

TotalFBO® PCI Implementation Guide

Version 1.1, Released December 19, 2008

1. Payment Systems Security

1.1. Introduction

In order to address the growing national and international concern for securing credit card information, Visa began to develop standards and announced the Cardholder Information Security Program (CISP) in April, 2000. These standards became required in June, 2001, for all entities that store, process or transmit Visa cardholder data.

Since that time, other credit card companies have become involved, and a new group called the Payment Card Industry Security Standards Council was formed to standardize security requirements across the entire credit card industry. The result is a new security standard called Payment Card Industry Data Security Standard (PCI DSS or simply 'PCI') which is designed to ensure standardized compliance for multiple associations.

This document is provided to guide users of **TotalFBO®** into becoming and remaining PCI compliant.

1.2. Why you need to be concerned about this

Credit Card companies are requiring compliance with PCI standards for every entity that is involved in the storage, processing, or transmission of credit card information. Failure to comply can result in denial or revocation of your organization's ability to process credit cards.

Furthermore, as these standards have become widely recognized, non-compliance places your organization at risk of legal and/or civil consequences if credit card information becomes compromised.

Compliance with PCI standards is necessary whether or not you use **TotalFBO®** to process transactions "online." Even if you use a POS terminal or other method to process transactions, and simply retain information in **TotalFBO®**, you must be concerned about proper use of the program to maintain security and confidentiality of customer data.

Beginning October 1, 2008, Credit Card Processors and Bank Card Acquirers must only accept level 3 and 4 merchants that are PCI-DSS compliant or that utilize PA-DSS compliant applications.

Beginning October 1, 2009, all payment applications which are not PA-DSS compliant will be de-certified.

Beginning July 1, 2010, Credit Card Processors and Bank Card Acquirers must insure that merchants and agents use only PA-DSS compliant applications.

1.3. The PCI Data Security Standard

The “PCI DSS” is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

To learn more about PCI, visit www.pcisecuritystandards.org.

The standard must constantly evolve in order to remain viable in today’s rapidly changing internet and computing environment. Thus, the PCI DSS will be reviewed at least every 24 months, and can be updated at any time.

TotalFBO® Version 6.0 has been certified as compliant under the Payment Application Data Security Standard (PA DSS). The PA DSS is a separate security standard that applies to software vendors that develop applications for sale to merchants to process and/or store cardholder data. Just because **TotalFBO**® has been certified as PA DSS compliant does not automatically make you, as a merchant, PCI compliant. It is an important and necessary step toward that goal. Payment applications validated per the PA-DSS, when implemented in a PCI DSS-compliant manner, will minimize the potential for security breaches leading to compromises of sensitive cardholder data, and the damaging fraud resulting from these breaches, and speed you on your way to PCI compliance.

2. Merchant Requirements for Compliance

There are twelve basic requirements which a merchant must meet in order to become certified as PCI-compliant, organized into 6 areas. Each of these requirements, along with Horizon’s recommendations, are noted below. However, you must familiarize yourself with the details of each requirement as set forth in the PCI Data Security Standard documentation. (See Section 4 “Resources” for guidance on where to get more information.)

Build and Maintain a Secure Network

2.1. Install and maintain a firewall configuration to protect cardholder data

Your entire network must be protected with a firewall which is configured to deny all traffic except that which you expressly need and permit in order for your business to function. Your firewall configurations must be documented and reviewed regularly to insure that they continue to meet the standard.

It will be necessary to segregate any computer which stores cardholder data from the rest of your network and from any public access. Thus, you must insure that the SQL server that manages your **TotalFBO**® database is not located on the same server that hosts email or websites, and the like.

2.2. Do not use vendor-supplied defaults for system passwords and other security parameters.

In Section 3.3 below, we provide guidance on creating and managing passwords for Windows, SQL, and *TotalFBO*®. However, you must be vigilant about passwords for all areas of your network infrastructure, which includes network administration and monitoring, firewall and router appliances, and wireless devices.

Protect Cardholder Data

2.3. Protect stored cardholder data

You must develop a data retention and disposal policy as well as monitoring procedures to insure that your policies are adhered to. Generally, cardholder data must not be stored longer than is strictly necessary for business, and certain items (such as the PIN) cannot be stored at all. During the time you retain cardholder data, it must be encrypted and/or masked and protected from unauthorized access.

Cardholder data stored in your *TotalFBO*® database meets these requirements and the software will assist you with purging unneeded information. However, you must also be careful to manage email and any hand-written or printed materials which may contain sensitive data.

Encryption technology requires the use of a “key” which is used to consistently “scramble” and reassemble information automatically as needed. Managing these keys is a critical aspect of your security, which must be performed by two designated custodians. Your custodians must be familiar with their responsibilities as outlined by the PCI Data Security Standard, and your policies must insure their compliance.

2.4. Encrypt transmission of cardholder data across open, public networks

Not only must the data be encrypted when it is stored, it must be encrypted any time it is in transit across the Internet or a wireless network. *TotalFBO*® negotiates an encrypted SSL transmission for authorization and settlement of all transactions. However, you are responsible for the secure transmission of information when using remote connections, VPNs, wireless devices, email, websites, etc.

Maintain a Vulnerability Management Program

2.5. Use and regularly update anti-virus software

Anti-virus software is a critical component of your network security, and should be deployed to protect your network and each computer or other device (such as disks or USB drives) that may connect to it. Your policy should insure that anti-virus software is updated frequently and that you are monitoring the logs that it generates continually. You should also install software which guards against other hazards such as spyware, pestware, worms, Trojans, and any malicious software which may attack your network environment.

2.6. Develop and maintain secure systems and applications

As new security risks are identified, you must be prepared to meet them. Vendors such as Microsoft regularly release updates and patches to improve their software and remove or limit vulnerabilities. But you must be vigilant to obtain and install security patches quickly when they are released. Your policy must insure that you are keeping up to date with software releases for your operating system, *TotalFBO*®, any internally developed applications, appliance firmware, etc.

In addition, any web-facing applications must be protected by an “application layer” firewall – one which inspects the web traffic at a deeper layer than just the IP address and port.

Implement Strong Access Control Measures

2.7. Restrict access to cardholder data by business need-to-know

Within the security structure of *TotalFBO*®, you must specifically grant permission to a user in order for them to view stored cardholder data, and their ability to access the data is further limited by security privilege level and module limitation. It is not necessary to have this level of access to carry on most normal transactions, even at the point of sale.

Outside of *TotalFBO*® you must also insure that cardholder data is limited to those individuals with a business need-to-know. This would include printed or written materials, POS machine records, concierge activities, etc.

2.8. Assign a unique ID to each person with computer access

Each user must have a unique login and password or other authentication method for access to your computer systems. Further, you must actively manage user accounts and passwords and limit computer access so that unauthorized users may not gain access through the use of an authorized user’s credentials.

2.9. Restrict physical access to cardholder data

Your physical security practices are the outer perimeter of your data security. Give consideration to alarm systems, security cameras, wireless devices, the location of servers and other computer equipment, and the handling of physical media such as backup tapes or disks, etc. Your policies must address access by employees, visitors, and vendors.

When not needed for a stated business purpose, your procedures should include shredding or otherwise destroying physical records and media which contain cardholder information.

Regularly Monitor and Test Networks

2.10. Track and monitor all access to network resources and cardholder data

Although you may have developed good policies and procedures, they will be useless unless they are followed. That will require that you have a way to log and monitor access to your resources so that you can take effective measures to improve your security, train employees and others, and respond to any breaches

which may occur. You'll need to keep these logs for some time in order to properly research issues which may arise.

2.11. Regularly test security systems and processes

Just because a breach hasn't happened is no guarantee that it couldn't. Good security practice must include testing to identify potential vulnerabilities and help you develop appropriate safeguards. While you should approach testing from a variety of angles, PCI standards require that you perform an external vulnerability scan from by a qualified vendor at least quarterly and submit the results.

Approved Scanning Vendors (ASVs) are listed on the PCI Security Standards Council website.

Maintain an Information Security Policy

2.12. Maintain a policy that addresses information security

Throughout these requirements we have mentioned "your policies," and this requirement is the formalization of these concepts into a document that guides your entire organization. However, it is more than words on paper that sit on a shelf – it is a living awareness that permeates every employee's behavior, every system, every aspect of your corporate activities; and which is designed to grow and change in response to lessons learned and industry developments.

3. TotalFBO® PCI Security Practices

Because it has been certified as compliant under the PA-DSS requirements, using **TotalFBO®** as a tool will support you in meeting some of your merchant requirements to become and remain PCI-DSS compliant. However, it is important that you use the software as designed, and that you follow certain practices and procedures internally both when you install the software and as you enter transactions. The following steps will guide you in your efforts.

3.1. Sensitive data must never be stored

Although necessary for initial processing of a transaction, certain portions of the cardholder data must not be stored subsequently in any form. Sensitive data includes the following:

- Full contents of magnetic stripe track
- Card validation code
- PIN number

TotalFBO® V6.0 software will transmit this information initially but does not store it in your database or in log files.

Tip: Do not forget to inspect your paper files and remove any sensitive data which is stored there. In addition to the sensitive data mentioned above, full un-encrypted card numbers should never be saved in printed form.

3.1.1. Delete sensitive data from previous versions

Earlier versions of **TotalFBO®** may have stored some sensitive information. Thus, if you have upgraded from an earlier version of the software, you will

need to take steps to purge sensitive data from your database. Note that you must follow these procedures not only on your “live” database, but also on any archived or “training” databases.

A. Updating a previous database.

Simply updating your database from a previous version will activate an automatic process whereby sensitive information is detected and securely purged.

B. Verification

After the automatic process is complete, please inspect the following areas (in all previous version installations) and securely delete any remaining files:

- a. Home Directory Log Files: These files start with either “Auth” or “Setl”, and all end in “.xml”. These xml files may also be in sub-folders below your **TotalFBO®** home folder.
- b. Compressed Log Files: These are named “CCyyyyymm.clf”.
- c. Zips of multiple Log Files: These are named “CCyyyyymm.zip”.

C. Manual Deletion

If any of the XML, ZIP, or CLF files are found, they should be deleted securely using these steps:

- a. Copy the files “SDelete.exe” and “CCDelete.bat” from the TFBO6 folder to the folder where the offending files are found. One folder will likely be your TFBO5 folder where TotalFBO version 5.30 resided, but if you ever copied or moved credit card log files to other folders then those need to be securely cleaned as well.
- b. Run the “CCDelete.Bat” from the target folder by simply double-clicking on the file name “SecureDelete.bat” in that target folder. This will delete the necessary files from the folder the batch file is run in as well as any sub-folders that exist below that folder.

Note that these files, when created from Version 6, do **not** contain sensitive cardholder data and do not need to be deleted.

3.1.2. Delete sensitive data from troubleshooting operations

Beginning with Version 6.0, no sensitive data is stored in any form as a result of troubleshooting operations. Should such operations be changed in the future to require secure deletion operations, these instructions will be altered and provided concurrently with delivery of program revisions that contain such changes. Following the procedures outlined in the previous section will securely delete any files created for troubleshooting purposes in earlier versions.

3.2. Stored Data Protection

Some information must be retained for accountability, financial reporting, and future transactions. Your corporate Data Retention Policy must indicate the purpose for retention and the length of time you will retain each type of data.

Take care to consider the physical security of your backup files when creating your Data Retention Policy. While backups are necessary, it is not appropriate to retain large numbers of backup files for long periods of time. And while it is appropriate to take backups offsite, their security while in transit and in storage must be considered.

While the data is retained in *TotalFBO*®, it is encrypted for security, and further protected by masking (when displaying the Primary Account Number) and by limiting access to authorized users. Currently, *TotalFBO*® uses either Blowfish or AES 128-bit encryption algorithms. For best security, the encryption keys used must be changed regularly. *TotalFBO*® V6.0 provides for automatic encryption key rotation.

3.2.1. Encryption key management

Encryption keys must be changed at least annually to remain compliant with PCI standards, but more often is suggested. A new key can be generated automatically within *TotalFBO*® by using the function located at: Utilities> Security> Encryption Keys. If a new key has not been generated within the past year, *TotalFBO*® will not continue to process new credit card authorizations. If you are upgrading from Version 5.30, the encryption countdown is set to 90 days from when the database upgrade is performed.

Your organization must designate 2 custodians who will jointly be responsible for this task, with each individual contributing half of the key. Each custodian must sign a form stating that they understand and accept their responsibilities, as detailed in the PCI Data Security Standard.

Note that it is not necessary to write down the key unless you intend to use it for another piece of software which also accesses your *TotalFBO*® database. In that case, custodians must be responsible for maintaining physical security over the written key.

Once a new key has been generated, the “Re-Encrypt” button in the same function will be used to immediately re-encrypt all existing information in your database using the new key. Note that while a new key could be created at any time, the re-encryption process requires that all other users be logged out of the program. You can lock the program at Utilities> Program Administration> Administratively Lock/Unlock Program.

If you believe a key has been compromised, this process should be completed immediately on both your current and all archived, training, or backup database files. After successfully completing the re-encryption process, your Key Change Due Date will be rolled forward one year, and the previous key will be deleted.

Tip: Use different keys on each database, whether used for current, archived, or training purposes.

3.2.2. Purging cardholder data

Upgrading from any prior version of *TotalFBO*® will automatically securely purge all sensitive cardholder data which may have been stored in your database. However, your Corporate Retention Policy will govern purging unnecessary data on an ongoing basis.

Purging is done within *TotalFBO*® at Utilities> Program Administration> Purging Old Data. Within this function, you must select the following options to effectively purge cardholder data:

- Purge Customer Transactions
(Note that you must not retain Shop Orders)
- Purge On-File Credit Cards
(Removes cards which have not been used for any transaction within the number of days specified.)

Tip: Do not forget to inspect your paper files and remove any sensitive data which is stored there.

3.2.3. Deletion of prior-version encryption data

The process of re-encrypting your data as described above will securely delete all prior encryption data from your *TotalFBO*® database. This process should also be completed on all archived, training, or alternate database files.

3.3. Secure User IDs

User IDs are necessary for secure program operation on at least 3 levels. In each of these levels it is necessary to properly create and maintain these User IDs to maintain proper overall security. A common theme in management of all User IDs will be selection of strong passwords. In some areas you have software options to enforce good password management, in others you will need to enforce this behavior yourself.

In general, use passwords with 8 or more characters, two or more words, and that contain letters, numbers, and symbols from the entire keyboard.

3.3.1. Windows User IDs

Users should be required to log in to their workstations and prevented from using blank passwords. Best management of user logins is achieved when your network is part of an Active Directory domain and Group Policies are applied centrally by your network administrator. Group Policies can be created to require strong passwords and to insure that passwords are changed regularly.

Additionally, be sure to limit idle sessions and require passwords for resuming a paused session. Most users should be prevented from logging in except during specified hours.

Users should be limited to accessing those network resources which are necessary for their job duties. In the case of **TotalFBO®** users, this will include the program Home directory, and the user's local workstation only. Only a network administrator will have access to a SQL server location which may be used for creating database backups.

3.3.2. SQL User IDs

SQL Server literally holds all your program data. Every SQL Server installation automatically has a top-level administrative User ID called "SA", short for System Administrator. It is imperative that you do not use SA for daily operation of **TotalFBO®**. SA (or a suitably powerful alternate) must be used in initial installation of **TotalFBO®**, but thereafter you must use an alternate User ID with the minimum privileges required to operate the **TotalFBO®** program (db_owner). A button is provided for you on your licensing record (located in the User Utility Program) which will allow you to create a user for this purpose.

If you elect to install SQL 2005 Express from the **TotalFBO®** installation CD, you should change the default SA password when prompted during the installation. If you installed previously and are still using the default password, then it should be changed as soon as possible.

After you have successfully installed and started **TotalFBO®** you can easily change the SA password and/or add another user to your database by using the option at Utilities> Customizing> Set Global Options> Tab3.

Tip: Because of enhancements to the security and the interface to SQL itself, we recommend that you upgrade from an old installation of MSDE to SQL 2005 Express.

3.3.3. TotalFBO® User IDs

Each user should be provided with his own login credentials. An administrator setting up a new user can assign a temporary password and require that the user change it upon his first login, thus insuring that passwords are not known by anyone.

An administrator should regularly attempt to log in with a user's ID and the temporary password in order to monitor password usage. When a login is not being used, the administrator should determine how or if the user is gaining access to the software by other means and delete the login if it is not needed or else insure that the user is not sharing a login with someone else.

Note that an account is automatically locked for 30 minutes after 3 failed login attempts. Only an administrator can remove the lock for a specific account.

Password security rules can be established within *TotalFBO*® at Utilities> Security> User Setup> Password Rules Button. You can customize the rules to fit your organization's security policy in order to enforce the use of strong passwords. If you need to update your rules, they become effective immediately when the next user logs in.

In keeping with section 2.2 above, be sure to remove administrator-level access for the default "FBO" password supplied with a new program. You can do this in several ways:

- Delete the FBO user
- Change the FBO user password
- Reduce the FBO user privileges and access to the minimum (level 1) so that you might use this login only for guest access (such as an auditor running reports)
- Disable the account

When a user no longer needs access to *TotalFBO*®, it is important not to delete their login immediately, as this will also delete their access logs. Instead, simply disable their account. When these logs are no longer needed (per your security policy), you may then delete the login. You can also temporarily disable a login during vacation periods, extended leaves, etc., for added security.

All passwords are encrypted when stored within *TotalFBO*®, and the entry fields are entirely masked. If a user forgets his password, an administrator should simply reset it a temporary password, and require that the password be changed immediately upon the next login.

3.4. Application Audit Trails

There are several audit trails maintained by the *TotalFBO*® program. The one that is critical to PCI compliance is the Credit Card Access Log. For greater security, this report is not located with other reports, but is found at Accounting> Receivables> Update Credit Card Files> Reports.

In addition, you will want to monitor the Access Logs, found at Utilities> Security> User Setup. For greater detail in this log, check the box to "Log All Menu Operations." Be sure to set the retention period for this log to be consistent with your Retention Policy.

3.5. Wireless technology

3.5.1. Wireless LANs

It is critical to enforce security on all wireless connections to your network. You should require the installation of firewalls on all devices which connect in this manner, including PDAs, Pocket PCs, laptops, etc. A simple measure is the use

of timers on the power connections supplying wireless routers, so that they are automatically disabled during off-hours.

3.5.2. Wireless Encryption

Your network administrator must configure any wireless connection to use the highest level of encryption possible. Do not use the common WEP encryption which is the default of many wireless routers.

3.6. SQL Server must not have a Public IP Address

Proper installation of *TotalFBO*® includes installation to a workstation and/or to a Remote Terminal Server, and it is only in these locations (never on the SQL server itself) that the software should be run. Following this recommendation assists you in meeting this requirement, as there should not then be any need to expose the SQL server to the Internet in order for users to access the program.

Your network should segregate the SQL server from any other server functions, such as web-hosting, email, or remote access, both for security and for performance considerations.

3.7. Secure Software Updates

Horizon performs a virus scan on all software files prior to release for posting to the website or mastering CDs. The website itself is also scanned regularly.

In order to obtain a program update, you must log in to the secured Support section of the website using the login credentials provided with your program license. Note that your login credentials automatically expire when your service agreement terminates. When you successfully log in to the Support section of the website, all further transmissions are then encrypted using SSL.

3.8. Secure Remote Access to *TotalFBO*®

When accessing *TotalFBO*® remotely, whether from another building across your ramp or another city across the country, it's critical to secure the connection from the workstation to the remote server.

3.8.1. Two-Factor Authentication Required

Users must enter login credentials at least twice, so that they are authenticated first to establish a connection to your network, and then to run *TotalFBO*® itself. You may also use additional technology such as fingerprint scanners or physical devices to authenticate users.

3.8.2. Use Secure Remote Access Technology

When accessing *TotalFBO*® remotely, it is necessary to use a thin-client solution such as Windows Terminal Server, Citrix, Go-Global, PowerTerm, etc. With each solution it is possible to secure the connection using technologies such as SSL or RSA RC4 encryption. You may further secure the connection by adding the additional layer of a VPN or SPN structure.

Be sure to set limits on the length of a single session and to disconnect idle sessions quickly. Take steps also to prevent the transmission of unencrypted passwords.

3.9. Encrypt traffic over Public Networks

TotalFBO® automatically encrypts cardholder data when it is transmitted for authorization or settlement. No sensitive cardholder information is stored in logs or other files which may be needed for troubleshooting.

3.10 Use of email and other electronic messaging

Email access through *TotalFBO*® is provided through your own email server. No sensitive cardholder data is automatically generated in email form. However, it is possible for a user with sufficient privilege to print an unmasked card number. Your corporate policy must include procedures which prohibit emailing, faxing, or otherwise transmitting such a document, and provide for properly destroying it when printed.

4. Resources for Additional Study

- To learn more about PCI, and to download PCI requirements documentation, visit www.pcisecuritystandards.org.
- For assistance with developing a security policy, visit www.watchguard.com
- To learn more about network security, visit <http://www.interhack.net/pubs/network-security/>
- To test the strength of a password, visit <http://www.microsoft.com/protect/yourself/password/checker.msp>
- To learn how to create strong passwords, visit <http://www.microsoft.com/protect/yourself/password/create.msp>
- For guidance on developing a Data Security Policy, visit http://www.sun.com/blueprints/tools/samp_sec_pol.pdf
- For information on a free application layer firewall to protect web-facing applications, visit <http://www.armorlogic.com/>
- To obtain a list of Approved Scanning Vendors, visit https://www.pcisecuritystandards.org/pdfs/asv_report.html
- To obtain a list of Qualified Security Assessors, visit https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
- QSA used as preferred partner by Multi Service:
Bob Chandler, 312-873-7278, RChandler@trustwave.com
Trustwave, 70 W. Madison, #1050, Chicago, IL 60602
- For customized security policy manual, visit <http://isecuritypolicy.3dcartstores.com/>

5. Acknowledgements

Horizon gratefully acknowledges the guidance and assistance of Kenneth Rowe. His company, Chief Security Officers, is an approved QSA organization, specializing in assisting companies in becoming PCI compliant. Because his familiarity with Horizon and *TotalFBO*® may be valuable to our customers, we are providing his contact information here:

Kenneth Rowe
Chief Security Officers
(602)363-4610
www.chiefsecurityofficers.com
krowe@chiefsecurityofficers.com

ENCRYPTION KEY CUSTODIAN DUTIES

Payment Card Industry (PCI) Data Security Standard Version 1.1 includes the following requirements relative to data encryption keys which are used to protect cardholder information, and the duties of key custodians:

- 3.5** Protect encryption keys used for encryption of cardholder data against both disclosure and misuse.
 - 3.5.1** Restrict access to keys to the fewest number of custodians necessary
 - 3.5.2** Store keys securely in the fewest possible locations and forms.
- 3.6** Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:
 - 3.6.1** Generation of strong keys
 - 3.6.2** Secure key distribution
 - 3.6.3** Secure key storage
 - 3.6.4** Periodic changing of keys
 - As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically
 - At least annually.
 - 3.6.5** Destruction of old keys
 - 3.6.6** Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)
 - 3.6.7** Prevention of unauthorized substitution of keys
 - 3.6.8** Replacement of known or suspected compromised keys
 - 3.6.9** Revocation of old or invalid keys
 - 3.6.10** Requirement for key custodians to sign a form stating that they understand and accept their key-custodian responsibilities.

(Name) _____
has been designated as a Key Custodian for:

(Organization) _____

By affixing (his/her) signature below, the named individual certifies that they understand the duties and requirements of the Custodian position, and accept these responsibilities.

(Signed)

(Date)