CHARGE Anywhere®
4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

QuickSale for Windows
Version 2.2.*.*
Secure Payment Solutions
Client Implementation Document
PA-DSS 3.2

Last Revision: 12/27/2016

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

Revision #	Date	Name	Description
1	11/08/07	CP	Added sections 13 and 14
2	11/12/07	CP	Updated section 12 to include recommendations for browser security.
3	11/15/07	CP	Reviewed all sections
4	11/20/07	CP	Updated section 12 and added section 15
5	11/30/07	CP	Updated section 12 to include Storage card information
6	1/15/08	CP	Added section regarding key rotation and troubleshooting procedures
7	3/17/08	CP	Removed sections that are no longer relevant
8	5/02/08	CP	Modified the section related to WiFi configuration
9	6/04/08	CP	Added wording regarding upgrades.
10	11/24/08	CP	Updated uninstall section for J2ME device
11	3/18/09	CP	Added the User Management section
12	1/29/10	TS	Added Uninstall procedure for Blackberry and Android
13	5/11/10	AL	Added Uninstall procedure for Brew, extra requirements for PA-DSS
14	9/07/10	CP	Added uninstall procedures for iPhone
15	9/30/10	CP	Added screen lock procedures for iPhone
16	10/15/10	TS	Added User Management for QuickBooks.
17	09/30/13	TS	Review and Edit for PA-DDSS 2.0
18	11/18/13	CP	Edits for PA-DSS 2.0
19	12/31/13	CP	Additional Edits for PA-DSS 2.0
20	01/03/14	CP	Additional Edits for PA-DSS 2.0
21	4/1/14	CP	Added Customer Database Section
22	6/11/14	CP	Added Card Protection Steps for QB
23	6/12/14	CP	Accepted PA-DSS changes
24	12/8/16	VV	Updated password security, Added Application Registration, Updated Key generation section, Update Secure Storage with database information, Added Supported Platform, Added Information Section, Added section implementation guide
25	1/3/16	TS	Application Versioning, Document Formatting, Update of several PA-DSS Requirements.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

CHARGE Anywhere®
4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

WARNING: If all recommendations in this guide are not followed the application will not be PA-DSS compliant.

CHARGE Anywhere®
4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

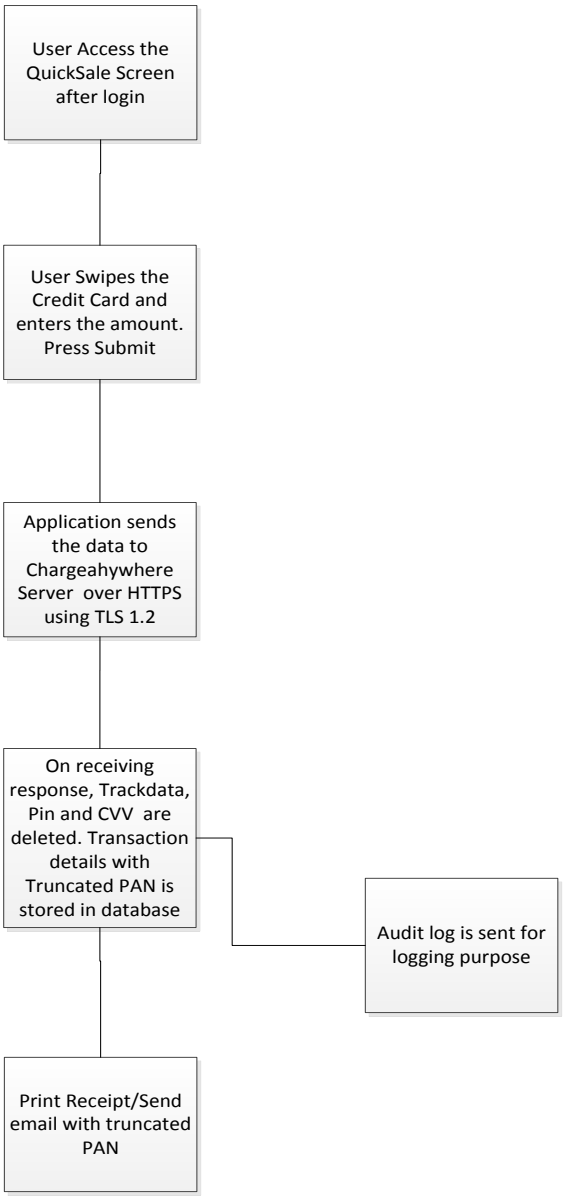
About this Document

This document describes the steps that must be followed in order for your QuickSale installation to comply with the 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 3.2 dated October, 2016).

QuickSale for Windows is desktop application used to process Credit card and Debit card payments.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

1. **Data Flow through QuickSale**



4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

2. **Secure Deletion of Sensitive Data**

(PA-DSS Req 1.1)

Secure Deletion on Windows (prior to uninstall)

Download sdelete from Microsoft's website here: http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx

1. From a command prompt, navigate to the QuickSale for Windows install directory, typically C:\QuickSale For Windows\
2. Run the command: sdelete –p 3 userInformation.dat
3. Run the command: sdelete –p 3 comstarpos.mdb
4. Run the command: sdelete –p 3 config\config.dat
5. To ensure that free space on drive c: is wiped clean, run the command: sdelete –c c:

ChargeAnywhere does not collect sensitive data or PAN on consumer systems for debugging or troubleshooting.
Debugging/troubleshooting is performed locally to reproduce the problem.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

3. **Secure Storage of Sensitive Data**

(PA-DSS Req 2.2)
All transaction attempts, successful or not, are logged.

Transactions are stored in password protected database.

PAN stored is masked and contains only the first 6 and last 4 by default, and there is no way to unmask the PAN.

The masking of the account number is in accordance with PA-DSS requirement 2.2

PAN displayed is masked to show only last four on receipts, QuickSale Customer Profile and Reports screen.
In case of manual entry on Quick Sale screen, the card number is masked once the valid Cardnumber is entered. Also CVV is masked once a valid CVV length is entered. (PA-DSS requirement 2.3)

Application does not retain track data, card verification code or PIN block data

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

4. **Card Holder Data retention.**
(PA-DSS Req 2.1)

All our application rotates data daily. All cardholder data is moved automatically at day end to the next day archive log. There are 3 archive logs in the application, after day 4 the, archive 3 is purged. The merchant also has the ability to purge all this data from the application manually from the maintenance menu by choosing, rotate logs.

For the Customer Database, the merchant has the option to delete any profiles that have not been used for a certain period of time. The typical workflow for deleting a customer profiles is as follows:

1. Access the Customer Database Screen
2. Select the filtering option for Last Used
3. Choose the cutoff date for the Last Used value
4. Perform Search
5. Delete the desired profiles

All data is stored in a Database at the following location:
C:\CHARGE Anywhere\QuickSale for Windows\comstarpos.mdb

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

5. **Pan protection at rest**
(PA-DSS Req 2.3)

PAN is stored in the database encrypted using AES-256. It is as such rendered unreadable.

The application at installation creates the necessary keys to manage the encryption process and the merchant does not need to perform any task to ensure that the process is in place.

All data is stored in a Database at the following location:
C:\CHARGE Anywhere\QuickSale for Windows\comstarpos.mdb

PAN is never available in the Database or any other part of the application, inside or outside in clear. Any backup will only contain encrypted PAN.

Debugging Logs **DO NOT** contain any clear PANs.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

6. **Key Maintenance**
(PA-DSS Req 2.4)

There are no physical keys for these app, all keys are dynamic. Generation and destruction is a function of the application.

DEK and KEK are generated dynamically when user Account is created for the first time. DEK is encrypted with KEK with complex algorithm and stored in password protected database. (PA-DSS Req 2.5)

Keys are automatically generated by the application when the admin use is created. (PA-DSS Req 2.5.1)

No Interaction is required by the user to create, manage and distribute keys, the application, generates all keys and is responsible for all aspects of key management including distribution of keys. (PA-DSS Req 2.5.2)

DEK is stored in the Database securely encrypted, while KEK is dynamically generated every time from and mask and Entropy stored in a file located at:
C:\CHARGE Anywhere\QuickSale for Windows\config\config.dat
(PA-DSS Req 2.5.3)

Required and enforced crypto period is one year. The merchant can perform a key rotation from the maintenance menu. It is recommended to perform key rotation more often, and/or any time a compromise is suspected. (PA-DSS Req 2.5.4)

Keys can be retired or replaced as deemed necessary when the integrity of the key has been weakened or keys are suspected of being compromised using the key rotation process below. (PA-DSS Req 2.5.5)

Keys are fuly managed by the app and no peson has access to the keys, and as such Split knowledge and dual control for any manual clear-text cryptographic key-management operations is not applicable. (PA-DSS Req 2.5.6)

Key generation process and management by the application prevents of unauthorized substitution of cryptographic keys. (PA-DSS Req 2.5.7)

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

7. **Key rotation Process:**
(PA-DSS Req 2.6)

- Launch the application
- Enter the required password
- Select Maintenance from the Main Screen
- Enter the required password
- Select Rotate KEK
- Select Rotate Keys

Suggested Key Rotation Period

Keys should be rotated periodically. CHARGE Anywhere suggests the following crypto period for encryption keys.

Key	Rotation Schedule
Key Encryption Key(KEK)	Every year
Data Encryption Key(DEK)	Every year

The key rotation process creates new Keys and destroys the old ones, rendering them irretrievable. Merchant must use the above process to rotate data whenever the crypto period is reached, or when ther integrity of the key has been weakened or keys are suspected of being compromised using the key rotation process below. The key rotation process takes care of
re-encrypting historic data with new keys.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

8. Compromised Key Procedures
(PA-DSS Req 2.5.5)

In the event that the merchant suspects or knows that their key has been compromised, a key rotation must be performed immediately to prevent the disclosure of sensitive data. To rotate the keys, follow the steps that are detailed in the section labeled Key Maintenance.

Clients are advised to have latest security updates installed on the machine hardware as recommended by PA-DSS.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

9. **Secure authentication of Application**
(PA-DSS Req 3.1)

When the application is first installed, the user must provide the password for the default user admin. This is the highest level user, and its session will expire after 15 minutes. It is strongly recommended that a low level user is immediately created. If a function requires admin level, the low level user should see his manager for a password override, if applicable. Passwords expire every **90** days and the user is required to change them. User cannot reuse any one of the last 4 passwords. User ID is unique in the application.

User passwords are secured with strong cryptography hash algorithm with salt.

Application uses strong password policy described below.

Password Policy:
- Password has to be at least 8 alphanumeric characters
- Password must have digits
- Password must have both upper and lower case letters
- Symbols are recommended but not required

The application contains the means to recover password by integrating a security phrase that is created by the user.

Every time user restarts the device and enters the application, the application will inform the user if he is using default/expired passwords. It is the responsibly of the user to immediately change the default passwords, and to changes the expired passwords.

Please note that when you are entering the password, you will be able to see what you are entering however, when you are entering the password on any other screen, your password will be masked (you will see asterisks).

Also, when you enter a screen to change a password, you will see your password since you have just entered it, so it is no secret at this point.

A user can be given permissions from **Security/Transaction Security.** These permissions can limit his access thus reducing the risk, and when necessary, a manger override will be required.

After 3 failed password attempts, the application will lock out for 30 minutes before allowing another 3 attempts. For users with admin level permission, if application is idle for 15 minutes, the application will lock out and require password for re-entry. A user can unlock his app by using the password recovery functionality. If successful, he will be required to change his password immediately.

Password can be edited from User Management Screen and the new password should also confirm to Password policy described above.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

10. **User Management(CHARGE Anywhere for Windows)**
(PA-DSS Req 3.2)

When starting the application for the first time, you will be presented with a screen to set the password on the admin account; this password should follow the guidelines of Section 7. This account is required and has access to all the functionality available within the application.

It is strongly advised that users Control access via unique usernames and PCI DSS-compliant complex passwords to any system hosting QuickSale Application.

User accounts should be created by logging in with the admin" account or an account with the User Management privileges. The following steps should be followed to create a new user:

1. Sign in with an account that has the appropriate privileges
2. Right click on the CHARGE Anywhere icon in the system tray
3. Select **User Management**
4. Select **Add User**
5. Fill in the **Username**
6. Assign a **Password**
7. Assign a **Clerk Number**
8. Select a **Permission Template** or check the desired permissions
9. Press **Create**

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

11. **User Management (QuickBooks)**

QuickBooks has a built-in user called **Admin**, and QuickBooks by default does not assign it a password. However, when using CHARGE Anywhere QB Plug-in, it **required** that **Admin** user get a password in compliance to the "**Password Policy**" included in this document. Admin can subsequently create more users and give them passwords in compliance to the "**Password Policy**" included in this document.

Give Admin a Password:

1. From the "**Company"** Menu, choose **Users**
2. Choose "**Set Up Users and Roles…**"
3. **Admin** user will be highlighted. Click "**Edit**" button the right side of the window.
4. Give **Admin** user a password in compliance to the "**Password Policy**" included in this document.

Create More Users:

1. From the "**Company"** Menu, choose **Users**
2. Choose "**Set Up Users and Roles…**"
3. Click "**New**" button the right side of the window.
4. Enter Required Info and choose Roles, then click Ok. Password must be given in compliance to the "**Password Policy**" included in this document.

Enable Customer Credit Card Protection:

1. From the "**Company"** Menu, choose **"Customer Credit Card Protection…"**
2. Choose "**Enable Protection**"
3. Follow the prompts to setup the Admin password if not already configured

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

12. **Logging**
(PA-DSS Req 4.1, 4.4)

Access to several parts of the application is logged and traced including and not limited to the below: Logging is performed automatically by the application and no configuration is needed by the user to enable audit trails. Also, there is no mechanism to disable audit trails. (PA-DSS Req 4.1)

- All individual accesses to cardholder data.
- All actions taken by any individual with root or administrative privileges.
- Access to all audit trails.
- Invalid logical access attempts.
- Use of identification and authentication mechanisms.
- Initialization of the audit logs.
- Creation and deletion of system-level objects.
- Key management details

Each log entry contains at least:

- User identification.
- Date and time.
- Application that originated the event.
- IP Address
- Message describing the event.

Centralized Logging
(PA-DSS Req 4.4)

These logs are downloaded to the server as they are generated and are stored for the merchant to review 24/7 for a period of one year. Merchants can access their application logs at:

https://www.chargeanywhere.com/transactionmanager/login.aspx

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

13. **Application Versioning Methodology**
(PA-DSS Req 5.4.4)

Application version is in format a.b.c.d

a. Version number of the application
b. Major version that denotes PA-DSS requirements and security impacting change
c. Wildcard card element that denotes minor feature changes that does not impact PA-DSS requirements and security
d. Wildcard element that denotes minor Bug fix

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

14. **Secure Wireless(WiFi) Setup**
(PA-DSS Req 6)

CISP-compliant wireless settings for deployment of a payment application in a customer environment per PA-DSS 6.1.

Wireless POS solutions are permitted to be deployed at a customer's facility. The wireless POS communicates directly with the customer's access point and data is then routed to CHARGE Anywhere's data center via the internet in a VISA/Master card approved encrypted methodology.

The following configuration steps **MUST** be used as the basis for all Wireless Access Point (WAP) system deployments:

- Change the default SSID (Service Set ID or network name)
- Change the default password for the WAP's Administrator account
- Enable MAC Address Filtering
- Limit the number of allowed connections to the minimum needed
- Disable DHCP
- Enable the highest encryption possible:
    - WPA with TKIP or AES (802.11g) or better
- Enable the WAP's firewall
- Disable the 'DMZ' feature
- Disable the Remote Management feature
- Disable Universal Plug 'n' Play (UPnP) feature
- Place the WAP near the center of buildings and avoid placing near exterior walls
- Change the SNMP community string or disable SNMP
- Periodically update WAP firmware

There should be a firewall configured between the wireless network and the network that contains card holder data so that only known traffic is being allowed access to the card holder data.

Under no circumstances should the encryption strength be configured to be less than 128 bits. Wireless encryption keys will be changed periodically, or whenever an administrator with knowledge of the keys is terminated.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

15. **Secure installation of patches and updates**
(PA-DSS Req 7.2.3)

When updates are available, ChargeAnywhere sends an email to the affected customers and provides a list of relevant information related the issues and update process.

QuickSale for Windows is downloaded from your secure site:
https://www.chargeanywhere.com/chargeanywheremanager/download_index.asp

The merchant would need his license number to be able to download the app. Furthermore, the app is digitally signed with the Charge Anywhere certificate.

QuickSale update process entails un-installing previous version and installing the new one. There is no patch install or update, a full un-install and re-install is required.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

16. **Secure Access to systems with cardholder data**
(PA-DSS Req 9.1)

Use unique username and complex passwords to access machines with payment applications and/or cardholder data per PA-DSS**. Also use unique usernames and PCI DSS compliant secure authentication for databases containing cardholder data.**

All devices that hold card data must be accessed with a complex password. Please follow the same guidelines as in section 6: "Secure authentication of Application".

Default passwords must be changed immediately upon the user's next login.

Keep passwords secure. Authorized users are responsible for the security of their passwords and accounts. These passwords must be changed every 90 days.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

17. **Secure Transmission of Data**
(PA-DSS Req 6.2)

QuickSale is designed to transmit data over HTTPS using TLS version 1.2.

CardNumber printed on receipt/email are masked.
Please note that unencrypted card numbers should **NEVER** be sent over messaging systems like email or SMS.
It is responsibility of the end user to establish and utilize proper encryption technologies and procedures when accessing the system over wireless device.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

18. **Secure Network Configuration for Systems with Card Holder Data**
(PA-DSS Req 9.1)

Systems that store cardholder data should **NEVER** be connected directly to the Internet. No direct inbound access to systems storing cardholder data should be allowed. There is no reason to allow inbound Internet access to any systems running CHARGE Anywhere software. There should be a firewall placed between the Internet and the cardholder data system that only allows legitimate outbound traffic through from systems to the Internet. The only outbound port required for CHARGE Anywhere is 443 (HTTPS).

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

19. **Remote Access to payment Application**
(PA-DSS Req 10.1)

If this system is to be accessed remotely, then multi-factor authentication **MUST** be used and the connection needs to use strong encryption; a clear text protocol (e.g. telnet) should **NEVER** be used. This can be accomplished by providing each required user with a unique certificate and login/password for their account access, while using SSH as the connection medium.

QuickSale Application does not provide/Support any components for remote access. Use of remote desktop applications to connect to the Application requires use of token in addition to a user name and password to maintain PCI compliance.

In addition, the following security features should be set for remote access, if applicable:

- Change default settings in the remote access software (for example, change default passwords and use unique passwords for each user).
- Allow connections only from specific (known) IP/MAC addresses.
- Use strong authentication and complex passwords for logins
- Account should be locked out after 4 invalid login attempts
- Configure the system so a remote user must establish a Virtual Private Network ("VPN") connection via a secure firewall before access is allowed.
- Enable the logging function.
- Establish user passwords settings according to PCI guidelines
- Restrict access to only authorized users. Deactivate users after use.
- Never allow an unsolicited caller remote access to the host containing card holder data
- Telnet or rlogin must never be used

All Non-console administrative access by customers and integrators/resellers to the CDE requires multi-factor authentication. (PA-DSS Req 12.2)

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

20. **Upgrade Procedures**
(PA-DSS Req 10.2.1)

The standard procedure for an upgrade is to uninstall the old software version, thereby removing all historic data and cryptographic material as per PA-DSS requirements, before installing the latest version. It is also recommended that if the merchant no longer has need of the application that they delete the app to remove all historical data from the device.

An email is sent with link to download securely from the Chargeanywhere site.
Only authenticated users with valid license are authorized to download Application.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

21. **Application of Security Updates**

All Charge Anywhere customers, Resellers, System integrators must apply security updates to their systems as available. In the event that there is a security related update that is required of the application an email will be sent to the effected parties. There will also be an announcement posted on the main site.

The communications will contain instructions on what actions need to be taken to update the effected pieces of software.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

22. **Remote Access to Application**
(PA-DSS Req 10.1)

QuickSale Application does not provide/Support any components for remote access. Use of remote desktop applications to connect to the Application requires use of token in addition to a user name and password to maintain PCI compliance.

- Only allow authorized users to remotely access the application
- Allow Connections from only specific IP
- Allow access to system with VPN connection via a firewall
- New allow an unsolicited caller remote access to the host containing card holder data
- Telnet or rlogin must never be used
- Account should be locked out after 4 invalid login attempts

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

23. **PAN over user messaging**
(PA-DSS Req 11.2)

QuickSale Application does not provide/Support any means of sending of PANs by end-user messaging technologies. Electronic receipts only include Masked PAN.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

24. **Ports Used By All Applications**
(PA-DSS Req 8.2)

CHARGE Anywhere is a stand-alone application and does not require services or daemons to run. No third party components are included/used in the application. It also does not require any inbound traffic. The following outbound ports are needed for CHARGE Anywhere to operate.

Port Number	Service
443	HTTPS

To further lock down outbound traffic, restrict outbound traffic for CHARGE Anywhere to the following domain:

*.chargeanywhere.com

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

25. **Supported platforms**

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

26. **Uninstall procedures**

It is a requirement of PCI that sensitive data is removed securely when an application is uninstalled from a device. Please follow the process below for your specific device. The process performed from within the app securely removes all sensitive, cryptographic keys, cryptograms, log files, debugging files, and any data that pertains to the application that is of sensitive nature.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

27. **Training Sessions**
(PA-DSS Req 14)

Training sessions will be held periodically per PA-DSS requirement .The session information will be sent out in an email two weeks prior to the scheduled date of the training. The training will cover the PA-DSS requirements to deploy the payment application in a secure manner.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

28. **Troubleshooting Procedures**

During the troubleshooting of a device, the data on the device will not be copied nor transmitted in any fashion. The troubleshooting process involves a customer support representative directing the merchant to take specific steps to remedy the issue. If the customer support representative cannot resolve the issue, they document the exact error and if possible the steps required to recreate it. The issue is then posted to the development team. The development team tries to reproduce the issue, resolves it, and then publishes a new version for download.

The steps described above also apply to any reseller's or integrator's support staff. Under no circumstances should application data be copied from the device or transmitted in any fashion.

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

29. **Information Guide**

Instructions on how to configure the Application is located at the following location

http://kb.chargeanywhere.com/index.php/QuickSale_for_Windows

Also it is available under 'Help' menu inside the Application

4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

30. **Implementation Guide**
(PA-DSS Req 13)

All customers, resellers and integrators using the application are provided with implementation guide upon request. Updated implementation guide is communicated to the customers via email.
Implementation guide is updated annually or any changes in PADSS requirements

CHARGE Anywhere®
4041 B Hadley Road
South Plainfield, NJ 07080
tel. 800.211.1256
fax. 732.417.4448

About CHARGE Anywhere: CHARGE Anywhere is a leading provider of secure Point of Sale (POS) solutions and electronic payment services. Our proprietary Visa PA-DSS Charge Anywhere® v2.2.0 Mobile Payment and POS software solution designed for QuickBooks®, Smartphones and e-commerce environments, and the Web Terminal Payment Solution - ensures Payment Card Industry (PCI) Level 1 compliance via ComsGate® Payment Gateway. CHARGE Anywhere offers business partners and customers the most secure and robust selection of industry specific and customized POS solutions and services, including; IP/Wireless Payment Gateway, POS software, Encryption and Data Security Services, Custom Card Issuance, and Merchant Billing Services. For more information contact them at www.chargeanywhere.com , or (800) 211-1256.