CardSpot® Activation Software Installation Guide

Prior to installation

Windows XP, or Vista Operating System
Start Menu → Control Panel → Add or Remove Programs
✓ Microsoft .NET Framework 3.5

Please note that you may have other versions of the .NET Framework (2.0, 3.0) on your system. Do not modify these, as they may be necessary for other programs you have installed. However, the .NET Framework 3.5 must be installed for CardSpot® to operate.

To obtain the program(s) go to **www.microsoft.com** and search for .net Framework 3.5.

Please select the link **Download details: .NET Framework 3.5** and follow the onscreen instructions for downloading and installing the program(s).

Windows 7 Operating System
Control Panel (All Items view) → Programs and Features → Turn Windows features on or off (left pane link) → Blue box should appear next to .NET 3.5.1.

Remove Current Version of CardSpot®

If CardSpot® has never been installed on this computer, go to Installing New Version of CardSpot®.

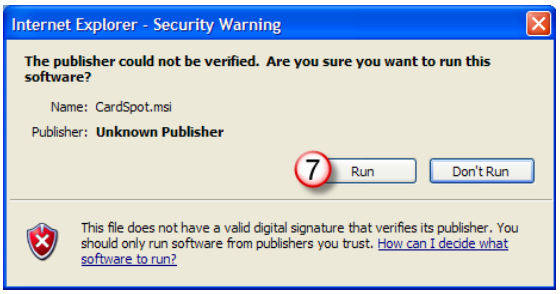
If CardSpot® has been previously installed on this computer, it will need to be removed.

1 Go to *Control Panel > Add or Remove Programs*

2 Select CardPoint and select the *Remove* option

3 Follow the onscreen instructions to remove the software.

Installing New Version of CardSpot®



1. Go to https://getmyreports.storefinancial.net/.
2. The Username is: clientsupport
3. The Password is: watermain123
4. Click on the file ending in Production Latest
5. Click on the CardSpot.msi link
6. Select Run from the File Download – Security Warning window
7. Select Run from the Internet Explorer – Security Warning window
8. Follow the onscreen instructions to install the Software through the InstallShield Wizard. Do not alter the default install location

When complete, a new CardSpot® shortcut icon will appear on the desktop.

Configuring CardSpot®

To configure CardSpot® double click the CardSpot® icon on the desktop.

Location Configuration

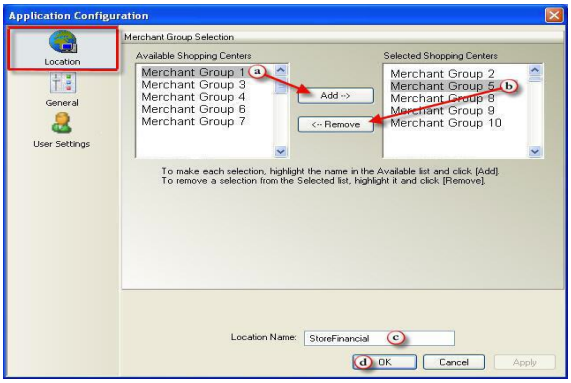
The first time CardSpot® is launched, a dialog box will appear stating "Your location.config file is either missing or corrupted. A dialog will now be shown to create this required file." Click "OK" to continue configuring CardSpot®.

Merchant Group Selection and Location Name

To configure your dealership and location name, click on the "Location" icon (if it is not already selected).

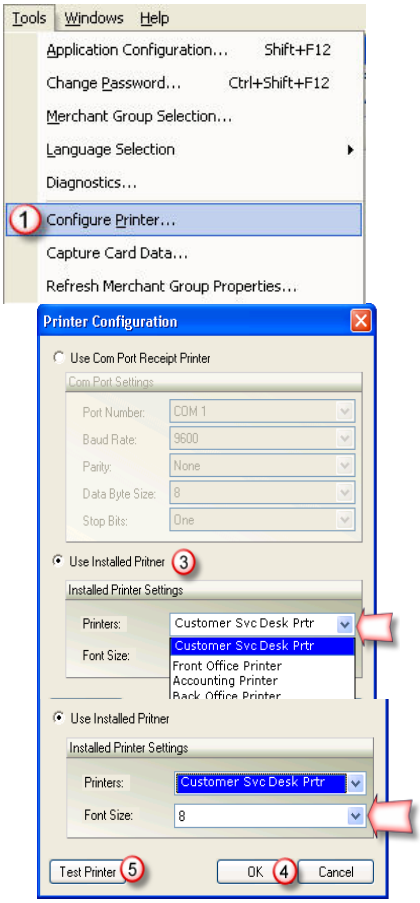
You will be required to enter your username and password, which was emailed to you by StoreFinancial. After entering your password provided by StoreFinancial, the system requires you to change your password immediately. Your new password must be at least 8 characters with at least one letter and one number.

a. Click on your property name in the Available Shopping Centers column.
b. Click "Add". The Add button is grayed out until your property name has been selected in the Available Shopping Centers column.
c. Change the "Location Name" to the desired selling location name (ex-Customer Service 1).
d. Click "OK" to save new settings.



Printer Configuration

Use this function to select the printer to print receipts.



1. Select (Configure Printer) from the tools menu. The Printer Configuration dialog opens.

2. If a serial (COM Port) printer is detected, CardSpot® uses this printer as the default.

3. To change to a local or network printer, select the Use Installed Printer option and choose the printer from the drop-down menu. Select the font size.

   To add a printer to this drop-down, the printer must be added via the standard Windows process. If you are not an administrator on the computer, you may not be able to add a printer.

4. Click [*OK*] to save changes or click [*Cancel*] to make no changes and exit the dialog.

5. Click [*Test Printer*] to verify selections are saved and that the selected printer is functioning properly. The selected printer should print a test receipt.

CardSpot® Activation Software Installation Guide

StoreFinancial (SF) provides CardSpot® software ("Software") to its clients. The primary purpose of the Software is to sell (activate) prepaid gift cards ("Cards"). The Software is developed for use in a VISA Payment Application Best Practice (PABP) / Payment Card Industry (PCI) Data Security compliant configuration. SFS follows Visa's PABP and has undergone an independent third-party audit of our development processes as well as the actual Software.

This CardSpot® Activation Software Installation Guide contains configuration recommendations for SF Software. The purpose of this guide is to instruct clients on secure product implementation.

CISP/PCI Requirements

Each section lists the PABP and PCI DSS requirement that applies to the Software implementation. The requirements are listed to cover all PABP specifications.

Magnetic Stripe, CVV data

Requirement : PABP 1.1.4 Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data. PCI DSS 3.2

The Software does not allow for local data storage. Therefore, no specific guidance is required.

Cryptographic Keys

Requirement : PABP 1.1.5 Securely delete any cryptographic key material or cryptogram stored by previous versions of the software. This could be cryptographic keys used for computation or verification of cardholder data or sensitive authentication data. PCI DSS 3.2

The Software does not allow for local data storage. Therefore, no specific guidance is required.

Log Files

Requirement : PABP 1.1.6 Securely delete any log files, debugging files, and other data sources received from customers for debugging or troubleshooting purposes, … PCI DSS 3.2

The Software can be configured to log debugging information to a local drive. However, no sensitive data will be written to a local drive with debugging turned on. Therefore, no specific guidance is required.

Usernames and Passwords

Software Requirement : PABP 3.1 Application must require unique usernames and complex passwords for all administrative access and for all access to cardholder data. PCI DSS 8.1 and 8.2

The following are requirements to support best practices implementations:

- User should not use administrative accounts, such as “sa” or “root” for application access to the system.
- Administrator should assign strong passwords to default system accounts, and then disable the accounts
- Clients and administrators should assign strong application and system passwords whenever possible.
- Administrators should not assign group, shared or generic accounts and passwords.
- Administrators should configure the system to force user’s to change their passwords at least every 90 days.
- Administrators should require a minimum password change of at least seven characters.
- Administrators should configure the system to force passwords containing both numeric and alphabetic.
- Administrators should configure the system to not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
- Administrators should limit repeated access attempts by locking out the user ID after not more than six attempts.
- Administrators should set the lockout duration to thirty minutes or until administrator enables the user ID.
- Administrators should set the session idle timeout for 15 minutes, and require the user to re-enter the password to activate a new session.

PC, Network Logins

Requirement : PABP 3.2 Access to PCs, servers, and databases with payment applications must require a unique username and complex password. PCI DSS 8.1 and 8.2

Clients should ensure that access to PCs that have the Software installed should be controlled via unique usernames and PCI DSS-compliant complex passwords. As of PCI DSS version 1.1, the following are compliant complex passwords:

- Administrators should require a minimum password change of at least seven characters.
- Administrators should configure the system to force passwords containing both numeric and alphabetic.

Wireless Networks

Requirement : PABP 6.1 For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi Protected Acess (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. PCI DSS 4.1.1

Clients implementing wireless networks should encrypt the transmissions according to PCI DSS standards. The Software will be complaint in a wireless implementation due to the fact that the Software transacts over https or SSL\TLS.

Server Internet Connectivity

Requirement : PABP 9 Cardholder data must never be stored on a server connected to the Internet. PCI DSS 1.3 and 1.3.4

The Software does not allow for local data storage. Therefore, no specific guidance is required.

Internet Connectivity, Personal Firewalls

Requirement : PABP 10 Facilitate secure remote software updates PCI DSS 1.3.9 and 12.3.9

The Software requires an “always-on” Internet connection. It is recommended for clients to use a personal firewall product to secure these “always-on” connections.

Remote Application Access

Requirement : PABP 11 Facilitate secure remote access to application PCI DSS 8.3

It is not recommended that the Software be implemented where it can be accessed remotely. For a majority of the implementations, remote access is not feasible due to the need for a card swiper and printer connectivity.

However, if the Software can be accessed remotely, two-factor authentication is required.

Encryption over Public Networks

Requirement: PABP 12 Encrypt sensitive traffic over public networks PCI DSS 4.1

The Software is automatically configured to transact over https or SSL\TLS. Therefore, no specific guidance is required.