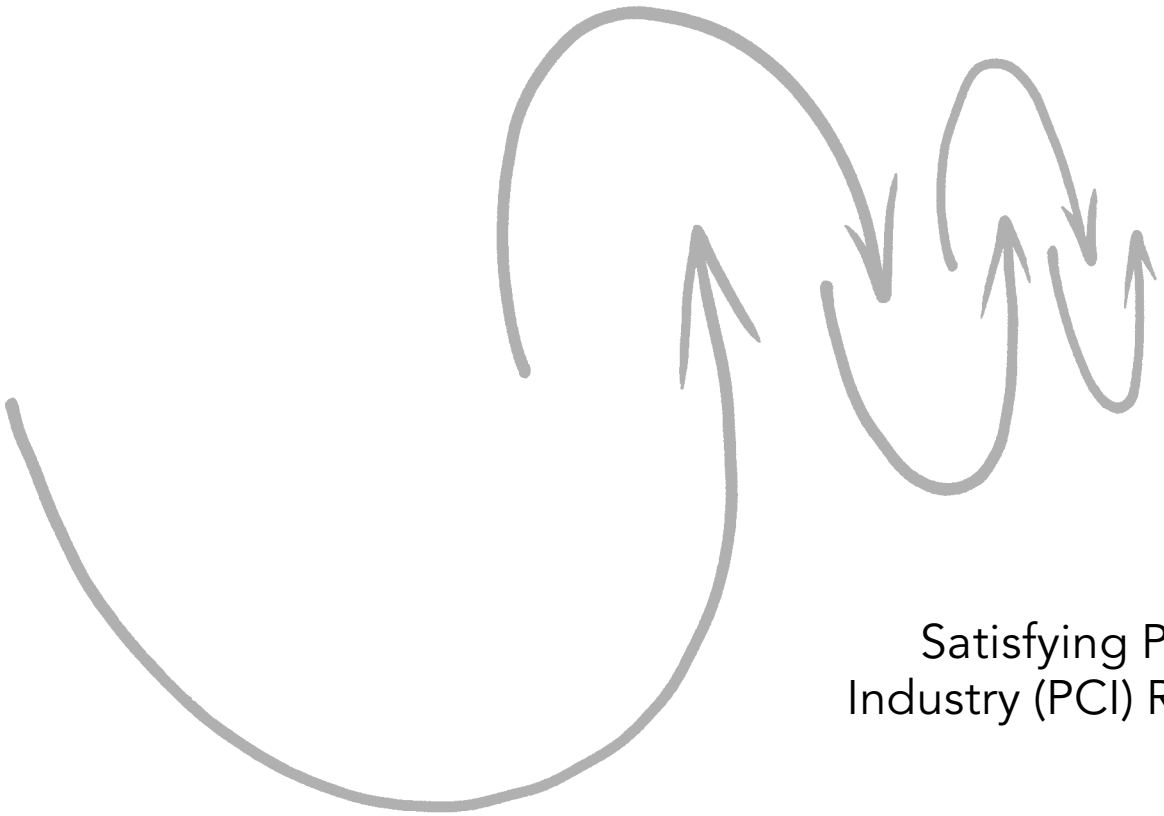
STERLING COMMERCE WHITE PAPER

Protect Your Cardholder File Transfers Against Data Breaches



Satisfying Payment Card Industry (PCI) Requirements

Sterling Commerce
An IBM Company

Protect Your Cardholder File Transfers Against Data Breaches and Satisfy Payment Card Industry (PCI) Requirements

Identity theft and credit card crime are on the rise.

Organizations today rely increasingly on open protocols and the Internet for business-to-business file transfers. Security attacks have become ever more sophisticated in targeting institutions for financial gain. "All sensitive electronic data needs to be protected, but enterprises should be aware that the low hanging fruit for the criminals is electronic card and checking account numbers, as well as user IDs and passwords for online financial accounts," said Avivah Litan, vice president and distinguished analyst at Gartner[1]. According to Gartner, unauthorized credit card charges increased fourfold from 2005 to 2006.

Identity theft is the crime of the 21st century. Results feature eroding consumer confidence and escalating costs that include liability and litigation. In its 2006 data security survey, Ponemon Institute[2], a leading research institute on privacy and data protection practices, estimated an average cost of $182 per lost customer record and an average total cost of $4.8 million per breach — a 30% increase over 2005.

Consumer credit card information is an attractive target for criminals across the world. Selling fraudulently-obtained credit card information over the Internet is a growing business for the new breed of cyber criminals. While virus and phishing may obtain the credit card information of a few thousand cardholders, hacking into a single large retailer's database is a lot more lucrative, granting access to millions of cardholder accounts. A recent example is the security breach at TJX (parent company of TJ Maxx department stores) that compromised approximately 45 million cardholder accounts.

The most recent Internet security threat report released by Symantec Corporation[3] reveals "an increase in data theft, data leakage, and the creation of targeted malicious code for the purpose of stealing confidential information that can be used for financial gain. Cyber criminals continue to refine their attack methods in an attempt to remain undetected and to create global, cooperative networks to support the ongoing growth of criminal activity.

Symantec Corporation has been tracking and monitoring underground economy servers across the Internet. Underground economy servers are used by cyber criminals to sell stolen information, including credit cards, bankcards and personal identification numbers (PINs), for subsequent use in identity theft. According to the Symantec Internet Security Threat Report, 51% of underground economy servers are located in the United States and most of the credit cards for sale are those issued by US banks. Simple economics — an abundant supply of fraudulently obtained credit cards issued in the United States — may well be the reason that stolen credit cards issued in the United States sell for half the price of those issued in the United Kingdom.

---

1 Gartner research: *The Truth behind Identity Theft Numbers:* Avivah Litan, February 28, 2007.

2 *U.S. Survey: Confidential Data at Risk* published by Ponemon Institute LLC, August 15, 2006

3 *Symantec Internet Security Threat Report; Trends for July -December 06*, Vol. XI, Published March 2007

Symantec Corporation lists the following prices of items traded on underground economy servers:

Identity Theft Items for Sale	Price (US dollars)
United States based credit-card with card verification value	$1–$6
United Kingdom based credit-card with card verification value	$2–$12
An identity (including US bank account, credit card, date of birth, and government issuing identification number)	$14–$18
List of 29,000 emails	$5
Online banking account with a $9,900 balance	$300
Yahoo mail cookie exploit advertised to facilitate full access when successful	$3
Valid Yahoo and Hotmail email cookies	$3
Compromised computer	$6–$20
Phishing Web site hosting — per site	$3–$5
Verified PayPal account with balance (balance varies)	$50–$500
Unverified PayPal account with balance (balance varies)	$10–$50

(Source: Symantec Internet Security Threat Report, Trends for July–December 06, Vol. XI, Published March 2007).

Background — Payment Card Industry Data Security Standards

Numerous high profile security breaches over the past few years, including those at TJX Companies, Sam's Club, and CardSystems Inc., have consumers and credit card companies on the hunt for answers. The major credit card companies, Visa, MasterCard, Discover, American Express and JCB implemented a set of security standards called Payment Card Industry Data Security Standards (PCIDSS). PCIDSS aims to reduce the risk of Internet attacks with the use of firewall configuration, antivirus software, data encryption and additional security best practices.

Payment Card Industry Data Security Standards (PCIDSS) refers to a framework of twelve common security requirements for the credit card industry developed by MasterCard and Visa. Initially published in 2005, these standards were updated in September, 2006. At the same time the PCI Security Standards Council, an independent organization responsible for developing and overseeing the standards, was also established. The deadline for compliance with PCIDSS (version 1.1) for level 1 and level 2 merchants is September 30, 2007.

Level 1 and Level 2 merchants categories are:

Level 1:

- Processing over 6,000,000 Visa transactions per year
- Have suffered a hack or an attack resulting in an account data compromise
- Visa or another payment card has determined should meet the Level 1 merchant requirement

Level 2:

- Processing 1,000,000 to 6,000,000 Visa transactions per year

Visa is stepping up PCI enforcement with serous consequences for non-compliance, including hefty fines and refusal to allow organizations to use the Visa brand. In 2005, Visa and MasterCard terminated CardSystems Inc. as a transactions processor after a hacker stole 263,000 customer credit card accounts and exposed 40 million more. The Federal Trade Commission also charged CardSystems for putting tens of millions of customers' sensitive information at risk.

Verisign® was one of the first organizations to conduct audits and scans for PCI compliance. Information gathered from customer PCI assessments conducted over a four-year period by Verisign's Global Security Consulting Services[4], the ten most commonly failed PCI requirements and the percentage of non-compliance for each are:

[4] *Lessons Learned: Top Reasons for PCI Audit Failure and How to Avoid Them*, Verisign Global Security Consulting Services, June 2006.

©2007. Sterling Commerce, Inc.

PCI Requirement	Percentage failing assessments
Requirement 3: Protect Stored Data	79%
Requirement 11: Regularly test security systems and processes	74%
Requirement 8: Assign a unique ID to each person with computer access	71%
Requirement 10: Track and monitor all access to network resources and cardholder data	71%
Requirement 1: Install and maintain a firewall configuration to protect data	66%
Requirement 2: Do not use vendor supplied defaults for system passwords and other security parameters	62%
Requirement 12: Maintain a policy that addresses information security	60%
Requirement 9: Restrict physical access to cardholder data	59%
Requirement 6: Develop and maintain secure systems and applications	56%
Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks	45%

In 2006, Visa charged acquiring institutions over $4.6 million in fines. Acquiring institutions process and deposit credit card trnasactions into merchant accounts. Visa now uses a "carrot and stick" approach that offers acquiring institutions financial incentives for merchant compliance and stiff penalties for non-compliance. The Visa Compliance Acceleration Program (CAP) has invested some $20 million as incentive to acquiring financial institutions that validate PCI compliance by August 31, 2007 for merchants that have not suffered a data breach. On the other hand, Visa will fine acquiring institutions $5,000 and $25,000 per month, for each merchant that is not PCI compliant by stipulated deadlines.

However, many merchants and processors are still not clear on how to meet PCIDSS requirements. PCIDSS is very large in scope and while it is a guide for PCI compliance, it does not give instructions on how organizations are to meet each requirement. Strategies and techniques used to meet PCI compliance need to be tailored to each organization's unique credit card processing environment. In addition, the tight deadline for PCI compliance puts additional pressure on merchants.

Credit card transactions involve the capture, processing and routing of cardholder information during authorization and settlement of cardholder information. This information is exchanged in the form of electronic files, that are often transmitted internally within organizations and externally between merchants, processors and banks. Since credit card authorization and settlement transactions involve capturing, processing and routing of sensitive cardholder data, this information must be kept secure during each step in the process.

Sterling Commerce provides managed file transfer solutions that facilitate the secure movement of files containing confidential information, including credit card data. For decades, banks, government agencies and other organizations have used our solutions to transfer sensitive and confidential information in a secure and reliable way. The IBM® Sterling Managed File Transfer solution has never been breached.

The next section discusses specific Sterling Managed File Transfer capabilities that provide increased security for your cardholder file environment and facilitate satisfying PCI requirements.

©2007. Sterling Commerce, Inc.

How Sterling Managed File Transfer Solutions Facilitate Compliance with PCI Requirements

PCIDSS includes twelve requirements grouped under six categories as displayed below.

The PCIDSS Framework

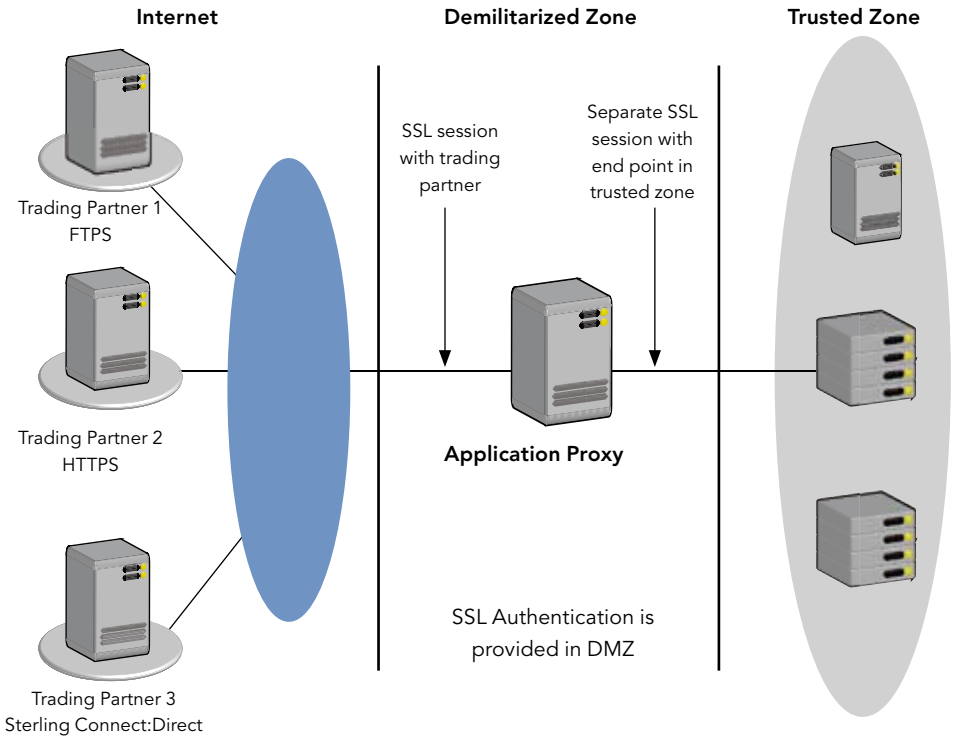
Build and Maintain a Secure Network	
Requirement #1:	Install and maintain a firewall configuration to protect cardholder data
Requirement # 2:	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	
Requirement # 3:	Protect stored cardholder data
Requirement # 4:	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	
Requirement # 5:	Use and regularly update anti-virus software
Requirement # 6:	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	
Requirement # 7:	Restrict access to cardholder data by business need-to-know
Requirement # 8:	Assign a unique ID to each person with computer access
Requirement # 9:	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	
Requirement # 10:	Track and monitor all access to network resources and cardholder data
Requirement # 11:	Regularly test security system and processes
Maintain and Information Security Policy	
Requirement # 12:	Maintain a policy that addresses information security

The twelve PCIDSS requirements are extensive in scope and the "one size fits all" approach does not work for meeting compliance with PCI requirements. The optimal solution depends upon each organization's unique business needs and credit card information processing environment. Sterling Managed File Transfer solutions can help with several requirements, specifically with the secure transmissions of sensitive cardholder data, both within the global enterprise and across multiple trading partners.

PCI Requirement 1.2: Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.
Sterling Commerce provides "defense in depth" with our suite of file transfer solutions. A "defense-in-depth" approach provides multiple layers of defense and a combination of security techniques that often overlap to provide increased protection from unauthorized access to sensitive and confidential information. Just as firewalls provide layers of security at the network layer, Sterling Commerce can provide similar capabilities at the application layer. Whether you use FTP, FTP(s), HTTP, HTTP(s) or IBM® Sterling Connect:Direct® to transfer files, we provide application level proxy capabilities. Such capabilities provide the required separation of the trusted environment from the external one.

Sterling Commerce proxy capability enforces an SSL session break with the external client and authenticates the remote trading partner in the DMZ before establishing a separate SSL session with the internal application. This prevents direct communications between the external trading partner and the internal network. By authenticating the remote trading partner in the DMZ before establishing a separate session to the trusted zone, the internal network is better protected from external threats.

©2007. Sterling Commerce, Inc.



Session limits and support for SSL and TLS encryption algorithms guard against common attacks like man-in-the-middle and eavesdropping to ensure business continuity. The proxy capability provides protocol inspection and sensitive control information, enabling configurable error handling for protocol violations.

Sterling Commerce proxy capability eliminates the need to open multiple ports in your firewall. The application proxy establishes sessions between the trusted zone and the DMZ using tunneling technology that eliminates the need to open multiple ports. As an added measure of safety, sessions are established from the trusted zone to the DMZ.

Mutual Authentication is also enforced where each trading partner is required to present a certificate as part of the SSL protocol. This certificate can be checked against a Certification Revocation List (CRL) via the Lightweight Directory Access Protocol (LDAP) or the subject name of the certificate can be located in LDAP to validate that the remote client is a trusted trading partner.

With Sterling Commerce multifactor authentication capability, organizations' gain more stringent validation of trading partner identity. Sterling Managed File Transfer solutions have the capability to perform configurable certificate validation functions, including CRL Checking, Standard Certificate Validation, Application Policy Enforcement, and LDAP queries.

PCI Requirement 1.3: Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks.
Sterling Commerce application proxy terminates all sessions in the DMZ. All inbound connections are restricted from reaching the trusted zone. A separate SSL session is generated between the trusted zone and the DMZ once the trading partner is successfully authenticated in the DMZ. Thus the trusted zone environment is a separate environment from the external environment.

©2007. Sterling Commerce, Inc.

The use of the application proxy eliminates the need for storing data in the DMZ. No cardholder information is saved in the DMZ when the proxy is deployed in the DMZ. The proxy authenticates incoming traffic to validate trading partner identity before establishing a separate connection to the trusted zone. The proxy gives you the ability to deny all inbound and outbound traffic that is not specifically allowed.

PCI Requirement 1.4 Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).
By enforcing SSL session breaks between external trading partners and the trusted zone, the application proxy prohibits direct access from external networks to the trusted zone.

The application proxy restricts outbound traffic with a forward proxy capability that locks down the firewall. All outbound sessions are directed to the proxy in the DMZ, which then routes it to the appropriate trading partner. This allows companies to enforce their security policies for all outgoing sessions.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

PCI Requirement 4.1: Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

Unauthorized access to data is a problem that all companies face when they transmit sensitive customer information. Sterling Commerce capabilities include comprehensive cryptographic security for data exchange to ensure that your sensitive cardholder data is transferred with the utmost safety and surety. Sterling Commerce has also taken steps to further strengthen encryption capabilities by achieving FIPS 140-2 and Common Criteria certifications for its Sterling Connect:Direct products. FIPS 140-2 is a standard by which cryptographic solutions are certified against predefined requirements. Today this certification is recognized in Canada and the United States but other countries are showing interest in FIPS 140-2. Common Criteria is an international standard that is recognized by 22 countries. Common Criteria evaluates a product's security capabilities, not just cryptographic capabilities. In addition, this standard evaluates the processes used by vendors to construct its products. The evaluation of Sterling Commerce solutions by third party evaluators provides added confidence for companies that utilize these solutions to solve key data transmission requirements, including the movement of credit card transaction data.

Sterling Managed File Transfer provides strong mutual authentication, data encryption and data integrity checking. Encryption capabilities use X.509 certificates to identify entities with which cardholder data is being shared. Strong mutual authentication occurs each time a session is established using our file transfer solutions.

Sterling Managed File Transfer solutions help you keep sensitive cardholder data confidential and hidden from prying eyes by employing secure transport technologies including Secure Sockets Layer (SSL), Transport Layer Security (TLS) and Station-to-Station (STS) protocols. It ensures data integrity with industry standard hashing algorithms and terminates the transfer at the first indication of tampering.

Requirement 10: Track and monitor all access to network resources and cardholder data.
Sterling Managed File Transfer offers full capabilities for defining and managing user accounts, including a platform-appropriate interface. Capabilities include the ability to define user IDs and passwords, to activate and expire access and define role-based permissions. Log files are consolidated into a central database with over 50 standard reports and custom reporting through Crystal Reports.

©2007. Sterling Commerce, Inc.

Our solutions allow you to manage your file transfer operations using a centralized or decentralized structure. Our solution gives you the ability to analyze operational metrics, which facilitates auditing and reporting. You gain the ability to audit data movement activities and gain insight into questions like who moved what, when and how.

With Sterling Managed File Transfer solutions, you gain the ability to run numerous standard as well as custom reports. You can query, view and save reports in multiple formats. Flexible analysis for customized reporting helps address compliance requirements. Our solutions also provide detailed audit logs that can be used for non-repudiation purposes.

Summary

With the increase in identity theft and account fraud, credit card security breaches are the focus of media attention, as institutions risk millions of dollars and cardholders suffer from the consequences of identity theft. This has resulted in a push for stronger legislation to mandate strict security requirements that organizations keep sensitive consumer information secure. Currently, several states within the United States are considering legislation to make retailers and merchants responsible for security breaches. Costs associated with credit card data breaches are escalating and the long-term damage to an organization's reputation is often irreparable. Businesses need to adopt a proactive approach in securing cardholder data to avoid becoming the next headline due to a data breach.

In an age of growing identify theft and account fraud, the practical approach is to take adequate measures to protect against such attacks. It just makes good business sense to take a proactive approach and make security a top priority to protect your information assets from unauthorized access. At a very minimum, organizations need to comply with requirements like PCI and then build upon them to deploy security strategies that reduce the risk of security breaches. At the very top of its list of recommended enterprise best practices, Symantec lists the need to "employ defense-in-depth strategies, which emphasize multiple, overlapping and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method." [5]

Organizations often feel the need to justify putting adequate security measures in place by quantifying the ROI of compliance. While one can take into account the costs of implementing security measures, potential fines and other associated costs, it is difficult to measure the benefit derived from protecting against security breaches until such a breach occurs — and by then it may be too late. When focusing on the ROI of compliance, keep in mind that it may well be the cost of going out of business, because a major security incident could very easily drive an organization to bankruptcy.

5 *Symantec Internet Security Threat Report*, vol. XI, published March 2007.

©2007. Sterling Commerce, Inc.

About Sterling Commerce

Sterling Commerce, an IBM® Company, helps organizations worldwide increase business agility in their dynamic business network through innovative solutions for selling and fulfillment and for seamless and secure integration with customers, partners and suppliers. More information can be found at **www.sterlingcommerce.com.**

Sterling Commerce
An IBM Company

For all Sterling Commerce offices worldwide, visit **www.sterlingcommerce.com**

©2007–2010, Sterling Commerce, Inc.
All rights reserved. Sterling Commerce and the Sterling Commerce logo are trademarks of Sterling Commerce, Inc. or its affiliated companies. All products referenced are the service marks, trademarks, or registered marks of their respective owners. Printed in U.S.A.
SC0482 12/10