

PCI Implementation Guide

Prepared by VersiTouch, Inc.

March 12, 2009

Table of Contents

PCI Compliance Statement	3
Part 1 – Introduction	4
Part 2 – Overview of PABP and PCI Compliance	6
Part 3 – Guidelines and Responsibilities.....	7
Part 4 – POS Security Principles	11
Part 5 – Practical PABP Implementations.....	17
Part 6 – Additional Resources.....	22
Appendix – Glossary	25

PCI Compliance Statement

To Our Resellers and Merchant Customers

VersiTouch, Inc. is committed to helping our merchant customers comply with current Payment Card Industry Data Security Standards (PCI DSS). This letter should help you understand some of the steps we are taking to facilitate this process.

Based on our analysis of the PCI DSS, *VersiTouch Credit v9.2.7* meets the requirements of the Payment Application Best Practices (PABP) program and will help you to achieve PCI compliance.

What that specifically means is that *VersiTouch Credit, v9.2.7* and higher, does not store full track data from a card's magnetic stripe subsequent to authorization. *VersiTouch Credit* does not support or store authorizations using CVV2, CVC2, and CID numbers from the physical card or PIN block data for Debit transactions.

Furthermore, *VersiTouch Credit v9.2.7* protects all stored transaction data with *strong encryption*, which is defined as using an industry-standard technology such as 3DES or AES with a cipher of 128 bits or greater. In the case of *VersiTouch Credit, v9.2.7*, 128-bit AES is used to protect data such as transaction amounts, approval codes, Primary Account Numbers (PAN), expiration dates, and cardholder names. Users of *VersiTouch Credit v9.2.7* do not have access to view the full PAN, at any time. The PAN is masked with X's, except for the first six and last four digits, at any point within the program and on all reports and logs, whether viewed or printed.

VersiTouch, Inc. has successfully completed a compliance scan using 403 Labs "Tracker" program. In addition, we are in the process of completing our PABP audit for inclusion on the Visa website. If deficiencies are identified in our documentation or feature implementation, we'll be issuing updates as quickly as possible to rectify the situation. Any updates or bulletins will be transmitted directly to our Reseller network and also posted to our website at <http://www.versitouch.com>.

Sincerely,

Jonathan E. Bauder, President
VersiTouch, Inc.

Part 1 – Introduction

Payment by electronic card — credit or debit — is the fastest growing transaction type in the food and beverage industry.

There is no mystery why: cards are convenient and their use is encouraged in the industry because cashless transactions average 30 percent higher than cash transactions. Today most single-store food and beverage businesses process nearly 3,000 electronic-card transactions a month.

The Federal Reserve reports the fastest growing segment of electronic card use is purchases of less than \$10 and many of these small purchases are made at food and beverage businesses. In addition to convenience for the cardholder, merchants benefit because customers not only tend to spend more, but electronic transactions can make a business's cash-management processes —such as end-of-day cash reconciliations — more efficient.

Threat of Compromised Data

With the growing use of electronic payment cards, networks and databases where cardholder information is stored even momentarily have become prime targets for for-profit hackers. The magnitude of some security breaches is astounding. In 2005, CardSystems was hacked for 40 million card numbers. Just a year later, that record was broken when hackers attacked TJX — the parent company of Marshalls and T.J. Maxx — and captured data on 45 million cards.

Hackers go after electronic card data for one simple reason: there's big money in it.

- A credit card number and users address and date of birth is worth about \$20 on the Internet black market, reports CNN.
- A Gold VISA or MasterCard number, user's name and billing address and phone number gets \$100 on the black market, according to the New York Times.
- Hackers have even set up Internet chat rooms for peddling credit card numbers, social security numbers, mothers' maiden names and other personal information, according to Fox News.

At the high end of the Internet black market, a hacker's payback for stealing electronic card information from a single food and beverage merchant who is doing 3,000 electronic payments a month could approach \$300,000 a month, month after month, until the compromise is detected. And today's compromise-disclosure laws in most states force merchants to publicly reveal these breaches, which in some cases results in closure of the businesses due to fines and damaged reputations.

Until recently, food and beverage merchants have been mostly spared the threat of for-profit hackers because large corporations were the low-hanging fruit. But as tougher security measures have been rolled out at larger companies, hackers have begun looking down-market towards smaller merchants who have fewer security measures in place.

Food and beverage outlets fit this smaller, more vulnerable merchant profile. VISA reports that 40 percent of the known VISA compromises in 2006 involved restaurants.

Security Breach Costs and Impacts

Costs associated with security breaches are difficult to pinpoint but are known to be significant. As examples:

- CardSystems went out of business in the wake of its huge security breach.
- AOL's IT management was fired after a data compromise was disclosed.
- TJX took a \$4.5 million charge due to its 2006 security breach and lost more than \$1.8 billion in market capitalization in the two months after disclosing the breach.
- The full extent of Heartland Payment Systems' massive breach in 2008 is still being investigated.

Forrester Research says business costs associated with credit card security incidents is \$50 per compromised record, in addition to related business costs and lost revenue. This does not include fines by credit card companies such as VISA and MasterCard if the security breach occurs when their security standards are being ignored. VISA alone fined companies \$5 million in 2006.

This means that a food and beverage merchant with 3,000 electronic payment transactions per month is exposed to potentially \$150,000 in damages when the security breach occurs, plus \$150,000 in additional damages for each month the security breach is undetected. The total in damages can quickly reach more than twice the average food and beverage single-store revenue for the month.

As quoted from Visa's website "If a merchant or service provider does not comply with the security requirements or fails to rectify a security issue, Visa may:

- Fine the acquiring member
- Impose restrictions on the merchant or its agent
- Permanently prohibit the merchant or its agent from participating in Visa programs

Members receive protection from fines for merchants or service providers that have been compromised but found to be CISP-compliant at the time of the security breach. Members are subject to fines up to \$500,000 per incident for any merchant or service provider that is compromised and not CISP-compliant at the time of the incident."

Use of electronic payment cards will continue to grow in the food and beverage industry, and its merchants will need all the protection they can get to enjoy the benefits of electronic payment cards without the dangers.

Part 2 – Overview of PABP and PCI Compliance

Major credit card companies including VISA, MasterCard, American Express, Discover, and JCB — in forming the Payment Card Industry Security Standards Council (PCI SSC) — have developed comprehensive standards and guidelines for electronic payment data security for POS applications.

Acknowledging the need for a separate validation for software providers, VISA in 2004 created the Payment Application Best Practices (PABP), a set of voluntary guidelines addressing the design and implementation of payment processing software.

The PABP guidelines for software providers were aligned in 2005 with the joint Payment Card Industry (PCI) standards for merchants. This enables merchants to understand the relationship between the software they use — especially as more software providers become PABP-certified in the coming years — and their own compliance responsibilities.

The distinction between the council's security standards for merchants and the PABP for software developers is important. As a merchant, you can enjoy the confidence and security of using PABP-accredited software, but you still have an obligation as a payment acceptor to demonstrate compliance with the applicable electronic-payment assessment standards and guidelines for your business.

As a software vendor, our responsibility is to be "PABP Compliant". PABP is the standard against which VersiTouch tests its software products.

As a part of our obligation in meeting the PABP requirements, we provide this PCI Implementation Guide to help you better understand your responsibilities and the relationship between the standards governing you -- the merchant -- and those governing us -- the software provider. This document further provides specific installation, configuration, and ongoing management best practices for using VersiTouch software as PABP applications operating in a PCI Compliant environment.

- A more complete discussion of the PCI security standards appears later in this document, in Part 5, Practical PABP Implementations.
- For more information on PCI DSS, visit the PCI Security Standards Council's website at www.pcisecuritystandards.org.
- You can examine the latest version of the PABP by following the links for Payment Applications at <http://www.visa.com/cisp>.

VersiTouch also recommends that you evaluate your payment processing operations in relation to the comprehensive security guidelines published by the Open Web Application Security Project.

- You can download and review their documentation at <http://www.owasp.org>.

Part 3 – Guidelines and Responsibilities

The following table (from the PCI DSS) illustrates commonly used elements of cardholder data and sensitive authentication data, whether storage of that data is permitted or prohibited, and whether this data needs to be protected. This table is not meant to be exhaustive; its sole purpose is to illustrate the different type of requirements that apply to each data element.

The Primary Account Number (PAN) is the defining factor in the applicability of PCI DSS requirements and the PABP. If PAN is not stored, processed, or transmitted, PCI DSS and PABP do not apply.

	Data Element	Storage Permitted	Protection Required	PCI DSS REQ. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

* These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (e.g., related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

** Do not store sensitive authentication data subsequent to authorization (not even if encrypted).

VersiTouch can assist you in your compliance efforts by confirming that our latest software meets current PABP standards. It protects all stored **cardholder data** with "strong encryption," using industry-standard AES technology with a cipher of 128 bits or greater and does not store **sensitive authentication data** subsequent to authorization.

As a merchant, your obligation to protect consumer data does not end with your VersiTouch products. You should institute the practices listed on the following pages,

regardless of how you use your software. VISA and MasterCard may require that you develop them, so be sure to periodically verify with those associations and your merchant bank that you are complying with all applicable data security regulations and guidelines.

Always remember, you have an ongoing responsibility to your merchant bank and to your customers to treat their data with the utmost of care.

Responsibilities for Entire System

VersiTouch provides you with a comprehensive POS system. A POS vendor should be able to demonstrate a commitment to maintaining security best practices and to continuously improving the security associated with its technology.

For example, although multiple types of encryption are available for transmitting POS data, only AES encryption is formally recommended by the U.S. Department of Commerce National Institute of Technology Standards (NIST). Use of outdated encryption technology can jeopardize security compliance.

POS environments are complex and vulnerable to security breaches at several points. For this reason, the processes associated with POS environments are mission critical. For example, lines cannot be allowed to slow or transactions to take longer to process as a result of security measures.

It is important to remember that your data security obligations as a merchant extend to the payment-acceptance system in its entirety.

As a merchant, you should conduct a thorough assessment of all software modules associated with your payment system because you may be required to make representations to your merchant bank as well as to the card associations about your entire payment system. VersiTouch can only furnish information about its own products, not your entire system.

Merchants and Card Providers

All merchants who accept credit cards should be concerned with POS security. However, each credit card provider segments merchants by credit card transaction volume and type.

For example, VISA now requires credit card acquirers — financial institutions that provide credit card processing services to merchants — to ensure and document that all merchants meet VISA requirements. As part of this requirement, VISA segments merchants into four levels, based on credit card transaction volume and transaction type.

Merchant Level	Description	On-Site Security Assessment	Self-Assessment & Questionnaire	Network Scan
1	Over 6,000,000 credit card transactions; has had a previous card-related security breach. Any merchant that VISA, at its sole discretion,	Required Annually	Required Annually	Required Annually

	determines should meet the Level 1 requirements.			
2	1,000,000 to 6,000,000 credit card transactions/year		Required Annually	Required Quarterly
3	20,000 to 1,000,000 VISA/e-commerce transactions a year		Required Annually	Required Quarterly
4	20,000 or fewer VISA/e-commerce transactions a year; All other merchants processing up 1,000,000 transactions/year		Required Annually	Required Quarterly

VISA puts most of the burden for enforcement of these standards on the credit card acquirers who maintain merchant relationships and who receive all card transactions from merchants. Acquirers have the responsibility to ensure that their merchants are appropriately validated and documented, and they must submit monthly status reports to VISA.

Compliance Management and Governance

The most significant challenge facing organizations implementing PCI DSS is how to monitor the organizations compliance posture to ensure a rapid response to change in the standard or their own infrastructure, staff or supporting processes.

The model below summarizes the key disciplines required to support your compliance management architecture, mapping these capabilities to the technology service requirements needed to achieve and then maintain compliance with the PCI standard.

	Discipline	Explanation
Incident Prevention	Risk Analysis & Assessment	Completion of Independent Compliance Audits or Self Assessment External Vulnerability Assessments (Independent Scanning Vendor) Internal Port Scanners Security threats assessment against database of known threats vs IT assets and current configuration
	Protection	Firewalls, Perimeter Security Anti-virus Data Encryption (VPNs email encryption, encryption of stored data) Hardened operating system & secure application configuration Equipment disposal
	Control	Identity Management, Rights of Access, User Authentication, Strong Authentication Activity Logs Auditable processes for issuing and amending access rights & permissions to systems, applications and data
Incident Management	Detection	Alerting, Event Monitoring & Correlation; Severity Classification and Management Intrusion Detection, Content Screening, Virus Scanning, Log analysis, Notification of acquirer or processor and cardholders
	Investigation	Assessment of breach, notification of cardholders Forensic tools, providing log analysis, audit trail, to support evidence gathering, root-cause analysis

	Response	Contingency planning, business continuity, strategy, assessment of risk vs existing policy, recommendation for change
--	----------	-----------------------------------------------------------------------------------------------------------------------

For external auditing and threat analysis, we recommend contacting the following Visa U.S.A. approved certification firms:

403 Labs, LLC
17125-C West Bluemound Road
Suite 200
Brookfield, WI 53005
Phone: 1.877.403.5227

Coalfire Systems, Inc.
361 Centennial Parkway,
Suite 150
Louisville, CO 80027
Phone: 303.554.6333
Fax: 303.554.7555

Part 4 – POS Security Principles

POS security is a highly complex matter, but it can be distilled to three central principles: Authentication, Access, and Auditing. Understanding these three principles and the activities they involve will help you understand POS security more comprehensively.

This section contains some discussion of best practices for POS security. A more detailed discussion of best practices is in Part 5, Practical PABP Implementations.

Authentication

Authentication is the practice of ensuring that when users attempt to login to a network or host, they must authenticate against predetermined criteria to validate their identity. Authentication is made up of authentication protocol and password management.

Typical authentication protocol requires a unique username and password for each user. The best practice for password security is the requirement of a strong password containing at least eight characters, and preferably 14 or more characters. The password should contain a combination of letters, numbers, and symbols.

To ensure comprehensive network security, best practices password management policy must be implemented across:

- Operating systems
- POS applications
- Database applications
- Remote access products

VersiTouch recommends that you secure your POS system through use of a site manager and that you lock down the PC on which the product resides. Require your staff to log in using complex passwords and configure the operating system to force users to change their passwords routinely, such as every 30 or 90 days.

Access

After users have been authenticated, they should be granted access only to the resources they absolutely need for business purposes. This best practice is referred to as granting a minimum set of privileges.

With VersiTouch POS software, you can “lock down” access to only those users with a legitimate need to use it. Familiarize yourself with these capabilities so you can assign usage profiles, create users and manage user passwords effectively. Follow the rule of thumb that users should not be granted a particular privilege unless there is a legitimate need for them to use it.

To maintain a secure network, never install a payment software application on a computer that has a direct link to the Internet unless that link is secured. If you are using the Internet for your transaction transport, make sure your Internet hardware — cable modem, DSL router and other connectivity devices — has built-in firewall

capabilities. Be sure to change any administrator-level passwords from their default configuration to a complex password that only you know.

Other software installed on the computer where your VersiTouch POS system resides could present a security risk. Be sure to carefully evaluate other applications — such as remote-access software — and consider removing it or locking it down to reduce the risk of malicious attack. Limit or remove the file- and directory-sharing capabilities of the operating system. Disable or uninstall unused software, devices and drivers.

VersiTouch software is designed to work on any network that supports TCP/IP protocols, without direct knowledge of the physical devices or communication technologies underlying the TCP/IP layer. If you use wireless devices of any kind to store or transmit payment transaction data, those devices must be configured to encrypt transmissions using technologies consistent with the standards in the PCI guidelines.

Security issues have been found with the WEP Wireless Encryption Protocol. It is strongly recommended that you implement additional security measures on top of WEP, such as IPsec or SSL. Remember, any link over a public network, regardless of physical transport media used, should be secured by no weaker than 128-bit encryption.

Also note that VersiTouch does not perform remote access operations and does not test with remote access software. If you use any remote access software to manage the computer on which your VersiTouch software is installed, it is your responsibility to configure and operate that software in a manner consistent with PCI guidelines.

Access Vulnerabilities

These procedures may require a security professional to implement them.

Keep in mind that for-profit hackers are looking for software storing sensitive cardholder data with personal identifying information and account numbers. Most of this information is stored on the payment card magnetic stripe and is captured when the card is swiped through a reader.

In a typical POS environment, there are four primary tactics hackers use to gain access to credit card data.

- Unauthorized Network Access
- Unauthorized Host Access
- Unauthorized Remote Access
- SQL Injection Attacks

1. Unauthorized Network Access

The network is the primary means of transmitting information between devices in the POS environment as well as out to external entities for applications like credit card approval, email and general Internet access. Most networks use open TCP/IP protocols.

For-profit hackers frequently focus on the open TCP/IP network to attack POS systems. These attacks most often take the form of unauthorized network access, viruses, worms and Trojan Horses.

Preventing Unauthorized Network Access.

To prevent this type of breach you should first implement firewalls to protect against unauthorized access from outside your network. These firewalls, as with most devices physically attached to your network, use default settings and passwords that you should always update to settings and passwords unique to your environment. The updated passwords should meet the "strong passwords" definition, which calls for passwords of at least eight characters and containing combinations of letters, numbers and symbol characters.

If you have a web server, it should reside in a "DMZ" where the firewall is between the server and the Internet, and a second firewall is between the web server and your internal network. The only open network ports and enabled services should be those necessary for day-to-day business. All other ports and services should be disabled across both inbound and outbound traffic.

For POS system network security, the POS environment should be physically partitioned from other non-critical or un-trusted networks such as those allowing open access to the Internet or having wireless access points. There also should be a documented change policy and log for any changes to your network and firewall. This change policy should include a regularly scheduled review of those logs.

2. Unauthorized Host Access

A POS host is the server that enables payment-processing functionality within the POS network. For security purposes, the host must be properly configured and segmented from other devices on the network.

Typical host vulnerabilities include:

- Default users and passwords remaining unchanged after initial install.
- Blank administrator passwords.
- Unnecessary ports and services being enabled, such as web service, ftp, or email.
- Omitted security features, such as audit logging and lock-out options.

Preventing Unauthorized Host Access

To guard against attacks on your POS host, data not required for business purposes should not be stored. The risk of a compromise is generally much more than the cost of ensuring that your systems are properly configured and that you are only retaining the data you absolutely need.

Second, ensure the latest operating system and application versions are installed, along with the latest security patches, anti-virus engines and

signature files. Disable any ports and services not needed for business functions. Also, limit access to specific devices by implementing a process known as white-listing via IP or MAC address filters.

Next, the POS host should only be used for payment data processing, and not for activities such as web browsing or email, since malicious software easily propagates through both of these activities.

Finally, the naming convention of POS system resources should obscure the business nature of the system resources — do not name your POS server something as evident as “POS Server.” The POS system should not be physically connected to networks with high-risk profiles such as those used for email or Internet access.

3. Unauthorized Remote Access

Remote access products like PC Anywhere, VNC and Webex SmartTech are frequently the primary means by which POS vendors support POS systems. These products can simplify maintenance and troubleshooting as well as assist with menu updates, system health, and reporting.

However, products that enable unattended remote access — access without a person specifically authenticating and authorizing remote access each time it occurs — are significant threats to the POS environment because they essentially open a “back door” into the POS network and host systems.

Preventing Unauthorized Remote Access

Upgrade to the latest version of the remote access product or service and ensure the latest security patches are applied prior to full deployment. If the remote connection is configured via dial-up, make sure the modem and its software provide dial-back functionality where applicable.

Automatically block remote IP addresses after a pre-defined number of failed login attempts. Multiple failed logins are an indicator that hackers have targeted a system. Also, after an abnormal session — one that includes a session expiration, time-out, or broken connectivity — remote users should be prevented from reconnecting to the host without re-authenticating and reconfirming with the host operator.

Also, remote access products should use data encryption and, if the remote access product is a hosted service, the encryption should be end-to-end AES encryption.

Last, the same measures applying to preventing unauthorized network and host access also apply to unauthorized remote access. Make sure strong passwords are required, and never continue using default passwords or settings after the initial installation is complete. Audit logging should be required when your POS vendor makes changes while remotely accessing devices.

4. SQL injection Attack

SQL attacks can occur if you have a web page or application allowing users to enter text into a textbox that will then be used to execute a query against a database.

Most web forms are susceptible to SQL injection attacks where a hacker enters a malformed SQL statement into the textbox and changes the nature of the query so it can be used to break into, alter, or damage the back-end database. In this way, hackers can manipulate and extract data from databases and can access back-end database via the web form interface.

A successful SQL injection attack can result in compromised data — data that has been revealed, altered or destroyed — as well as the creation or elevation in system access privileges, and/or a host system takeover.

Preventing an SQL injection attack

Be sure all web applications validate user input. This means when a user enters data through a web form, the values entered into the form are validated before being entered into the database. This validation includes checking that required fields are not empty, email addresses and phone numbers are entered in the correct format, and fields intended for numeric information contain only numeric information.

Web applications should avoid using dynamic SQL statements that combine user data with dynamic SQL to send SQL commands to the database. These dynamic SQL statements can be exploited by SQL injection attacks to gain access to the database and can be replaced with prepared or stored SQL procedures without losing functionality.

Run regular scans at the database level for known SQL vulnerabilities. SQL statements should always be executed with a minimally privileged account. Also, SQL statements should be encapsulated in stored procedures that should be kept to a minimum. Only these stored procedures should be allowed to access database tables. Direct access to these tables should be not allowed.

Auditing

Maintain a log of all actions taken on all systems accessed. This log should keep a record of additions, edits and deletions made to the system, along with timestamps of when those actions occurred. The log should be easily queried when needed for auditing, providing a satisfactory audit trail.

Keep in mind that VersiTouch software allows you to store transaction data for a long time. While this is important to some merchants, you should ask yourself how long you really need to retain transaction data. Develop a schedule for deleting or destroying data when you are certain you no longer need it.

External reviews are always a possibility, depending on the amount of card transactions you process. If the number is substantial, you may be obligated to engage an external security assessment company to judge your level of compliance with the various security compliance programs. If you choose to follow this path, consider engaging a CISP-qualified assessor versed in the latest requirements from

the card associations. Cardholder security is a rapidly changing subject and the standards can change as well.

Third-party Integration

Through software resellers or other system integrators, collectively referred to as Value Added Resellers (VAR), merchants may use VersiTouch software as part of a larger, integrated payment-processing system. If this is your situation, you should follow the principles discussed in this section — Authentication, Access, and Auditing — to gather important information from your VAR related to all components of your electronic payment system.

- **Document Software Products and Versions**

You or your VAR should determine the product and version numbers of all components of your payment system. For example, the product and version numbers are listed on the opening screen of your VersiTouch software or can be obtained through the VAR from whom you purchased your software. Compile these numbers for all software associated with your electronic payment system.

- **Document Software Integration Method Used**

Once you have established your system's products and versions, your VAR needs to confirm that the integration method used is supported and conforms to the recommendations cited in this document. If your VAR is using an integration method designed for a product that is no longer supported — such as RCS-100 POS, RCREDIT, or RCS-CREDIT — your system should be updated to maintain acceptable levels of security. We encourage you to share this document with your VAR and to involve VersiTouch, Inc., in these discussions as you see appropriate.

- **Assess All System Components**

Your VAR may have selected VersiTouch software as the core payment processing engine for your payment system, but the VAR has the same responsibility to demonstrate compliance with data storage rules as VersiTouch, Inc. Request any relevant documentation or procedures detailing how to install, secure and operate all parts of your payment system, with close attention to any components that store or manage customer data — such as customer databases, system activity logs and reporting systems — to determine their level of adherence to current standards.

This is important because merchants are under special obligation to represent to their merchant acquiring bank that they are processing transactions securely. With this in mind, you should take the initiative with your integrator/reseller to compile this information.

Part 5 – Practical PABP Implementations

There are several steps compiled by the PCI Security Standards Council that merchants can take to significantly improve their security profiles.

The information in this section is derived from PCI Data Security Standards and should serve as a high-level guide to POS security as well as to easy actions you can implement immediately to improve POS security.

Build and Maintain a Secure Network

Requirement 1: [Install and maintain a firewall configuration to protect cardholder data](#)

Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Internet firewall security needs to be installed and functional on all computers and POS systems using IP connectivity, including those with a dial connection to the Internet. VersiTouch recommends that you install and configure a router with a hardware firewall to protect your network. This firewall should use a "white list" to allow only approved devices.

On each PC, install and configure a software firewall, such as Windows XP firewall, ZoneAlarm, or an equivalent of your choice.

Requirement 2: [Do not use vendor-supplied defaults for system passwords and other security parameters](#)

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information. Examples of default administrator accounts include "administrator" (Windows systems), "sa" (SQL/MSDE), and "root" (UNIX/Linux).

For wireless environments, change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.

Passwords should be personalized for all users of computers and POS systems. The PCI DSS requires the following password complexity for compliance (often referred to as using “strong passwords”):

- Passwords must be at least 7 characters
- Passwords must include both numeric and alphabetic characters
- Passwords must be changed at least every 90 days
- New passwords can not be the same as the last 4 passwords

All unnecessary services, such as FTP, open ports, and resource sharing, should be disabled.

Protect Cardholder Data

Requirement 3: [Protect stored cardholder data](#)

Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods for protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.

VersiTouch POS v9.2.18 and VersiTouch Credit v9.2.7 do not store track data from the magnetic stripe on the credit card after receiving a valid authorization. VersiTouch software does not support authorizations using card-validation code (CVC) or value (CVV) or personal identification number (PIN) and does not store this sensitive data. Pre-authorized data is encrypted using 128-bit AES encryption.

Only store cardholder account information that is essential to your business. Hard copies of batch reports and paper receipts must be placed in a secured area where only authorized personnel can enter. VersiTouch software stores the PAN, expiration, and authorized amount, indefinitely, in 128-bit AES encrypted format. Implement a policy on how long data will be stored and for what business or legal purposes it is needed. When discarding, make sure you shred or otherwise permanently destroy all documents and securely delete the restricted data identified above.

Requirement 4: [Encrypt transmission of cardholder data across open, public networks](#)

Databases and files containing payment card information must be encrypted. Encryption software is required for POS systems using Internet connectivity for transmission of cardholder information. VersiTouch transmits credit card data in 128-bit AES encrypted format. Transmission of credit card data over the Internet for authorization and settlement is encrypted either by Heartland Payment Systems or by DSIClient for Mercury Payment Systems.

It's important that unencrypted PANs never be transmitted by e-mail.

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

The number one reason for hacker fraud is Trojan/Backdoor virus intrusion, most commonly introduced to the network via employees' e-mail activities. Install and maintain updated anti-virus software on all computers and POS systems. VersiTouch recommends separating card processing functions from servers or PCs used for e-mail and/or web surfing and to also install an anti-virus suite of programs – such as Norton Anti-Virus or McAfee Anti-Virus — on all PCs on the network to detect viruses and other malware. Enable audit logs on your anti-virus program.

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations.

Check with your VAR to ensure you are using the latest versions of software applications. Old and insufficient technology is an open invitation for hackers. Don't take for granted that your VAR has informed you of possible vulnerabilities or updates. Remember, it is you who will be subject to fines if your business is compromised.

VersiTouch Credit is scheduled for a third-party audit by Coalfire Systems beginning in August of 2007. Legacy products such as RCS-100 POS, RCS-100 Back Office, RCredit, and RCS-Credit have not received updates since 2004 and will not be audited for PCI security issues. VersiTouch recommends that our merchants upgrade to VersiTouch POS/Office v9.2.18 or higher, and VersiTouch Credit v9.2.7 or higher, bearing in mind that newer versions of these programs may be forthcoming if issues are identified during the audit process. Updates can be obtained through your installing VAR or our website at www.versitouch.com.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

Passwords should always be used to limit access to cardholder information by business need-to-know.

Set user passwords on any PCs connecting to the VersiTouch POS network. Configure passwords and job/employee profiles within VersiTouch Office to restrict access to business-need-to-know functions.

Requirement 8: Assign a unique ID to each person with computer access

Ensure each employee has a unique user name and password to restrict access to computers and POS system data. Each employee with access to

POS functions should be assigned a unique password or mag-card. Make sure you update passwords when any trusted employee leaves your establishment.

Requirement 9: Restrict physical access to cardholder data

In addition to systems data access, ensure procedures are in place to restrict physical data access. Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data. Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. Store media back-ups and hard copies of cardholder data in a secure (preferably offsite) location. Destroy media containing cardholder data when it is no longer needed for business or legal reasons.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Track and monitor all access to network resources (i.e. computers, POS systems). You must be able to show proof of tracking. Retain audit trail history for at least one year, with a minimum of three months online availability.

VersiTouch POS automatically logs activity entered through the POS interface. You should configure VersiTouch Launch to restrict a user's ability to minimize or exit the POS interface, or that allow for terminal restart or shut down.

Additionally, sites should consider using Windows auditing to track activity in the following directories:

C:\RCS (and subdirectories)
C:\Program Files\VersiTouch (and subdirectories)

Requirement 11: Regularly test security systems and processes

Vulnerabilities are being discovered continually by hackers and researchers, and being introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.

Document a policy/schedule for testing of security systems and processes. You must be able to show proof of testing of your Internet security and policy processes.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

Document and maintain an enforceable policy that details safeguarding of payment card information. Be prepared to respond immediately to a system breach.

A compromise can be even more costly than the thousands of dollars spent on forensic audits and fines for non-compliance. It can cost you your reputation, your customers, even your business. Please make time to review these safeguards. Check them off, one by one, as you implement each one to protect your customers and your business.

For more information on PCI DSS, visit the PCI Security Standards Council's website at www.pcisecuritystandards.org or contact your installing VersiTouch reseller.

Part 6 – VersiTouch Security Vulnerabilities

This section provides specific configuration settings that you must implement in order to achieve PCI Compliance with VersiTouch products. Failure to follow these guidelines may require you to implement additional security measures to compensate for increased vulnerabilities. Our goal has always been to provide our merchant customers with the most flexible solutions to their unique issues in the hospitality industry. This gives you the flexibility to decide for yourself what risks are acceptable to your business. Our recommendation is to err on the side of caution (i.e. lock down your system as tight as possible while maintaining reasonable access to data to meet the needs of your business).

Following are specific guidelines and settings for each of our software products that must be maintained in order for you to achieve PCI Compliance:

VersiTouch Credit

- Create unique user accounts on the PC that runs VersiTouch Credit.
- Enable Windows auditing of the folder/directory (and subdirectories) where the merchant configuration file (.rcm) is located.
- Create unique user accounts for users, protected by strong passwords.*
- Limit the ability to manually settle credit card batches based on business need-to-know.*

VersiTouch Office/POS

- Create unique user accounts on any PCs that run VersiTouch Office.
- Enable Windows auditing of the C:\RCS folder/directory (and subdirectories).
- Create unique user accounts for users, protected by strong passwords.*
- Verify that user logging is enabled in SETUP. <default to "enabled">*
- Specifically limit the user ability to access PAYMENTS, REPORTS, and EMPLOYEE INFO based on business need-to-know.
- Verify settings for the Credit Card payment:
 - Select "Do NOT allow delete"
 - Deselect "Use Cr. Card ACCT# hold file"
 - Select either: "X out middle ACCT# digits" or "X all but last 4 digits"
 - Select "Don't print expiration"
 - Deselect "Show all info on merchant copy"

Sterling Manager/POS

- Create unique user accounts on any PCs that run Sterling Manager.
- Enable Windows auditing of the C:\Program Files\VersiTouch folder/directory (and subdirectories).
- Create unique user accounts for users, protected by strong passwords.*
- Verify that user logging is enabled.
- Specifically limit the user ability to access "Full PAN", PAYMENTS, and EMPLOYEE INFO based on business need-to-know.
- Verify settings for the Credit Card payment:
 - Deselect "Show all info on merchant copy"

Legacy products that do not meet the requirements of the PCI DSS:

RCS-100 POS

RCS-100 Back Office

RCredit

RCS-Credit

Part 8 – Additional Resources

Data and site security is a complex matter. We hope this guide has been of value to you in your ongoing evaluation of your business and technical operations and the role of your VersiTouch products within them.

Please remember that it is ultimately your sole responsibility to conform to the applicable security regulations, guidelines and standards for your type of business and processing volume.

VersiTouch, Inc., and our resellers can provide general suggestions and guidance, but the obligation to show and maintain compliance is yours. To assist you, here is a list of key reference resources that can serve as a starting point for your research:

- **PCI Security Standards Council:** Considerable information regarding this open global forum on security standards and data protection is at <http://www.pcisecuritystandards.org>. Here, for example, you can download the PCI Data Security Standards (PCI DSS) in their entirety.
- **Visa Cardholder Information Security Program (CISP):** The most recent information concerning CISP is at <http://www.visa.com/cisp>. Follow the appropriate links to determine your compliance obligations.
- **MasterCard Site Data Security (SDP):** The most recent information about SDP is at <https://sdp.mastercardintl.com>.
- **American Express Data Security Standards (DSS):** Review the latest high-level card security standards from American Express at http://www125.americanexpress.com/merchant/oam/ns/USEng/FrontServlet?request_type=navigate&page=generalRequirements.
- **Discover Card Information Security and Compliance (DISC):** You can get the latest information about the DISC program at http://www.discoverbiz.com/resources/data/data_security.html.

Some additional resources that may be applicable to you, depending on the type of merchant business you operate, are:

- **The Open Web Application Security Project (OWASP):** The free guides available at the OWASP site, <http://www.owasp.org>, are invaluable industry-standard resources, full of recommendations regarding installing and operating secure server-based applications.
- **Privacy Rights Clearinghouse:** A number of state laws regarding consumer privacy rights for credit card and check transactions can be found at <http://www.privacyrights.org/fs/fs15plus.htm>.

Appendix – Glossary

To help you understand the many terms, abbreviations and acronyms used in documents related to electronic payment system data security, here is a glossary compiled by the PCI Security Standards Council.

Term	Definition
AAA	Authentication, authorization, and accounting protocol
Accounting	Tracking of users' network resources
Access control	Mechanisms that limit availability of information or information processing resources only to authorized persons or applications
Account Harvesting	Process of identifying existing user accounts based on trial and error. [Note: Providing excessive information in error messages can disclose enough to make it easier for an attacker to penetrate and 'harvest' or compromise the system.]
Account number	Payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Primary Account Number (PAN)
Acquirer	Bankcard association member that initiates and maintains relationships with merchants that accept payment cards
AES	Advanced encryption standard. Block cipher adopted by NIST in November 2001. Algorithm is specified in FIPS PUB 197
ANSI	American National Standards Institute. Private, non-profit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system
Anti-Virus Program	Programs capable of detecting, removing, and protecting against various forms of malicious code or malware, including viruses, worms, Trojan horses, spyware, and adware
Application	Includes all purchased and custom software programs or groups of programs designed for end users, including both internal and external (web) applications
Approved standards	Approved standards are standardized algorithms (like in ISO and ANSI) and well-known commercially available standards (like Blowfish) that meet the intent of strong cryptography. Examples of approved standards are AES (128 bits and higher), TDES (two or three independent keys), RSA (1024 bits) and ElGamal (1024 bits)
Asset	Information or information processing resources of an organization
Audit Log	Chronological record of system activities. Provides a trail sufficient to permit reconstruction, review, and examination of sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from inception to final results.

	Sometimes specifically referred to as security audit trail
Authentication	Process of verifying identity of a subject or process
Authorization	Granting of access or other rights to a user, program, or process
Backup	Duplicate copy of data made for archiving purposes or for protecting against damage or loss
Cardholder	Customer to whom a card is issued or individual authorized to use the card
Cardholder data environment	Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment
Card Validation	<p>Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. The following list provides the terms for each card brand:</p> <p>CAV Card Authentication Value (JCB payment cards)</p> <p>CVC Card Validation Code (MasterCard payment cards)</p> <p>CVV Card Verification Value (Visa, Discover payment cards)</p> <p>CSC Card Security Code (American Express)</p> <p>Note: The second type of card validation value or code is the three-digit value printed to the right of the credit card number in the signature panel area on the back of the card. For American Express cards, the code is a four-digit unembossed number printed above the card number on the face of all payment cards. The code is uniquely associated with each individual piece of plastic and ties the card account number to the plastic. The following provides an overview:</p> <p>CID Card Identification Number (American Express and Discover payment cards)</p> <p>CAV2 Card Authentication Value 2 (JCB payment cards)</p> <p>CVC2 Card Validation Code 2 (MasterCard payment cards)</p> <p>CVV2 Card Verification Value 2 (Visa payment cards)</p>
Compensating controls	Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must 1) meet the intent and rigor of the original stated PCI DSS requirement; 2) repel a compromise attempt with similar force; 3) be "above and beyond" other PCI DSS requirements (not simply in compliance with

other PCI DSS requirements); and 4) be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement

CIS	Center for Internet Security. Non-profit enterprise with mission to help organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls
Compromise	Intrusion into computer system where unauthorized disclosure, modification, or destruction of cardholder data is suspected
Console	Screen and keyboard that permits access and control of the server or mainframe computer in a networked environment
Consumer	Individual purchasing goods, services, or both
Cookies	String of data exchanged between a web server and a web browser to maintain a session. Cookies may contain user preferences and personal information
Cryptography	Discipline of mathematics and computer science concerned with information security and related issues, particularly encryption and authentication and such applications as access control. In computer and network security, a tool for access control and information confidentiality
Database	Structured format for organizing and maintaining easily retrieved information. Simple database examples are tables and spreadsheets
Data Base Administrator	Individual responsible for managing and administering databases
Default accounts	System login account predefined in a manufactured system to permit initial access when system is first put into service
Default password	Password on system administration or service accounts when system is shipped from the manufacturer; usually associated with default account. Default accounts and passwords are published and well known
DES	Data Encryption Standard (DES). Block cipher elected as the official Federal Information Processing Standard (FIPS) for the United States in 1976. Successor is the Advanced Encryption Standard (AES)
DMZ	Demilitarized zone. Network added between a private and a public network to provide additional layer of security
DNS	Domain name system or domain name server. System that stores information associated with domain names in a distributed database on networks, such as the Internet
DSS	Data Security Standard
Dual Control	Process of using two or more separate entities (usually persons) operating in concert to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person is permitted to access or use the materials (for example, the cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires dividing knowledge of the key among the entities. See also, "split knowledge"
ECC	Elliptic curve cryptography. Approach to public-key cryptography

	based on elliptic curves over finite fields
Egress	Traffic exiting a network across a communications link and into the customer's network
Encryption	Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure
FIPS	Federal Information Processing Standard
Firewall	Hardware, software, or both that protect resources of one network from intruders from other networks. Typically, an enterprises with an intranet that permits workers access to the wider Internet must have a firewall to prevent outsiders from accessing internal private data resources
FTP	File transfer protocol
GPRS	General Packet Radio Service. Mobile data service available to users of GSM mobile phones. Recognized for efficient use of limited bandwidth. Particularly suited for sending and receiving small bursts of data, such as e-mail and web browsing
GSM	Global System for Mobile Communications. Popular standard for mobile phones Ubiquity of GSM standard makes international roaming very common between mobile phone operators, enabling subscribers to use their phones in many parts of the world
Host	Main computer hardware on which computer software is resident
Hosting Provider	Offer various services to merchants and other service providers. Services range from simple to complex; from shared space on a server to a whole range of "shopping cart" options; from payment applications to connections to payment gateways and processors; and for hosting dedicated to just one customer per server
HTTP	Hypertext transfer protocol. Open-internet protocol to transfer or convey information on the World Wide Web
ID	Identity
IDS/IPS	Intrusion Detection System/ Intrusion Prevention System. Used to identify and alert on network or system intrusion attempts. Composed of sensors that generate security events; a console to monitor events and alerts and control the sensors; and a central engine that records events logged by the sensors in a database. Uses system of rules to generate alerts in response to security events detected. An IPS takes the additional step of blocking the attempted intrusion.
IETF	Internet Engineering Task Force. Large open international community of network designers, operators, vendors, and researchers concerned with evolution of Internet architecture and smooth operation of Internet. Open to any interested individual
Information Security	Protection of information to insure confidentiality, integrity, and availability
Information System	Discrete set of structured data resources organized for collection, processing, maintenance, use, sharing, dissemination, or disposition of information

Ingress	Traffic entering the network from across a communications link and the customer's network
Intrusion Detection Systems	See IDS
IP	Internet protocol. Network-layer protocol containing address information and some control information that enables packets to be routed. IP is the primary network-layer protocol in the Internet protocol suite
IP address	Numeric code that uniquely identifies a particular computer on the Internet
IP Spoofing	Technique used by an intruder to gain unauthorized access to computers. Intruder sends deceptive messages to a computer with an IP address indicating that the message is coming from a trusted host
IPSEC	Internet Protocol Security (IPSEC). Standard for securing IP communications by encrypting and/or authenticating all IP packets. IPSEC provides security at the network layer
ISO	International Organization for Standardization. Non-governmental organization consisting of a network of the national standards institutes of over 150 countries, with one member per country and a central secretariat in Geneva, Switzerland that coordinates the system
ISO 8583	Established standard for communication between financial systems
Key	In cryptography, a key is an algorithmic value applied to unencrypted text to produce encrypted text. The length of the key generally determines how difficult it will be to decrypt the text in a given message
L2TP	Layer 2 tunneling protocol. Protocol used to support virtual private networks (VPNs)
LAN	Local area network. Computer network covering a small area, often a building or group of buildings
LPAR	Logical partition. Section of a disk which is not one of the primary partitions. Defined in a data block pointed to by the extended partition
MAC	Message authentication code
Magnetic Stripe Data (Track Data)	Data encoded in the magnetic stripe
Malware	Malicious software. Designed to infiltrate or damage a computer system, without the owner's knowledge or consent
Monitoring	Use of system that constantly oversees a computer network including for slow or failing systems and that notifies the user in case of outages or other alarms
MPLS	Multi protocol label switching.
NAT	Network address translation. Known as network masquerading or IP-masquerading. Change of an IP address used within one network to a different IP address known within another network
Network	Two or more computers connected together to share resources

Network Components	Include, but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances
Network Security Scan	Automated tool that remotely checks merchant or service provider systems for vulnerabilities. Non-intrusive test involves probing external-facing systems based on external-facing IP addresses and reporting on services available to external network (that is, services available to the Internet). Scans identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network
NIST	National Institute of Standards and Technology. Non-regulatory federal agency within U.S. Commerce Department's Technology Administration. Mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology to enhance economic security and improve quality of life
Non consumer Users	Any individual, excluding consumer customers, that accesses systems, including but not limited to employees, administrators, and third parties
NTP	Protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks
OWASP	Open Web Application Security Project (see http://www.owasp.org)
Payment Cardholder Environment	That part of the network that possesses cardholder data or sensitive authentication data
PAN	Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Account Number
Password	A string of characters that serve as an authenticator of the user
Pad	Packet assembler/disassembler. Communication device that formats outgoing data and strips data out of incoming packets. In cryptography, the one-time PAD is an encryption algorithm with text combined with a random key or " <i>pad</i> " that is as long as the plaintext and used only once. Additionally, if key is truly random, never reused, and, kept secret, the one-time pad is unbreakable
PAT	Port address translation. Feature of a network address translation (NAT) device that translates transmission control protocol (TCP) or user datagram protocol (UDP) connections made to a host and port on an outside network to a host and port on an inside network
Patch	Quick-repair job for piece of programming. During software product beta test or try-out period and after product formal release, problems are found. A patch is provided quickly to users
PCI	Payment Card Industry
Penetration	Successful act of bypassing security mechanisms and gaining access to computer system
Penetration Test	Security-oriented probing of computer system or network to seek out vulnerabilities that an attacker could exploit. Beyond probing for vulnerabilities, this testing may involve actual penetration attempts. The objective of a penetration test is to detect identify vulnerabilities and suggest security improvements

PIN	Personal identification number
Policy	Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures
POS	Point of sale
Procedure	Descriptive narrative for a policy. Procedure is the “how to” for a policy and describes how the policy is to be implemented
Protocol	Agreed-upon method of communication used within networks. Specification that describes rules and procedures that computer products should follow to perform activities on a network
Public Network	Network established and operated by a telecommunications provider or recognized private company, for specific purpose of providing data transmission services for the public. Data must be encrypted during transmission over public networks as hackers easily and commonly intercept, modify, and/or divert data while in transit. Examples of public networks in scope of PCI DSS include the Internet, GPRS, and GSM.
PVV	PIN verification value. Encoded in magnetic stripe of payment card
RADIUS	Remote authentication and dial-In user service. Authentication and accounting system. Checks if information such as username and password that is passed to the RADIUS server is correct, and then authorizes access to the system
RFC	Request for comments
Re-keying	Process of changing cryptographic keys to limit amount of data to be encrypted with the same key
Risk Analysis	Process that systematically identifies valuable system resources and threats; quantifies loss exposures (that is, loss potential) based on estimated frequencies and costs of occurrence; and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure. Risk assessment
Router	Hardware or software that connects two or more networks. Functions as sorter and interpreter by looking at addresses and passing bits of information to proper destinations. Software routers are sometimes referred to as gateways
RSA	Algorithm for public-key encryption described in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at Massachusetts Institute of Technology (MIT); letters RSA are the initials of their surnames
Sanitization	Process for deleting sensitive data from a file, device, or system; or for modifying data so that it is useless if accessed in an attack
SANS	SysAdmin, Audit, Network, Security Institute (See www.sans.org)
Security Officer	Primary responsible person for security related affairs of an organization
Security policy	Set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information
Sensitive Authentication Data	Security-related information (Card Validation Codes/Values, complete track data, PINs, and PIN Blocks) used to authenticate cardholders, appearing in plaintext or otherwise unprotected form.

	Disclosure, modification, or destruction of this information could compromise the security of a cryptographic device, information system, or cardholder information or could be used in a fraudulent transaction
Separation of duties	Practice of dividing steps in a function among different individuals, so as to keep a single individual from being able to subvert the process
Server	Computer that provides a service to other computers, such as processing communications, file storage, or accessing a printing facility. Servers include, but are not limited to web, database, authentication, DNS, mail, proxy, and NTP
Service Code	Three- or four-digit number on the magnetic-stripe that specifies acceptance requirements and limitations for a magnetic-stripe read transaction.
Service Provider	Business entity that is not a payment card brand member or a merchant directly involved in the processing, storage, transmission, and switching of transaction data and cardholder information or both. This also includes companies that provide services to merchants, services providers or members that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded
SHA	Secure Hash Algorithm. A family or set of related cryptographic hash functions. SHA-1 is most commonly used function. Use of unique salt value in the hashing function reduces the chances of a hashed value collision
SNMP	Simple Network Management Protocol. Supports monitoring of network-attached devices for any conditions that warrant administrative attention
Split knowledge	Condition in which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic key
SQL	Structured (English) Query Language. Computer language used to create, modify, and retrieve data from relational database management systems
SQL injection	Form of attack on database-driven web site. An attacker executes unauthorized SQL commands by taking advantage of insecure code on system connected to the Internet. SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization's host computers through the computer that is hosting the database
SSH	Secure shell. Protocol suite providing encryption for network services like remote login or remote file transfer
SSID	Service set identifier. Name assigned to wireless WiFi or IEEE 802.11 network

SSL	Secure sockets layer. Established industry standard that encrypts the channel between a web browser and web server to ensure the privacy and reliability of data transmitted over this channel
Strong Cryptography	<p>General term to indicate cryptography that is extremely resilient to cryptanalysis. That is, given the cryptographic method (algorithm or protocol), the cryptographic key or protected data is not exposed. The strength relies on the cryptographic key used. Effective size of the key should meet the minimum key size of comparable strengths recommendations. One reference for minimum comparable strength notion is NIST Special Publication 800-57, August, 2005 (http://csrc.nist.gov/publications/) or others that meet the following minimum comparable key bit security:</p> <ul style="list-style-type: none"> • 80 bits for secret key based systems (for example TDES) • 1024 bits modulus for public key algorithms based on the factorization (for example, RSA) • 1024 bits for the discrete logarithm (for example, Diffie-Hellman) with a minimum 160 bits size of a large subgroup (for example, DSA) • 160 bits for elliptic curve cryptography (for example, ECDSA)
System Components	Any network component, server, or application included in or connected to the cardholder data environment
TACACS	Terminal access controller access control system. Remote authentication protocol
Tamper-resistance	System that is difficult to modify or subvert, even for an assailant with physical access to the system
TCP	Transmission control protocol
TDES	Triple Data Encryption Standard also known as 3DES. Block cipher formed from the DES cipher by using it three times
TELNET	Telephone network protocol. Typically used to provide user-oriented command line login sessions between hosts on the internet. Program originally designed to emulate a single terminal attached to the other computer
Threat	Condition that may cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the organization
TLS	Transport layer security. Designed with goal of providing data secrecy and data integrity between two communicating applications. TLS is successor of SSL
Token	Device that performs dynamic authentication
Transaction data	Data related to electronic payment
Truncation	Practice of removing data segment. Commonly, when account numbers are truncated, the first 12 digits are deleted, leaving only the last 4 digits
Two-factor authentication	Authentication that requires users to produce two credentials to access a system. Credentials consist of something the user has in their possession (for example, smartcards or hardware tokens) and something they know for example, a password). To access a system, the user must produce both factors

UDP	User datagram protocol
UserID	A character string used to uniquely identify each user of a system
Virus	Program or string of code that can replicate itself and cause modification or destruction of software or data
VPN	Virtual Private Network. Private network established over a public network
Vulnerability	Weakness in system security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy
Vulnerability Scan	Scans used to identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network
WEP	Wired equivalent privacy. Protocol to prevent accidental eavesdropping and intended to provide comparable confidentiality to traditional wired network. Does not provide adequate security against intentional eavesdropping (for example, cryptanalysis)
WPA	WiFi Protected Access (WPA and WPA2). Security protocol for wireless (WiFi) networks. Created in response to several serious weaknesses in the WEP protocol
XSS	Cross-site scripting. Type of security vulnerability typically found in web applications. Can be used by an attacker to gain elevated privilege to sensitive page content, session cookies, and variety of other objects