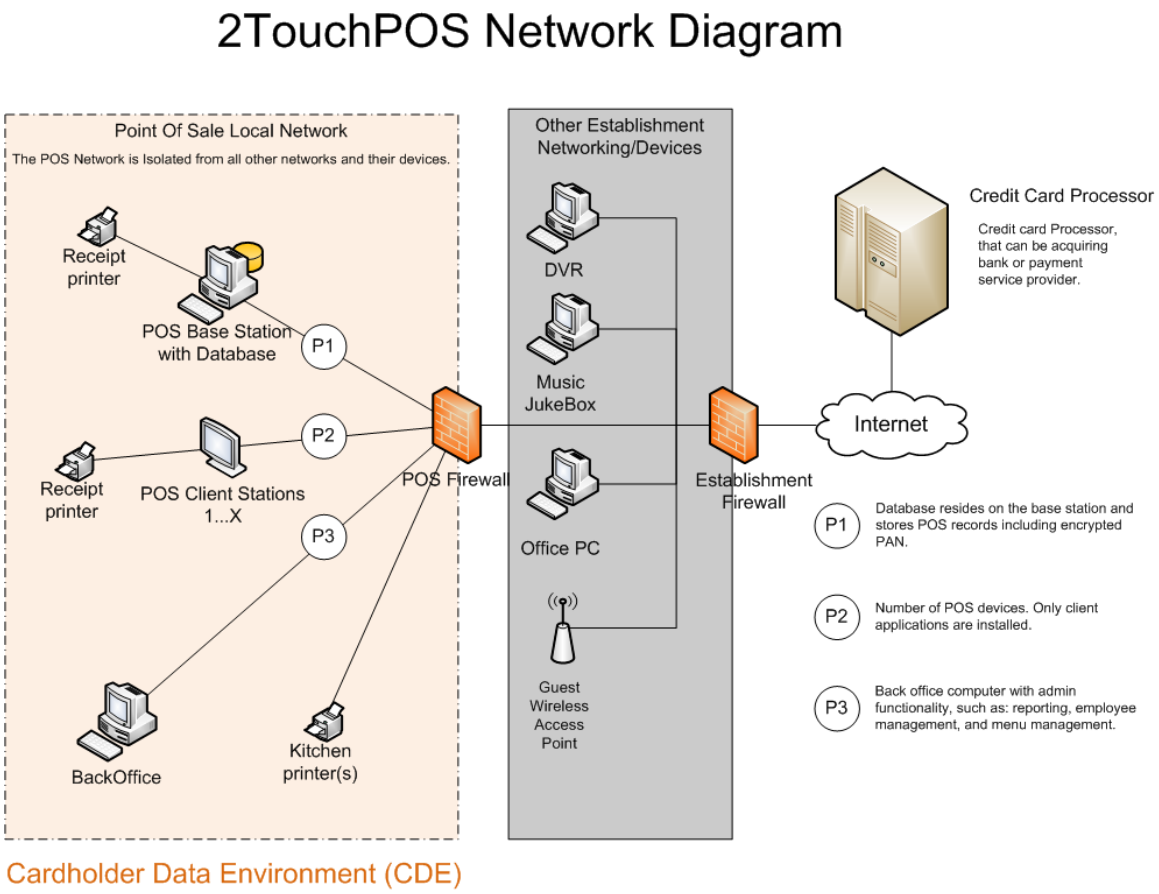
<table>
<tr><td>Application Functionality Supported</td><td>Select one or more from the following list:<table>
<tr><td>☒</td><td>POS Suite</td><td>☒</td><td>POS Admin</td><td>☐</td><td>Shopping Cart & Store Front</td></tr>
<tr><td>☐</td><td>POS Face-To-Face</td><td>☐</td><td>Payment Middleware</td><td>☐</td><td rowspan="3">Others (Please Specify):</td></tr>
<tr><td>☐</td><td>POS Kiosk</td><td>☐</td><td colspan="2">Payment Back Office</td></tr>
<tr><td>☐</td><td>POS Specialized</td><td>☐</td><td colspan="2">Payment Gateway/Switch</td></tr>
</table></td></tr>
<tr><td>Payment Processing Connections:</td><td>Credit card data is entered at a terminal running 2TouchPOS. 2TouchPOS passes the credit card data to the payment queue running on the base station. The payment queue in turn makes request to either the DSIClientX or Slipstream Batch Manager depending on the customer’s configuration. The payment queue returns the authorization data back to the 2TouchPOS terminal when it is received from the DSIClientX or Slipstream Batch Manager.</td></tr>
<tr><td>Application Authentication</td><td>Access to sensitive data is protected through unique usernames and passwords. Sensitive data is 3DES encoded when transmitted and when stored. Secure connections are used when communicating over public networks.</td></tr>
<tr><td>Application Encryption</td><td>2TouchPOS uses 3DES encryption at the application level encryption. The encryption key is generated for each transaction and not reused.</td></tr>
<tr><td>Description of Versioning Methodology:</td><td>2TOUCHPOS versioning has two levels, Major and Minor Number.
Major changes include significant changes to the application and would have an impact on PA-DSS requirements.
Minor changes include small changes such as minor enhancements and may or may not have an impact on PA-DSS requirements.</td></tr>
<tr><td>Payment Application Assessment Environment</td><td>The payment application was assessed in Coalfire’s lab and included 2TouchPOS 3.03 and Microsoft SQL Server 2008 R2.

The first system was a single base station running on Microsoft Server 2008 R2 and using Slipstream Batch Manager for credit card processing.

The second system was a base station with a client station. Both systems are running Microsoft Windows 7 SP 1 and configured to use the DSIClientX for credit card processing.</td></tr>
<tr><td>List of Resellers/Integrators (If Applicable):</td><td>Xenios LLC maintains a dealer program. Dealers sell, install, support, and upgrade 2TouchPOS.</td></tr>
<tr><td>Stored Cardholder Data:</td><td>The following tables hold encrypted cardholder data. All but tblOpenTab also hold authorization data
tblCCCredit
tblCustAcctDaily
tblOpenTab
tblOpenTabPmnts
tblSalesDailyPmnts
tblSalesHistPmnts
tblDeliveryPmnts
tblCCPreAuth
tblCCPreAuthHist
tblCCVoidDaily
tblCCVoidHist
tblVIPCards</td></tr>
</table>

	• tblCCSaleDaily • tblCCSaleHist
Access to cardholder data is logged:	2TouchPOS maintains a facility called the Secure Event Log. Access to cardholder data is logged by this facility.

Typical Network Implementation



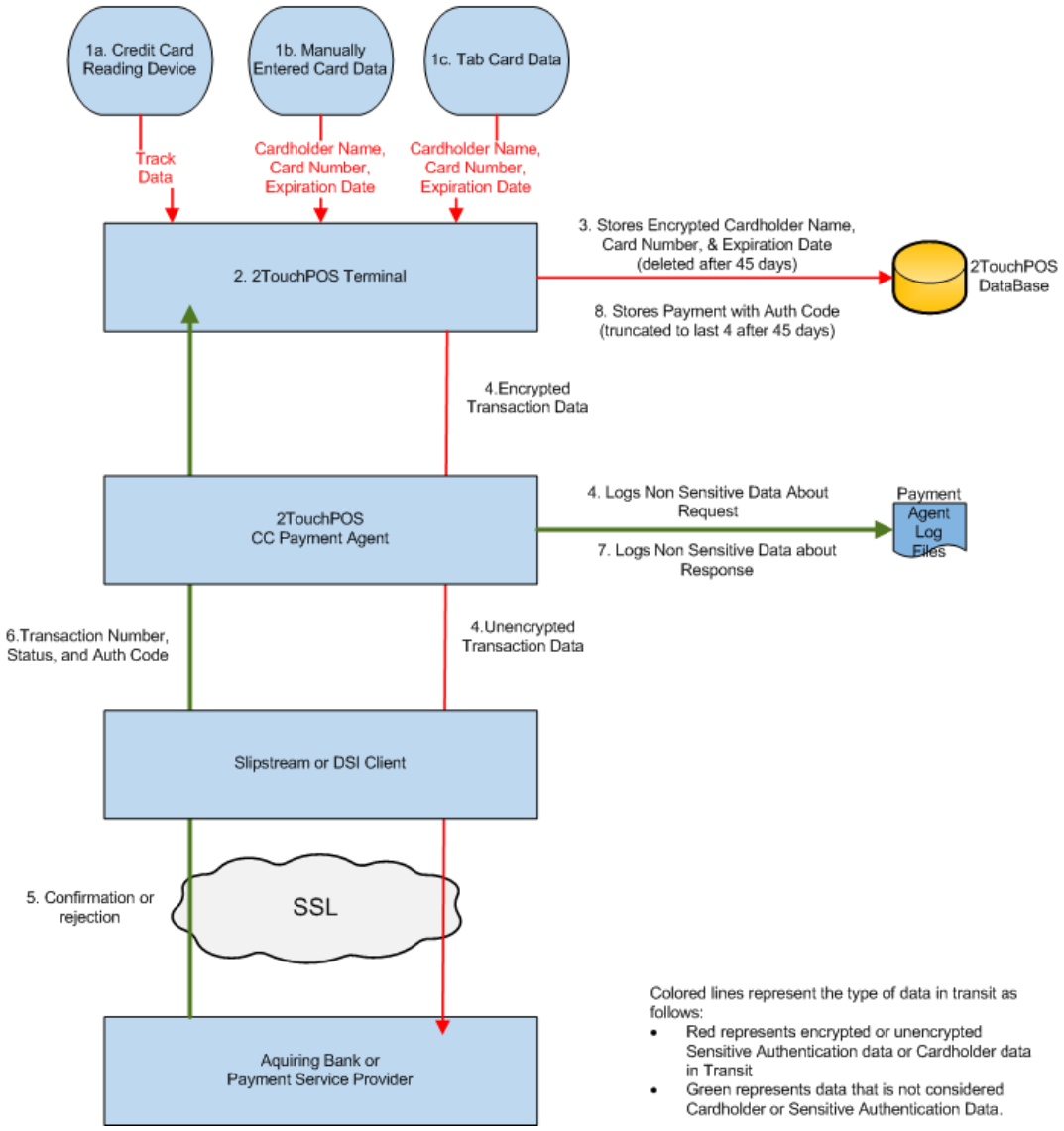
Cardholder Data Environment (CDE)

Dataflow Diagram

Dataflow When Credit Card is present at time of Payment

Simple Payment Data Flow Diagram

This is the Data Flow Diagram for processing a payment directly from the customers credit card at the time the card is presented or captured against a tab.



Difference between PCI Compliance and PA-DSS Validation

As a software vendor, our responsibility is to be "PA-DSS Validated."

We have performed an assessment and certification compliance review with our independent assessment firm, to ensure that our platform does conform to industry best practices when handling, managing and storing payment related information.

PA-DSS is the standard against which Payment Application has been tested, assessed, and validated.

PCI Compliance is then later obtained by the merchant, and is an assessment of your actual server (or hosting) environment.

Obtaining "PCI Compliance" is the responsibility of the merchant and your hosting provider, working together, using PCI compliant server architecture with proper hardware & software configurations and access control procedures.

The PA-DSS Validation is intended to ensure that the Payment Application will help you achieve and maintain PCI Compliance with respect to how Payment Application handles user accounts, passwords, encryption, and other payment data related information.

The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the DSS apply to all members, merchants, and service providers that store, process or transmit cardholder data.

The PCI DSS requirements apply to all system components within the payment application environment which is defined as any network device, host, or application included in, or connected to, a network segment where cardholder data is stored, processed or transmitted.

The 12 Requirements of the PCI DSS:

Build and Maintain a Secure Network

1. *Install and maintain a firewall configuration to protect data*
2. *Do not use vendor-supplied defaults for system passwords and other security parameters*

Protect Cardholder Data

3. *Protect Stored Data*
4. *Encrypt transmission of cardholder data and sensitive information across public networks*

Maintain a Vulnerability Management Program

5. *Use and regularly update anti-virus software*
6. *Develop and maintain secure systems and applications*

Implement Strong Access Control Measures

7. *Restrict access to data by business need-to-know*
8. *Assign a unique ID to each person with computer access*
9. *Restrict physical access to cardholder data*

Regularly Monitor and Test Networks

10. *Track and monitor all access to network resources and cardholder data*

11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

Considerations for the Implementation of Payment Application in a PCI-Compliant Environment

The following areas must be considered for proper implementation in a PCI-Compliant environment.

- Sensitive Authentication Data requires special handling
- Remove Historical Cardholder Data
- Set up Good Access Controls
- Properly Train and Monitor Admin Personnel
- Key Management Roles & Responsibilities
- PCI-Compliant Remote Access
- Use SSH, VPN, or SSLV3/TLS 1.0 or higher for encryption of administrative access
- Log settings must be compliant
- PCI-Compliant Wireless settings
- Data Transport Encryption
- PCI-Compliant Use of Email
- Network Segmentation
- Never store cardholder data on internet-accessible systems
- Use SSLV3 for Secure Data Transmission
- Delivery of Updates in a PCI Compliant Fashion

Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4.a)

- 2TouchPOS 2.12.0057 and earlier stored sensitive authentication data unencrypted.
- 2TouchPOS 2.12.0058 stored sensitive authentication data encrypted
- 2TouchPOS 3.01.0054 no longer stores sensitive authentication data and changes to 3DES encryption.

When you upgrade from a non-PCI compliant version of 2TouchPOS to a PCI compliant version of 2TouchPOS, the update process will purge any sensitive credit card data older than 12 months. All remaining data will be re-encrypted using current PCI-compliant encryption standards.

The following files that need to be securely removed are listed below. Note that some of these files may not be present on all systems depending on the configuration.

"Application Path" in the following table refers to the installation folder. The default installation folders are

- C:\Program Files\BarTouch
- C:\Program Files\TwoTouch
- C:\TwoTouch

Type	Name	Possible Locations	Directions
File	Backup.zip	• ApplicationPath • ApplicationPath\Public\Backup	Delete file

File	Backup.msde	• ApplicationPath • ApplicationPath\Public\Backup	Delete file
Directory	Queue	• ApplicationPath	Delete Entire Directory
File	UserX.inp	• C:\Program Files\Active-Charge\	Delete File and Empty Recycle Bin

If you do not currently use a secure delete tool, you can use one of the following:

- Heidi Eraser can be obtained from http://www.heidi.ie/eraser/
- Microsoft SDelete can be obtained from http://technet.microsoft.com/en-us/sysinternals/bb897443

Sensitive Authentication Data requires special handling (PA-DSS 1.1.5.c)

Xenios LLC does not store Sensitive Authentication data for any reason, and we strongly recommend that you do not do this either.

Purging of Cardholder Data (PA-DSS 2.1)

The following guidelines must be followed when dealing with cardholder data (PAN (primary account number) alone or with any of the following: expiry date, cardholder name or service code):

Cardholder data is kept encrypted in the database. The full cardholder data is retained for 45 days to allow reasonable opportunity to correct payments. Full cardholder data older than 45 days is automatically deleted from the database.

Encrypted cardholder data is also in database backups. We store database backups in several locations.

- The base station and client stations will contain at least the most current backup. It can be configured to keep a number of historical backups. The backups are stored in the 2TouchPOS application directory and the public\backups subdirectory.
- A copy of the current database backup is stored on a thumb drive on the base station.

The backups need to be securely deleted when a station or thumb drive is removed from the system. The backup locations are the same as those listed in the "Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4.a)" section.

Cardholder is in memory at the time of the transaction and windows could choose that point in time to swap the data into the page file. For this reason, the page file must be encrypted. The following commands can be used to check your page file and turn on encryption. Both commands require you run a CMD window as administrator.

1. Run the following command to check the status of your page file
   fsutil behavior query EncryptPagingFile
   A value of 0 means the page file is not encrypted.
2. Run the following command to turn on page file encryption
   fsutil behavior set EncryptPagingFile 1

Cardholder Data Encryption Key Management (PA-DSS 2.5.c and 2.6.a)

2TouchPOS uses 3DES encryption at the application level encryption. The encryption key is generated for each transaction and not reused.

The algorithm to generate the key is maintained in source control. Access to the source control project is limited to essential developers only.

Removal of Cryptographic material (PA-DSS 2.7.a)

Data encrypted in previous versions of 2TouchPOS are re-encrypted based on the new algorithm. Removal of encrypted data is as in the section 'Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4.a)'.

To remove the executables with the algorithm, you would additionally delete the following.

Type	Name	Possible Locations	Directions
Directory	<Application Path>	• C:\Program Files\BarTouch • C:\Program Files\TwoTouch • C:\TwoTouch	Delete Directory, Subdirectories, and Files

Set up Strong Access Controls (3.1.a and 3.2)

The PCI DSS requires that access to all systems in the payment processing environment be protected through use of unique users and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of generic group accounts used by more than one user or process.

Access to payment processing data in 2TouchPOS is protected by the basic permission system as well as a unique username and password system. 2TouchPOS provides an application level username and password facility that enforces the following:

1. The application must assign unique IDs for user accounts. (8.1)
2. The application must provide at least one of the following three methods to authenticate users: (8.2) 2TouchPOS requires a password.
    a. Something you know, such as a password or passphrase
    b. Something you have, such as a token device or smart card
    c. Something you are, such as a biometric
3. The application must NOT require or use any group, shared, or generic accounts or passwords.(8.5.8)
4. The application requires passwords to be changed at least every 90 days (8.5.9)
5. The application requires passwords must to be at least 7 characters (8.5.10)
6. The application requires passwords to include both numeric and alphabetic characters (8.5.11)
7. The application keeps password history and requires that a new password is different than any of the last four passwords used. (8.5.12)
8. The application limits repeated access attempts by locking out the user account after not more than six logon attempts. (8.5.13)

9. The application sets the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. (8.5.14)
10. The application requires the user to re-authenticate to re-activate the session if the application session has been idle for more than 15 minutes.

3.1.a: You must assign strong passwords to any default accounts (even if they won't be used), and then disable or do not use the accounts.

2TouchPOS does not have any default accounts.

3.2: Control access, via unique username and PCI DSS-compliant complex passwords, to any PCs or servers with payment applications and to databases storing cardholder data.

Access to PCs or servers at the operating system or file system level is prohibited.

Properly Train and Monitor Admin Personnel

It is your responsibility to institute proper personnel management techniques for allowing admin user access to cardholder data, site data, etc. You can control whether each individual admin user can see credit card PAN (or only last 4).

In most systems, a security breach is the result of unethical personnel. So pay special attention to whom you trust into your admin site and who you allow to view full decrypted and unmasked payment information.

Log settings must be compliant (PA-DSS 4.1.b, 4.4.b)

4.1.b: 2TouchPOS has PA-DSS compliant logging enabled by default. This logging is not configurable and may not be disabled. Disabling or subverting the logging function of 2TouchPOS in any way will result in non-compliance with PCI DSS.

Credit card logging is limited to the last 4 digits of credit card numbers.

4.4.b: 2TouchPOS logs to the Windows Event Log, log files, and to its database. 2TouchPOS configures all event logs automatically. All three of these sources could be exported to a centralized logging service.

Services and Protocols (PA-DSS 5.4.c)

2TouchPOS

- HTTPS
- SFTP
-

Third Party Products

- DataCaps DSIClientX

- HTTPS.

- Midnite Express Slipstream Batch Manager
  - HTTPS

PCI-Compliant Wireless settings (PA-DSS 6.1.f and 6.2.b)

2TouchPOS can be run in a wireless network. The customer is required to ensure the wireless network has been deployed in a manner that is PCI compliant.

2.1.1: Change wireless vendor defaults per the following 5 points:

1. Encryption keys must be changed from default at installation, and must be changed anytime anyone with knowledge of the keys leaves the company or changes positions.
2. Default SNMP community strings on wireless devices must be changed.
3. Default passwords/passphrases on access points must be changed.
4. Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks.
5. Other security-related wireless vendor defaults, if applicable, must be changed.

1.2.3: Perimeter firewalls must be installed between any wireless networks and systems that store cardholder data, and these firewalls must deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

Accessing 2TouchPOS via Microsoft Remote Desktop access requires the use of an encrypted remote desktop session. The following ports must be open.

- Ports 3389 Protocol TCP

The following ports must be opened when running a 2TouchPOS client on a wireless device.

- Ports 49152-49156 Protocol TCP
- Port 5657 Protocol UDP
- Port 5757 Protocol TCP
- Port 80 Protocol TCP
- Port 8080 Protocol TCP
- Ports 135-139, 445 Protocol TCP
- Ports 135-139, 445 Protocol UDP
- Port 5040 Protocol TCP

- Port 1434 Protocol UDP

4.1.1: Industry best practices (for example, IEEE 802.11.i) must be used to implement strong encryption for authentication and transmission of cardholder data.
Note: The use of WEP as a security control was prohibited as of June 30, 2010.

Never store cardholder data on internet-accessible systems (PA-DSS 9.1.b)

2TouchPOS must be deployed behind a firewall. The firewall must not allow any outside traffic into the cardholder data environment.

PCI-Compliant Remote Access (10.2)

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism. The means two of the following three authentication methods must be used:

1. Something you know, such as a password or passphrase
2. Something you have, such as a token device or smart card
3. Something you are, such as a biometric

Remote access to the 2TouchPOS is only available to 2TouchPOS employees and then only through LogMeIn's LogMeInRescue product. Employees must provide their username and password to access the LogMeInRescue client. Connections into the CDE are initiated and confirmed by personnel at the establishment. LogMeInRescue uses end-to-end, 256-bit SSL encryption.

PCI-Compliant Delivery of Updates (PA-DSS 10.3.1)

2TouchPOS updates are securely delivered.

1. The 2TouchPOS application contacts a 2TouchPOS server over an SSL connection. The application downloads a zip file containing the new applications files for the requested version.

2. The 2TouchPOS application obtains a list of files and MD5 hash values for the requested version over an SSL connection from the 2TOuchPOS server.

3. 3. The 2TouchPOS unzips the zip file with the new application files, and computes MD5 hash values for the files.

4. 4. The 2TouchPOS application compares the computed hash values with the values that were downloaded in step 2. If the files match the files are deployed to the appropriate place in the directory structure. If they do not match the files are not deployed and the user is alerted.

Once we identify a relevant vulnerability, we work to develop and test a patch that helps protect the 2TouchPOS application against the specific, new vulnerability. We attempt to publish a

patch within 10 days of the identification of the vulnerability. We will then contact vendors and dealers to encourage them to install the patch. Typically, merchants are expected to respond quickly to and install available patches within 30 days.

Delivery of patched code is delivered as a version upgrade through the process outlined above.

Version upgrades are delivered over an HTTPS connection.

Update integrity is verified using MD5 Hash comparison.

Updates are initiated by technicians through the remote access methods above. LogMeInRescue sessions are deactivated on disconnect.

A firewall product must be used to secure these "always-on" connections.

PCI-Compliant Remote Access (10.3.2.b)

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism (username/ password and an additional authentication item such as a token or certificate).

In the case of vendor remote access accounts, in addition to the standard access controls, vendor accounts should only be active while access is required to provide service. Access rights should include only the access rights required for the service rendered, and should be robustly audited.

If users and hosts within the payment application environment may need to use third-party remote access software such as Remote Desktop (RDP), Terminal Server, PCAnywhere, etc. to access other hosts within the payment processing environment, special care must be taken.

In order to be compliant, every such session must be encrypted with at least 128-bit encryption (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment). Additionally, the PCI user account and password requirements will apply to these access methods as well.

When requesting support from a vendor, reseller, or integrator, customers are advised to take the following precautions:

- Change default settings (such as usernames and passwords) on remote access software (e.g. VNC)
- Allow connections only from specific IP and/or MAC addresses
- Use strong authentication and complex passwords for logins according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS 8.1, 8.3, and 8.5.8-8.5.15
- Enable encrypted data transmission according to PA-DSS 12.1 and PCI DSS 4.1
- Enable account lockouts after a certain number of failed login attempts according to PA-DSS 3.1.8 and PCI DSS 8.5.13
- Require that remote access take place over a VPN via a firewall as opposed to allowing connections directly from the internet

- Enable logging for auditing purposes
- Restrict access to customer passwords to authorized reseller/integrator personnel.
- Establish customer passwords according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

Data Transport Encryption (PA-DSS 11.1.b)

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128 bit encryption strength (either at the transport layer with SSLV3 or IPSEC; or at the data layer with algorithms such as RSA or Triple-DES) to safeguard cardholder data during transmission over public networks (this includes the Internet and Internet accessible DMZ network segments).

PCI DSS requirement 4.1: Use strong cryptography and security protocols such as secure sockets layer (SSLV3) / transport layer security (TLS 1.0 or higher) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

Examples of open, public networks that are in scope of the PCI DSS are:

- The Internet
- Wireless technologies
- Global System for Mobile Communications (GSM)
- General Packet Radio Service (GPRS)

Refer to the Dataflow diagram for an understanding of the flow of encrypted data associated with 2TouchPOS.

PCI-Compliant Use of End User Messaging Technologies (PA-DSS 11.2.b)

2TouchPOS does not allow or facilitate the sending of PANs via any end user messaging technology (for example, e-mail, instant messaging, and chat).

Non-console administration (PA-DSS 12.1)

Although 2TouchPOS does not support non-console administration and we do not recommend using non-console administration, should you ever choose to do this, must use SSH, VPN, or SSLV3/TLS 1.0 or higher for encryption of this non-console administrative access.

Network Segmentation

The PCI DSS requires that firewall services be used (with NAT or PAT) to segment network segments into logical security domains based on the environmental needs for internet access. Traditionally, this corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming internet traffic to the trusted application environment can be allowed. Additionally, outbound internet access from the trusted segment must be limited to required and justified ports and services.

- Refer to the standardized Network diagram for an understanding of the flow of encrypted data associated with 2TouchPOS.

Maintain an Information Security Program

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data.

The following is a very basic plan every merchant/service provider should adopt in developing and implementing a security policy and program:

- Read the PCI DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
- Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
- Create an action plan for on-going compliance and assessment.
- Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self Assessment Questionnaire.
- Call in outside experts as needed.

Application System Configuration

Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PCI DSS compliance.

- Windows 7 Professional 64-bit, All latest updates and hot-fixes should be tested and applied.
- Windows 2008 Server 64-bit, All latest updates and hot-fixes should be tested and applied.
- 512 MB Ram minimum, 1GB or higher is recommended
- 50MB of available hard disk space
- TCP/IP network connectivity
- SQL Server 2008 R2, All latest updates and hot-fixes should be tested and applied.

Payment Application Initial Setup & Configuration

2TouchPOS and payment third party software is only installed by a 2TouchPOS technician. A test credit card transaction is performed following the configuration of credit card parameters and version upgrades.