



# Shopping For a Secure File Transfer Solution For Retail

Research and best practices provided by the PCI Knowledge Base Sponsored by Ipswitch File Transfer

# Shopping For a Secure File Transfer Solution For Retail

W H I T E P A P E R

## ABSTRACT

Retailers and merchant service providers are under increasing pressure to adhere to PCI DSS in an effort to avoid costly fines — and the even more detrimental loss of customer confidence that results from data leakage or data breaches. PCI DSS compliance requires organisations to protect the security, privacy, and confidentiality of cardholder information — and to document who accesses the information and the security measures taken to prevent theft, loss, or accidental disclosure. Ipswitch secure file transfer solutions deliver a proven, simple, and innovative method for exceeding your PCI DSS compliance needs.

## Shopping for a Secure File Transfer Solution for Retail

In March 2008, the Hannaford grocery chain in the U.S. acknowledged that 4.2 million credit and debit cards used at its stores in six states were compromised over a three-month period. According to Hannaford, malware loaded onto more than 300 servers resulted in card numbers and expiration dates being transferred overseas while in transit at the point of sale scanner. The attack occurred even though Hannaford had received Payment Card Industry Data Security Standard (PCI DSS) certification, and ironically was underway at the time the PCI DSS audit was being conducted. The company is currently spending millions of dollars to enhance the security of its data network.

Over a period of 18 months during 2005 to 2007, hackers gained access to major worldwide retailer TJX's networks, which includes TK Maxx, and stole more than 94 million credit cards. The data was accessed on TJX's computer systems in Watford, Hertfordshire, and Framingham, Massachusetts and covers transactions made by credit and debit cards dating as far back as December 2002. This high-profile breach became the poster child for lax corporate security practices, irreparably damaging TJX's reputation. SEC filings indicate that the total cost of the security breach could top \$250 million, with the financial aftermath affecting TJX through 2010.

“Retail security managers are committed to PCI, because it helps them get budget, but upper management, outside of the largest retailers, just want a green ROC. Some are still fighting PCI, arguing that their risk is too low to justify the spend, and they are not going to do anything until there are some real penalties or they have a breach or someone they know has a breach.”

PCI Knowledge Base  
Contributor, April 2008

# Shopping For a Secure File Transfer Solution For Retail

W H I T E P A P E R

In 2005, payment processor CardSystems admitted that more than 40 million credit card numbers were exposed after its systems were hacked. Visa and American Express stopped doing business with CardSystems, a class action lawsuit was filed, an FTC settlement was reached, and the company's assets were acquired by Pay By Touch Solutions later that year.

While each of these security breaches had different causes — external hacker breaches, insecure data transfer, and network security lapses — they had one thing in common: a too-casual approach to data protection.

## Securing Retail Transactions

As increasing volumes of business and customer data are sent over internal networks and the Internet, retailers are coming under greater pressure to implement security best practices that ensure secure cardholder information and regulatory compliance.

In response to these challenges, American Express, Discover, JCB, MasterCard, and Visa agreed in 2004 to create industry standards to help prevent theft of consumers' data. The five companies merged their separate data security programs to form an independent council to manage PCI DSS and secure payment account data in a globally consistent manner. The PCI DSS standards require any organisation that accepts, stores, communicates, or processes credit card transactions to protect the security, privacy, and confidentiality of cardholder information, and track who accesses it and the security measures taken to prevent theft, loss, or accidental disclosure.

PCI DSS compliance affects every organisation involved in payment transactions, from acquiring banks, issuing banks, and card associations, to cardholders, merchants, and third-party processors. As information is passed among these entities, every touch point becomes a potential opportunity for a data breach. PCI DSS requirements apply

### What is PCI DSS?

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. This comprehensive standard is intended to help organisations proactively protect customer account data. The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organised:

### Build and Maintain a Secure Network

- Req 1: Install and maintain a firewall configuration to protect cardholder data
- Req 2: Do not use vendor-supplied defaults for system passwords and other security parameters

# Shopping For a Secure File Transfer Solution For Retail

W H I T E P A P E R

any time when customer payment card account numbers are stored, processed, or transmitted. What is not well known is that the security requirements apply to effectively every component that makes up the network, defined as “any network component, server, or application that is included in or connected to the cardholder data environment.”

While merchant adoption of PCI DSS was initially slow, 2007 saw significant increases in the number of compliant merchants. According to Visa, compliance among the largest U.S. merchants grew from about 12 percent in March 2006 to 77 percent by December 31, 2007. Among midsize merchants, compliance grew from 15 percent in December 2006 to 62 percent as of December 31, 2007.

Failure to comply carries significant penalties. In addition to the loss of consumer confidence, noncompliant merchants can face large fines. Visa recently began levying monthly fines of \$25,000 to merchant banks (or acquirers) for each large merchant that hadn't validated PCI DSS compliance by the deadline. As of January 2008, Visa is levying monthly fines of \$5,000 to U.S. acquirers for noncompliant midsize merchants. And even PCI DSS compliant organisations can be fined for doing business with a noncompliant merchant.

## Security Beyond PCI DSS Compliance

As the Hannaford data breach shows, it is possible to be in compliance with industry regulations and yet not be fully secure. Every company must understand its threat profile, define its risk tolerance, and design best practices that may extend regulations such as PCI DSS to accommodate specific business practices and threat opportunities.

Your threat profile includes an understanding of your employees, customers, vendors, and systems. Are there weaknesses in any of these that make you especially vulnerable to data breaches? Examples could include a transient, low-paid workforce, poor security practices with your business partners, or insecure payment processes.

### Protect Cardholder Data

Req 3: Protect stored cardholder data

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

### Maintain a Vulnerability Management Program

Req 5: Use and regularly update anti-virus software

Req 6: Develop and maintain secure systems and applications

### Implement Strong Access Control Measures

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

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

Requirement 9: Restrict physical access to cardholder data

# Shopping For a Secure File Transfer Solution For Retail

W H I T E P A P E R

Your risk tolerance involves balancing the need for security with your ability to conduct business with your customers and vendors. How much risk can and should you tolerate?

While PCI DSS lays out important steps for securing retail transactions, it's up to you to define how your company will manage these steps. What tools, techniques, and processes will you put in place to effectively manage PCI DSS compliance and data security? These best practices can be the difference between the veneer of security and the reality.

## Is Your Company at Risk?

In assessing your company's risk of experiencing a security breach, there are a number of fundamental questions you should ask. If these questions cannot be answered satisfactorily, you likely have data vulnerabilities that are just waiting to be exposed.

- Who has access to your sensitive files and data?
- Who in your organization is responsible for compliance?
- What would be the impact if your sensitive company information was compromised?
- When, how often, and exactly what information is being exchanged?
- Where and with whom is your data being sent, both inside and outside your company?
- Do the areas of your network that handle PCI data touch other areas used for other business functions? Should they?
- How does regulatory compliance affect the way data needs to be handled and audited?
- Do you allow employees and partners to share your files over insecure FTP, email, and IM?

### Regularly Monitor and Test Networks

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

Req 11: Regularly test security systems and processes

### Maintain an Information Security Policy

Req 12: Maintain a policy that addresses information security  
Source:

[www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

# Shopping For a Secure File Transfer Solution For Retail

W H I T E P A P E R

With a clear understanding of how data moves both within your organization and among your business partners, you can begin to craft a compliance strategy that will govern and safeguard this information and provide protection for you and your customers.

## FTP, Email, and IM are Inadequate for Current Needs

Considering the file transfer and storage challenges facing retailers today, standard FTP, email, and IM are inappropriate options for managing secure data transfer. These insecure, unencrypted methods expose you to information breaches, and fail to provide a comprehensive way to manage and track information flow and security.

## A Better Way to Ensure Data Security

A few common encrypted file transfer protocols that help secure and increase the reliability of data transfer are Secure Sockets Layer (SSL), Secure Shell (SSH), and Electronic Data Interchange-Internet Integration (EDIINT) protocols such as AS2 and AS3. These are specifically designed to encrypt file transfers as well as the associated administrative network traffic. SSL and SSH enhance the security and reliability of file transfer by using encryption to protect against unauthorised viewing and modification of high-risk data during transmission across open networks such as the Internet. AS2 and AS3 “Applicability Statement” protocols define methods for securely exchanging structured data over the Internet. These AS protocols provide data protection and non-repudiation using S/MIME, digital signatures and Message Disposition Notifications (MDNs) for data encryption, authentication, and data integrity checking, respectively.

According to PCI DSS regulations, data must also be protected when it is in storage, or at rest. Combining SSL and SSH security with OpenPGP provides an additional level of protection for data at rest. OpenPGP encrypts files in storage through the use of cryptographic key pairs that authenticate users and data. Receivers need to use the corresponding private key to decrypt the file.

## Four Critical Considerations

When evaluating technology solutions for data security, you should look at how four categories — confidentiality, integrity, availability, and auditing — contribute to compliance.

Confidentiality includes authentication of login credentials and ensuring you have a strong password policy in place, with features like expiring accounts and password management. Access control includes support for 256-bit AES SSL encryption and TLS 1.1 or higher on all connections. This level of access should be mandatory for all clients connecting

# Shopping For a Secure File Transfer Solution For Retail

W H I T E P A P E R

into your infrastructure. If the clients connecting to your file transfer platform can't connect at 256-bit SSL or SSH or higher, access should be denied in order to protect your company from a potential data breach.

Integrity means ensuring you have uncompromised delivery of all correct data with full SHA-512 support. Secure, encrypted data delivery is critical for ensuring business continuity. Secure hashing algorithms ensure that files have not been compromised during transport, and that the source and destination files are exact matches. A single change in a file or writing a file to a bad sector on a disk can corrupt a file and produce faulty workflow notifications and business process events.

Availability can be achieved through load balancing and clustering architectures that support failover and centralized data to minimize the chance of a data breach. This also helps protect against anti-hammering and distributed denial of service attacks.

Auditing provides comprehensive logging and log viewing with analysing capabilities, and includes reporting and event driven notifications and workflow to ensure you know what's happening on your network, and that you'll be ready to respond in the event of compliance audit.

## Ipswitch File Transfer: Secure, Managed, and Compliant Solutions

Ipswitch solutions deliver secure and managed end-to-end file transfer, enabling merchants, payment processors, and payment card issuers to meet PCI DSS compliance objectives and still have ready access to necessary payment card information.

### Safeguard credit card information

Ipswitch file transfer solutions provide 256-bit AES encryption for transfers over SSL and SSH protocols — the highest commercially available encryption technology — making them the most secure solutions for retailers that require confidentiality when transferring customer data and credit card information over the Internet. Ipswitch solutions also leverage OpenPGP file encryption, SHA-512 integrity, and EDIINT protocols AS2 and AS3 to ensure uncompromised transfers and non-repudiation.

# Shopping For a Secure File Transfer Solution For Retail

W H I T E P A P E R

## Exceed stringent regulatory requirements

Our secure, automated, and reliable solutions track data access and security enforcement policies to enable a level of PCI DSS compliance unrivaled by other file transfer methods. With the ability to create multiple hosts, define user access, and block IP addresses in real time, administrators can help to ensure that confidential data is only accessible by those with explicit permissions.

## Increase ease of use and control IT operational and training costs

Ipswitch solutions feature intuitive graphical user interfaces that are easy to configure and require no expensive training. Secure web-based interfaces let administrators control access, define rules, and ensure enforcement from one customisable dashboard. Silent installs and virtualization are also major cost-control mechanisms supported by Ipswitch solutions.

## Improve customer satisfaction

The Ipswitch file transfer architecture scales to thousands of servers and clients — providing the server clustering and load balancing necessary to ensure the availability and performance of critical merchant applications, and ensuring quick, seamless, and secure customer transactions.

## Summary

Retailers and merchant service providers are under increasing pressure to adhere to PCI DSS in an effort to avoid costly fines — and the even more detrimental loss of customer confidence that results from data leakage or data breaches. PCI DSS compliance requires organisations to protect the security, privacy, and confidentiality of cardholder information — and to document who accesses the information and the security measures taken to prevent theft, loss, or accidental disclosure. Ipswitch secure file transfer solutions deliver a proven, simple, and innovative method for exceeding your PCI DSS compliance needs.

## About Ipswitch, Inc.

Ipswitch File Transfer is a global technology provider that builds solutions to securely move your valuable data. We enable companies and people to better manage their data interactions when visibility, management and enforcement matter. Our managed file transfer solutions deliver the control necessary to enable governance and compliance for our

# Shopping For a Secure File Transfer Solution For Retail

W H I T E P A P E R

---

more than 40 million global users – including the majority of Fortune 1000 enterprises and government agencies. These organizations trust Ipswitch File Transfer solutions to secure, manage, automate and streamline their critical and highly sensitive file transfers and data workflows. Learn more at <http://www.ipswitchFT.com> or to contact us at <http://www.ipswitchft.com/Company/Contact.aspx>, or on [LinkedIn](#) and [Twitter](#).