ProphetLine, Inc
POS System

PCI Implementation Guide

What You Need to Know About PCI DSS & Credit Card Security

ProphetLine, Inc.
2120 South Waldron Road
Suite 128B
Fort Smith, AR 72903
1-800-875-6592
www.prophetline.com

ProphetLine® for Windows

Introduction

This Implementation Guide explains what is required for ProphetLine and your network to be secure and compliant with the PCI DSS standards. Requirements that ProphetLine covers will be explained, as well as any requirements outside of ProphetLine, that you and your network administrator will need to meet. While this guide will go over, in general, the network requirements you will need to put in place, the details should be decided on between you and your network administrator.

Following these guidelines does NOT make you PCI DSS compliant, nor does it guarantee your network's security. It is your responsibility, along with your network administrator, to ensure that your hardware and network systems are secure from internal as well as external intrusions.

ProphetLine makes no claims on the security of your network, nor of your level of being PCI DSS compliant.

As of October, 2009 all ProphetLine merchants must enable PCI DSS mode in ProphetLine. New installations will warn merchants that no credit card transactions can be completed until PCI DSS compliance features have been enabled.

Credit Card Information in Previous Versions

ProphetLine stores credit card information for two purposes:

1. By transaction, for use in returns and voids. The sensitive information stored is card number, expiration date and receipt number.
2. For monthly automatic billing purposes. The sensitive information stored is card number, expiration date, AVS card holder name, AVS card holder address, AVC card holder zip code and pos customer account #.

ProphetLine version 8.52 had an automatic update process as part of the installation package which encrypted PAN using 3DES. The unencrypted PAN was encrypted and moved to another data file and the existing unencrypted PAN was overwritten with the last four digits of the PAN. This update process could not be turned on/off by the user and it automatically ran with no user input required.

Customers running a version prior to 8.52 must go through the 8.52 upgrade and conversion process if they want to save existing card info. If the 8.52 version is skipped and they upgrade to a more recent version, the unencrypted PAN is overwritten with the first four digits of the PAN and the complete, the original PAN is not stored in any data file and therefore no longer available.

With the release of ProphetLine version 9.50, the PCI DSS option encrypted all sensitive credit card information in historical and monthly billing data using 3DES or AES. A new function was added to delete credit card data older than xx number of days without having to delete Sales History.

No version of ProphetLine has ever stored track 2 data, CVV data or PIN's.

It is the customer’s responsibility to delete any credit card information that may be stored on backup tapes, CD's, DVD's, hard disk or other backup media. Historical data must be removed, such removal is absolutely necessary for PCI DSS compliance.

Troubleshooting

ProphetLine Technical Support will never ask a customer to reveal sensitive credit card data for problem troubleshooting. We may ask for non-sensitive data like type of card or last four digits of card number. If someone posing as ProphetLine Tech Support asks for sensitive credit card information while troubleshooting a software issue, please report the technician's name in a separate phone call or email, to the ProphetLine Technical Support Manager and ProphetLine Sales, at 1-800-975-6592.

When a database is sent to ProphetLine Tech Support for backup or troubleshooting purposes, credit card information is removed prior to sending the database. If credit card information is mistakenly sent to ProphetLine, it cannot be decrypted as the encryption key is not stored or available to ProphetLine staff. The files that contain the encrypted CC data are immediately removed.

Storage & Maintenance

Credit Card Data & Encryption Controls

The latest PCI DSS features in ProphetLine are enabled and maintained by going to File > Setup System Manager > Cash Register Security > Credit Card Processing. On the General tab there is a button named either "Convert this installation to PCI DSS Compliance" (existing non-PCI users only) OR "Change or Backup Credit Card Encryption Key".

Users with access to credit card setup or stored information, or to edit personnel information, will be required to enter a strong password. The strong password must contain a minimum of 8 characters, no more than 15 characters, at least one letter and one number. The strong password created in Credit Card Processing will be assigned to the Supervisor account.

ProphetLine uses a two part encryption key. One person should enter the first half of the encryption key, and another person should enter the second half of the encryption key. Neither person should share their half of the encryption key with anyone.

ProphetLine lets the user choose to use either 3DES encryption or AES encryption. Note – AES is supported on Windows XP SP2 or greater.

ProphetLine allows, and strongly suggests, that the Encryption Key is backed up to a removable device and that device is stored off site in a secure location. The final encryption process uses a mix of the user entered Encryption Keys, server specific hardware information and an internal calculation. If the encryption key is damaged or lost, or the server computer is replaced, the only way to restore the original encryption information is to restore from the removable backup device. If the backup device is not available all stored credit card information will be lost.

If the encryption key is compromised a new one should be entered by two trusted persons (one half of the key per person) and a new encryption backup should be created on the removable drive, overwriting the old backup. Any cardholder data backed-up using the old data should be destroyed and replaced with backups using the new encryption key.

A strong password is required to view unmasked, decrypted credit card information on either of the credit card reports "Print Monthly Billing Credit Card Information" and "Print Transaction Credit Card Information".

A strong password is also required to access the "Change or Backup Credit Card Encryption Key" feature. Selecting "Change or Backup Credit Card Encryption Key" and entering a strong password, will allow the user to change the Supervisor strong password, change the encryption key (requires two people), change the encryption method and backup the full encryption key.

Strong Passwords should be changed every 3 months and cannot match the existing strong password, or any of the last 4 strong passwords. The Encryption Key should be changed once a year. Old encryption keys are directly overwritten with any new encryption key that is entered and saved. And again, the old backup of the encryption key, on the removable drive, should be overwritten with a new backup of the encryption key.

Purging CC data

Starting with ProphetLine 9.50, the PCI DSS setup screen has a “Number of days to store credit card information for Returns and Voids”. Enter the number of days to store credit card information and select the <Purge Credit Card Information> option to delete credit card information past the retention date.

After the initial setup, the credit card purge is set to run automatically in daily After-Hours Processing. If After-Hours Processing is not used, the <Purge Credit Card Information> option should be run manually each day.

Verify Previous Cryptographic Material is Removed

ProphetLine does not have a need to remove cryptographic keys from previous software versions. Each software upgrade is installed in the same disk location so that keys are never 'copied' to another location. When a new key is entered, it overwrites the previous key. If a future version requires a change in key storage locations, this requirement will be addressed to provide secure deletion of cryptographic keys.

Access Control & Audit Trails

PCI DSS requires any person with access to the ProphetLine program have a unique Windows username and a complex password. No usernames or password should be shared, and no “generic” accounts should be used. Any default users or accounts should be disabled, renamed, or changed to use a complex password.

Each person who has access to ProphetLine POS Administrative functions should have their own unique ID and password setup in the Employee File. The unique information should include employee ID #, name, address and nickname. Employees should never 'share' an account. The ProphetLine administrative account should only be used for System Setup purposes, not as an account for daily POS functions.

ProphetLine does not allow access to Administrative Functions (Credit Card Setup, Credit Card Stored Data, Encryption Key Setup or Edit Personnel) using normal login password credentials. An employee must log in with their normal password, and then enter a strong password to gain access to these administrative functions.

A strong password consists of:

- At least 8 characters, no more than 15 characters
- Must include both numeric and alphabetic characters
- Must be changed at least every 90 days
- Must not be the same as the last 4 passwords, or the current password

ProphetLine has implemented several secure authentication points per PCI requirements. These enhancements include:

- All users will be required to enter a username (Employee ID) and password, when clocking in to ProphetLine
- All users with Admin Function access (Credit Card Setup, Credit Card stored data, Encryption Key setup or Edit Personnel) will be required to log in with a strong password before accessing any admin function.
- Any user who attempts to enter a strong password 6 times, incorrectly, will be locked out of admin functions for 30 minutes, or until another user with admin access clears their account
- All screens and prompts that can only be accessed via a strong password will timeout, and log the admin user out, after 15 minutes of inactivity. The user will have to reenter a strong password to regain access to any admin functions.

Remote Access

PCI DSS requires that if anyone is using remote access to ProphetLine, that access should be authenticated using a two-factor authentication mechanism (username/ password and an additional authentication item such as a token or certificate), along with strong encryption. If a customer requires permanent access to a remote ProphetLine terminal, we would recommend a product such as GoToMyPC, or LogMeIn.

In the case of ProphetLine technical support, access is only available during the time the support is being done. ProphetLine technical support will connect with a web application named Team Viewer, using full encryption

based on RSA private-/public key exchange and AES (256 Bit) session encoding. In addition the program generates a session password that changes with every start of the software to ensure added prevention of unauthorized access to a remote. This program can be run once, without being installed.

To use Team Viewer, ProphetLine techs will direct customers to the Team Viewer website to download and run the client. Once the program is running the customer will verbally tell the ProphetLine technician the Session ID and Password. The technician will then enter that information and connect to the customer's computer. ProphetLine will never have access to a customer's computer without the customer initiating the connection. We believe this requirement results in the most secure method of remote access possible, as no unattended connections can be made.

With specific customers ProphetLine may use Remote Desktop Protocol or Terminal Services, in these instances high encryption is enabled, along a unique username and password.

Audit Trails

ProphetLine produces a POS access log automatically and it cannot be disabled. To access this log, print a Z-Tape Report under System Manager/Daily Reports. One option in particular, "Credit Card Report" will show all access to reports that contain Credit Card Information.

ProphetLine has also added specific logging of Admin functions which can be reported on via the PCI PSS Log File report, located under File > Setup System Manager > Cash Register Security > Credit Card Processing > Reports. PCI Log File updates occur for the actions listed below. Under each action is the particular event that cause a log file entry to be created.

Code **Description**

10 Change Employee Password
- Edit/Employee/Password <OK>

11 Change Employee Strong Password
- Edit/Employee/Password <OK>

12 Invalid Password Accessing Employee
- Edit/Employee/Add: Strong Password Screen
- Edit/Employee/Delete: Strong Password Screen
- Edit/Employee/Password: Strong Password Screen

13 Invalid Password Accessing Credit Card Settings
- File/System Setup/Credit Card Processing: Strong Password Screen

14 Lockout Strong Password
- Edit/Employee/Add: Strong Password Screen
- Edit/Employee/Delete: Strong Password Screen
- Edit/Employee/Password: Strong Password Screen

- File/System Setup/Credit Card Processing: Strong Password Screen

16 Reset Password
- Edit/Employee/Password <Reset>

17 Change Password After Reset
- Edit/Employee/Add: Enter New Strong Password Screen
- Edit/Employee/Delete: Enter New Strong Password Screen
- Edit/Employee/Password: Enter New Strong Password Screen
- File/System Setup/Credit Card Processing: Enter New Strong Password Screen

18 Corrupted Password
- Edit/Employee/Add: Strong Password Screen
- Edit/Employee/Delete: Strong Password Screen
- Edit/Employee/Password: Strong Password Screen
- File/System Setup/Credit Card Processing: Strong Password Screen

21 Print Customer Report
- File/System Setup/Credit Card Processing/Reports <Print Monthly Billing Report>

22 Print Transaction Report
- File/System Setup/Credit Card Processing/Reports <Print Transaction Report>

30 Edit Credit Card Settings
- File/System Setup/Credit Card Processing

40 Add Employee
- Edit/Employee <Add>

41 Delete Employee
- Edit/Employee <Delete>

51 Add Customer Card On File
- Edit/Customer <D/L, Credit Card> entering a new card # and existing card # field is blank
- Electronic Credit Card Processing screen for Mercury
    - Check box “Save as Customer Card On File”
    - Click <OK>
    - Existing customer saved card is blank
- Electronic Credit Card Processing screen for Cynergy
    - Check box “Save as Customer Card On File”
    - Click <OK>
    - Existing customer saved card is blank
- Electronic Credit Card Processing screen for PC Charge
    - Check box “Save as Customer Card On File”

- Click <OK>
- Existing customer saved card is blank

52 Delete Customer Card On File

- Edit/Customer <D/L, Credit Card> <Clear All>

53 Change Customer Card On File

- Edit/Customer <D/L, Credit Card> <Change>
- Electronic Credit Card Processing screen for Mercury
  - Check box “Save as Customer Card On File”
  - Click <OK>
  - Existing customer saved card is not blank
- Electronic Credit Card Processing screen for Cynergy
  - Check box “Save as Customer Card On File”
  - Click <OK>
  - Existing customer saved card is not blank
- Electronic Credit Card Processing screen for PC Charge
  - Check box “Save as Customer Card On File”
  - Click <OK>
  - Existing customer saved card is not blank

Network, Wireless and Database Security

Wireless Networking

ProphetLine does not ship with or require any wireless technologies. If a customer, reseller or integrator uses wireless technology with ProphetLine, that wireless vendor's default settings must be changed per PCI DSS Requirements:

- Install a firewall and Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies—for example, port address translation (PAT).
- Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.
- Use appropriate encryption mechanisms such as VPN, SSL/TPS at 128 bit or WPA
    - For current wireless implementations, it is prohibited to use WEP after June 30, 2010
    - We highly discourage using WEP at all, due to the low level of security it provides

Encryption of Data Sent over Public Networks

PCI DSS requires specific methods be used to transmit cardholder data over the internet or other public networks. ProphetLine meets these standards by using strong cryptography and encryption techniques at the transport layer with SSL, to encrypt cc data to Mercury Payment Systems.

PCI DSS also requires that cardholder information is never sent via email, instant messaging, chat, etc. without strong encryption.

ProphetLine Communications uses Secure FTP/SSH for communications between stores. The only credit card data sent over Secure FTP is the last four digits of card number. No other credit card data is sent over a public network.

Database storage

Sharing a database server and web server is not a requirement for ProphetLine and is highly discouraged. Do not store cardholder data on Internet-accessible systems (for example, web server and database server must not be on same server).

The ProphetLine server should not be stored in the DMZ or on Internet-accessible systems. The use of a router and a firewall can be used to secure the server computer.

Network Segmentation

Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of the corporate network is not a PCI DSS requirement. However, it is recommended as a method that may reduce:

- The scope of the PCI DSS assessment
- The cost of the PCI DSS assessment
- The cost and difficulty of implementing and maintaining PCI DSS controls
- The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations)

Without adequate network segmentation (sometimes called a "flat network") the entire network is in scope of the PCI DSS assessment. Network segmentation can be achieved through internal network firewalls, routers with strong access control lists or other technology that restricts access to a particular segment of a network.

Router and Firewall

All systems should establish firewall and router configuration standards that include the following:

- A formal process for approving and testing all network connections and changes to the firewall and router configurations
- Current network diagram with all connections to cardholder data, including any wireless networks
- Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone
- Description of groups, roles, and responsibilities for logical management of network components
- Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure
    - Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.
    - Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service. An example of an insecure service, protocol, or port is FTP, which passes user credentials in clear-text.
- Requirement to review firewall and router rule sets at least every six months

You should also build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.

- An “untrusted network” is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.
- Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.
- Secure and synchronize router configuration files.

- Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

Anti-Virus Software

Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).

- Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.
- Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.

Visa's Validation Requirements

Visa states "CISP (Cardholder Information Security Program) compliance is required of all entities that store, process or transmit Visa cardholder data." To be CISP compliant a business must be PCI DSS Compliant must meet Visa's validation requirements. The validation requirements vary depending upon the size of the merchant, as listed here:

- Level 1 Merchants (merchants processing over 6 million transactions per year) must:
  - Have an annual audit by a Qualified Security Assessor
  - Have Quarterly ASV Scans
- Level 2 Merchants (merchants processing 1 million to 6 million transactions per year)
  - Fill out an annual Self Assessment Questionnaire
  - Have Quarterly ASV Scans
  - Fill out an Attestation of Compliance form
- Level 3 Merchants (merchants processing over 20,000 e-commerce transactions per year)
  - Fill out an annual Self Assessment Questionnaire
  - Have Quarterly ASV Scans
  - Fill out an Attestation of Compliance form
- Level 4 Merchants (merchants processing less than 1 million transaction per year or less than 20,000 e-commerce transaction per year)
  - Fill out an annual Self Assessment Questionnaire
  - Have Quarterly ASV Scans

Most ProphetLine users will fall into the Level 4 category. Our Links to More Information section provides a link to the Self Assessment Questionnaire and the Attestation of Compliance form on the PCI SSC website, as well as a link to Approved PCI Scanning Vendors.

ProphetLine Configuration

Windows Users

Each employee using the ProphetLine POS system should have a Windows User account, utilizing a strong password. Each user can be a "Power User" and must have read/write access to the DBF folder on the ProphetLine server. More restrictive user groups can be used, but will need to be modified, based on network security, to allow full access to ProphetLine.

For installations and upgrades, an account with Administrator access must be used.

ProphetLine Server Installation

The ProphetLine software should be installed, from the CD or the downloaded installation files, on the designated server machine.

- The ProphetLine folder should be shared with at least read access to all ProphetLine users
- The folder ProphetLine\DBF should be shared with full read/write access to all ProphetLine users
- By default ProphetLine is installed in C:\Program Files\ProphetLine
- There is generally only one server installation per company, with multiple workstation installs connecting to the server database (DBF folder)
- New installs and upgrade installation files are run only on the server
- All workstations should have ProphetLine closed during server upgrades

ProphetLine Workstation Installation

When the ProphetLine server has been installed all workstations are then installed and setup.

- From each workstation machine browse across the network to the shared ProphetLine folder on the server
- In the ProphetLine folder find a file named NETSETUP.EXE and run the file
- ProphetLine will be installed on the local workstation, defaulting to C:\Program Files\ProphetLine
- After an upgrade is done on the server, each workstation will automatically prompt to upgrade on first use

Enabling PCI DSS in ProphetLine

The latest PCI DSS features in ProphetLine are enabled and maintained on the Server only. To access the controls go to File > Setup System Manager > Cash Register Security > Credit Card Processing. On the General tab there is a button named either "Convert this installation to PCI DSS Compliance" OR (if already converted) "Change or Backup Credit Card Encryption Key"

- When enabling PCI DSS compliance for the first time:
    - Log in as Supervisor

- Selecting this option will first display a Notice explaining the conversion and prompting Yes or No to continue
- Select Yes and you will be prompted to create a strong password. This password will be assigned to the Supervisor account
    - The strong password must contain a minimum of 8 characters (maximum 15 characters), at least one letter and one number
- The next screen will prompt for the Encryption Key Part 1. One person should enter this part, minimum 8 characters (maximum 15 characters) with at least one letter and one number. This should be shared with no one, especially the person who enters the Encryption Key Part 2.
- The next screen will prompt for the Encryption Key Part 2. A different person should enter this part, again minimum 8 characters (maximum 15 characters) with at least one letter and one number. This should be shared with no one, especially the person who entered the Encryption Key Part 1.
- The next screen will allow the user to selected the encryption method 3DES or AES, and select whether to back up the Encryption Key to a removable disk or not.
    - AES is not supported on Windows 2000.
    - **ProphetLine strongly suggests the Encryption Key be backed up to a removable device and that device is stored off site in a secure location. The final encryption process uses a mix of the user entered Encryption Keys, server specific hardware information and an internal calculation. If the encryption key is damaged or lost, or the server computer is replaced, the only way to restore the original encryption information is to restore from the removable backup device. If the backup device is not available all stored credit card information will be lost.**
- After the conversion process is complete:
    - A strong password is required to access Credit Card Processing in File > Setup System Manager > Cash Register Security
        - Only the Supervisor strong password will give access to change the Encryption Key or change the Supervisor Strong Password
        - Only the Supervisor strong password will give access to the Reports options under Credit Card Processing
    - A strong password is required to access the Edit > Personnel Add, Delete or Password functions
- Strong Passwords should be changed every 3 months and cannot match the existing strong password, or any of the last 4 strong passwords.
- The Encryption Key should be changed once a year
- No one person should know the entire encryption key (part 1 and 2)

Links to More Information

- **The PCI Security Standards Council**

  https://www.pcisecuritystandards.org/

- **Mercury Payment Systems Card Data Security**

  http://www.mercurypay.com/security-help.htm

- **ProphetLine's PCI Implementation Guild (latest version of this document) on the Web**

  http://www.prophetline.com/library/

- **Visa's Cardholder Information Security Program**

  http://www.visa.com/cisp

- **PCI SSC Self Assessment Questionnaire**

  https://www.pcisecuritystandards.org/saq/instructions_dss.shtml

- **Attestation of Compliance Form**

  https://www.pcisecuritystandards.org/security_standards/pci_dss_supporting_docs.shtml

- **Approved PCI Scanning Vendors**

  https://www.pcisecuritystandards.org/pdfs/asv_report.html

Appendix A: ProphetLine Normal Activity Log

These access points are tracked beyond the PCI Logging feature in ProphetLine POS and available to print on the Z-Tape Report by user id and date/time that the access occurred. The access points that may touch credit card information are listed in bold.

CANCEL TRANSACTION
CLOSE DATA FILES
AFTER HOURS
CLOCK-IN
CLOCK-OUT
CLOCK-OUT SALARY
EMPLOYEE SPIFF
INITIALIZE DRAWER RECONCILIATION
PRINT DRAWER RECONCILIATION
RECONCILE
RUN 2-WAY COMMUNICATIONS
EDIT PRICE QUOTE
EDIT SALES ORDER
EDIT PURCHASE ORDER
MATERIAL USAGE
LATE PAYMENT PENALTY
NO SALE
FINALIZE DRAWER RECONCILIATION
FINALIZE DRAWER RECONCILE W/BAD RETAIL STOCK LEDGER
CHECK CASHING
TRADE-IN
LAYAWAY SALE
RETURN MERCHANDISE
MAKE A SALE
PRICE QUOTE
SALES ORDER
RECURRING SALE
OPEN ACCOUNT
VENDOR INVOICE
PURCHASE ORDER
VENDOR RETURN/CM
A/P-PAY INVOICE
A/P-REVERSE PAYMENT
RECURRING PAYABLE
RECEIVE-ON-ACCOUNT
A/R-PROMPT PAYMENT DISC
A/R-VOLUME DISCOUNT
A/R-REVERSE PAYMENT
GENERAL JOURNAL ENTRY
INVENTORY ADJUSTING ENTRY
INVENTORY TRANSFER OUT
INVENTORY TRANSFER IN
RECEIVING TICKET
VOIDED A/P CHECK
VOIDED P/R CHECK
VOIDED RECEIPT
CASH IN
CASH OUT
RENTAL
CREDIT CARD REPORT