

# PCI DSS Compliance Closing the Loop

Open Text Connectivity Solutions Group  
November 2009

## Abstract

The Payment Card Industry Data Security Standard (PCI DSS) is a collaborative effort to achieve a common set of security standards for use by entities that process, store or transport payment card data. The PCI DSS states 6 main objectives. Each objective is covered by a set of requirements each with a rationale and a set of sub-requirements specified for review.

This whitepaper will present a history and an overview of this standard, analyze the cost of non-compliance and discuss how your organization can achieve requirements of the PCI DSS.



## Contents

<b>Introduction .....</b>	<b>3</b>
<b>Overview of the PCI DSS .....</b>	<b>4</b>
History.....	4
Objectives and requirements.....	4
Scope.....	5
Roles and responsibilities.....	5
Compliance Mechanisms .....	6
Standard Adoption and Compliance levels .....	6
<b>Cost of non-compliance .....</b>	<b>7</b>
Non-Compliance fines .....	7
Cost of incidents .....	7
Indirect costs .....	7
Total cost of non-compliance.....	8
The TJX case .....	8
<b>Solutions for compliance .....</b>	<b>10</b>
Choosing the right tools.....	10
Open Text Connectivity Solutions.....	11
Data in transit security.....	11
Heterogeneous Networks Data Exchange .....	12
Data Integration and Transformation.....	12
Legacy Application Access .....	13
High-End UNIX Applications Access .....	14
Next Step.....	15



## Introduction

It may have all started in 2003, but at that time, no one noticed anything. On January 17<sup>th</sup> 2007, TJX announced that it suffered an unauthorized intrusion into its computer systems, potentially compromising customer credits and debit card data. On January 18<sup>th</sup>, financial institutions and credit card companies started to report fraudulent use of credit card numbers that had been stored in the TJX system, immediately cancelling thousands of cards. By October 2007, the fraud was found to have impacted 65 million of Visa accounts and 29 million of MasterCard accounts, for a grand total of 94 million accounts compromised. A Visa official put fraud losses to banks and other institutions that issued the card between \$68 million and \$83 million.

The TJX case attracted a lot of attention because of its magnitude and the media coverage around it, but it's only the tree that hides the forest. TJX is nothing else but the poster child of a phenomenon that has emerged in the past 15 years with the advent of electronic commerce and online transactions. This phenomenon which we will qualify as electronic fraud for the purpose of this document has manifested itself in multiple form, known from the public as hacking, phishing, identity theft or data breach.

In its 2008 security survey, the Computer Security Institute (CSI) found that the most expensive computer security incidents were those involving financial fraud with an average reported cost of close to \$500,000. Even worse, loss of customer data and loss of proprietary data which are currently counted as separate categories in the survey would come as second in front of viruses behind financial fraud if combined.

On March 19<sup>th</sup> 2007, Symantec released their annual Internet Security Threat Report, revealing that "the current Internet threat environment is characterized by 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.: (Symantec – March 19<sup>th</sup> 2007 Press Release).

One of the most interesting facts in Symantec's report was that credit cards were the most common commodity advertised on underground economy servers accounting for 22% of all items. 87% of these credit cards were issued by banks in the United States. Another very interesting fact was that only 4% of the malicious activities identified by Symantec were originating from Fortune 100 companies. 96% came from companies of all size and nature, putting an end to the belief that only mega corporations are the victim of these types of frauds.

This is the context in which the Payment Card Industry Data Security Standard (PCI DSS) has emerged in the past years. This whitepaper will present a history and an overview of this standard, analyze the cost of non-compliance and discuss how Open Text Connectivity Solutions can help organizations achieve some of the requirements of the PCI DSS.



## Overview of the PCI DSS

### History

The PCI Data Security Standard emerged recently among a cluster of other regulations that came out in the last 10 years: Basel II, Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, Sarbanes Oxley Act of 2002 and California State Bulletin 1386 to name a few.

Several credit card organizations are participating in the PCI effort: Visa, MasterCard, American Express, Diner's Club, Discover Card and JCB. All of these companies develop and manage their own standards independently:

- Visa – (AIS) Account Information Security
- MasterCard – (SDP) Site Data Protection
- American Express – (DSS) Data Security Standards
- Discover Card – (DISC) Discover Card Information Security and Compliance

The PCI DSS is a collaborative effort to achieve a common set of security standards for use by entities that process, store or transport payment card data.

The joint standard effort started in June 2004 with the four major credit card companies working on PCI DSS 1.0 which was release on December 15<sup>th</sup> 2004. On June 30 2005, the regulations took effect.

In September 2006, the PCI standard was updated to version 1.1. In October 2007, Visa announced a new set of Payment Applications Security Mandates to help companies comply with PCI. These mandates will need to be implemented by 2010. The latest PCI standard is version 1.2, which was released on October 2008.

### Objectives and requirements

The PCI DSS states 6 main objectives. Each objective is covered by a set of requirements each with a rationale and a set of sub-requirements specified for review. The 6 objectives are:

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy



## Scope

PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed or transmitted. Merchants and service providers who handle payments through cards are mandated to be PCI DSS compliant.

According to the PCI DSS 1.2, the security requirements apply to all “system components” that is included or connected to the cardholder data environment. These system components include:

- Network components: firewalls, switches, routers, wireless access points, network appliances, security appliances
- Servers: web, database, authentication, mail, proxy, DNS, NTP
- All applications, internal and external, purchased or custom

Of course these examples of system components are not limitative and the list could easily grow longer.

## Roles and responsibilities

Who	Mission	PCI DSS Role
Visa and MasterCard	They are made up of Member organizations who can be Acquirers or Issuers or both	<ul style="list-style-type: none"> <li>• Publish the PCI DSS guidelines</li> <li>• Certify products and providers</li> <li>• Certify audit assessors</li> <li>• Penalize non-compliant Acquirers</li> </ul>
Acquirers	Members of Visa or MasterCard which handle Merchants	<ul style="list-style-type: none"> <li>• Ensure their Merchants and Service Providers are PCI DSS compliant</li> <li>• Submit reports on compliance to Visa and MasterCard</li> <li>• Penalize non-compliant Merchants or Service Providers</li> </ul>
Merchants	Entities who accept card transactions from Cardholders	<ul style="list-style-type: none"> <li>• Submit compliance reports to their Acquirers</li> </ul>
Service Providers	Entities that provide processing, storing or transport services of card information on behalf of others.	<ul style="list-style-type: none"> <li>• Submit compliance reports to their Acquirers</li> </ul>

Other actors include cardholders and card issuers which have no direct obligation with regards to the PCI DSS unless they also fall in one of the above categories.



## Compliance Mechanisms

### Merchants

Merchants are segmented into 4 level based on the number of transactions per year, past compromising incidents and identification by other payment card brands.

Depending on their level, merchants could be required to:

- Be audited by Qualified Security Assessors. QSAs are companies certified by Visa for onsite audits. Audits are performed annually. Audits target all systems and networks that interact with cardholder information and include a review of 3<sup>rd</sup> party relationships. Audit reports are submitted to the Acquirer when the Merchant is found to be in compliance.
- Return an annual self assessment document to their Acquirer. The self assessment document is provided by Visa and consists in a subset of the onsite audit criteria in the form of a yes/no/not applicable questionnaire
- Perform a quarterly Network Security Scan using one of the offering from MasterCard certified provider. Issues are rated by severity. Scan results must be below Level 3 severity.
  - 3 (High): Limited exploit of read, directory browsing and denial of service
  - 4 (Critical): Potential Trojan Horses, file read exploit
  - 5 (Urgent): Trojan Horses, file read and write exploits, remote command execution

### Service Providers

Similarly to Merchants, Service Providers are segmented into categories, but where there were 4 categories for Merchants there are only 3 for Service Providers. Categories are determined by the number of transactions or accounts annually processed as well as the level of the Merchants they store the data for.

The compliance mechanisms are similar to those of the merchants with the requirement for QSA Onsite audits, self-assessment questionnaires and network security scan depending on the level of the Service Provider.

## Standard Adoption and Compliance levels

It seems that the standard is being widely adopted and compliance has grown significantly since its introduction. According to Visa in a press release from January 22, 2008, three-fourths of the largest US merchants and nearly two-thirds of the medium-sized merchants are now compliant with the PCI DSS.



## Cost of non-compliance

Similarly to any other industry standard that has emerged over the past decades, PCI DSS should be considered first and foremost as a way for organizations to mitigate risks and save money. In this section, we will discuss the various financial risks that could impact non-compliant organizations.

### Non-Compliance fines

The first thing that a non-compliant organization would be exposed to would be fines and penalties. Visa set compliance deadlines of September 30, 2007 for the largest merchants and December 31, 2007 for the middle-sized US merchants.

Since the beginning of this year, Visa has started levying monthly fines of \$25,000 to non-compliant US merchants and \$5,000 to their Acquirers.

But non-compliance fines are just the tip of the iceberg. Things get really interesting when you look at the cost of incidents.

### Cost of incidents

Many people have argued that the non-compliance fines did not represent much for large vendors (actually almost nothing) and that this would be the reason why PCI would fail. That's not entirely true.

In addition to non-compliance fines (which are enforced by Visa), the PCI DSS allow the various card brands to fine a merchant for non compliance with PCI for each incident. The fines can amount to \$500,000 **per incident per card brand per compromise type** (PCI includes both the PCI DSS and the PCI PIN requirements).

A merchant carrying 3 credit card types could end up paying \$3M for each incident.

But that's not all, what about all these other indirect costs?

### Indirect costs

Indirect costs are certainly the biggest stick that could hit merchants and on the contrary of the two previous costs, they would hit without discrimination, regardless of your PCI compliance status. This might be the biggest reason why companies need not only to adopt PCI quickly, but mostly make it efficient. Past standards were mere formalities and just a matter of taking the checkbook. The PCI DSS comes at a time where changes in merchants' business models have opened them to new vulnerabilities which need to be addressed. Put a blind eye on them and you risk losing your business



## Total cost of non-compliance

A 2007 Forrester study on the cost of security breach found that the cost could amount between \$90 and \$305 per record. The gap is a result of the many hard and soft costs that can vary from incident to incident. This means that if ten records are compromised, it can cost between \$900 and \$3,050; 1000 records can cost between \$90,000 and \$305,000.

Those costs are spread among several categories:

Category	Description	Cost per record
Discovery, notification and response	Legal counsel, mail notification, calls, call center, discounted product offers	\$50
Lost productivity	Employees diverted from other tasks	\$20-\$30
Opportunity cost	Impact on existing customers and difficulty getting new ones	\$20-\$100
Regulatory Fines	FTC, PCI, SOX	\$0-\$60
Restitutions	Money put aside in case breaches are discovered	\$0-\$30
Additional Security and audit requirements	Security and audit requirements levied as a result of a breach	\$0-\$10
Other liabilities	Credit Card replacement costs, civil penalties if fraud can be traced to the breach	\$0-\$25

## The TJX case

On October 24 2007, TJX reached a tentative settlement with attorneys representing consumers who were harmed by the breach for \$256 million.

Banking plaintiffs have not set an exact total for the damages they seek in their suit but they want the company to pay for unspecified losses and costs such as those encountered when reissuing compromised credit cards.

In addition, TJX is also facing state and federal investigations into the breach that could result in more fines.










Analysts have estimated the total amount that TJX would end up paying to be around \$1B. A cost estimate model established by security company Protegrity would put that number to \$1.7B.

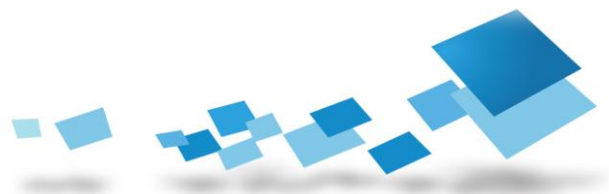


## Solutions for compliance

### Choosing the right tools

There is no one-size-fit-all when it comes to data security and the PCI DSS is a good example of that. Looking at the requirements for the standard, it is quite clear that there will never be a single tool or a single set of practices to address all these requirements. A successful PCI DSS compliance effort will rely on a set of tools, each suited for a specific requirement, and a group of best practices depending on each line of business.

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



As a leading connectivity solution vendor, Open Text has developed a successful line of network security products which could help companies in their efforts to become PCI DSS compliant. The table below highlights the PCI DSS requirements can be partially or fully address with Open Text Security products.

## Open Text Connectivity Solutions

With more than 20 years of experience in the enterprise connectivity market, Open Text Connectivity Solutions covers a broad spectrum of needs including:

- Data in transit security
- Heterogeneous networks data exchange
- Data integration and transformation
- Legacy applications access
- Access to high-end graphical Unix applications

We have been serving companies of all size which have deployed our solutions in a wide variety of mission-critical environments, from market room to engineering offices.

## Data in transit security

Open Text offers Open Text Secure Shell and Open Text Secure Terminal to organizations which require strong encryption and authentication capabilities for the data transiting on their network.

These solutions enable data to be transparently tunneled over a secured connection when travelling between user desktops and servers regardless of the application that has generated the data. For instance, Open Text Secure Shell can be used to secure:

- E-mails
- Instant messaging
- Client/Server communications
- Web communications
- File transfer operations
- Terminal emulation sessions

In addition to the examples above, Open Text Secure Shell can be configured to secure virtually any application that uses TCP/IP as its network transport. Even better, there is no need to modify the code of the application to enable this operation.

From an encryption standpoint, Open Text Secure Shell uses the latest cipher suites including AES and its encryption module as received FIPS 140-2 certification, a US federal government certification for cryptographic products.



When it comes to authentication, Open Text Secure Shell can authenticate users through a variety of ways including passwords, authentication tokens, public/private keys, X 509 certificates, Kerberos...

Deploying Open Text Secure Shell on users desktop in the context of PCI compliance will help organizations make sure that cardholder data cannot be eavesdropped upon when transiting over the network and that their authentication methods are stronger.

## Heterogeneous Networks Data Exchange

For more than 20 years now Open Text Connectivity Solutions Group has been offering a suite of network-based data exchange software based on the NFS protocol. These tools allow organizations to securely exchange data between Windows environments and UNIX or Mainframe environments.

The full portfolio of NFS solutions includes clients, servers and gateways for Windows desktops and servers, giving customers the flexibility to integrate their heterogeneous environments in an optimum way.

There are many advantages using NFS over other windows networking protocols such as SMB and CIFS:

- Performance: the NFS software architecture offers exceptional performance, allowing organization to use up to 99% of their available bandwidth when moving files
- User rights: NFS is designed to fully leverage ACLs (Access Control Lists) of the environment where the files are hosted
- Corporate Directory support: the Open Text NFS product family allow organizations to leverage most standard corporate directory formats including LDAP or Active Directory in order to maintain a coherent identity policy across all applications used throughout the IT infrastructure
- Advanced encryption: our NFS clients and servers support multiple encryption and security mechanisms such as SSL, LIPKEY, Kerberos or RPCSEC-GSS.
- Immune to viruses relying on SMB shares to spread

PCI compliance of network-based file systems and file exchange can be greatly facilitated by deploying the Open Text NFS product in windows-based or heterogeneous environments.

## Data Integration and Transformation

Open Text Integration Center represents a new generation of content and data integration solutions that transform, cleanse, enrich and direct unstructured and structured information across the entire spectrum of decision support systems and corporate applications, spanning projects that include data warehouses, data



markets, legacy applications, ERP systems, CRM systems, and content management deployments.

Open Text Integration Center delivers a rich set of benefits that offers organizations significant and tangible return on investments. Built on the foundation of four key principles of openness, flexibility, ease of use, and reusability, Open Text Integration Center decouples business processes from the complexity of the IT systems infrastructure, allowing organizations to better execute agile business practices

Open Text Integration Center is the ideal all-platforms data integration tool for any company, integrator or consulting firm looking to:

- Build and feed data warehouses of all sizes
- Use ETL functionalities to extract and transform data between multiple sources
- Solve complex data problems during EAI (Enterprise Application Integration) projects
- Implement a data-friendly SOA (Services Oriented Architecture)

Open Text Integration Center can help companies move into the PCI compliance path by giving them the capability to break the boundaries between data sources, allowing organizations to rethink their data infrastructure in the light of PCI compliance without having to worry about data transport and manipulation.

## Legacy Application Access

Mainframes continue to have a strong presence in the enterprise market and will continue to deliver mission critical applications for some time to come. Rewriting existing host applications can be significant and costly where an ROI is hard to justify. Transforming operational environments and increasing security threats require organizations to adapt within the restriction of their budgets.

The Open Text HostExplorer is the ideal solution for organizations that want to realize value from the latest Web-to-host technologies and security without incurring complex migration projects costs.

HostExplorer is a unique PC-to-host and Web-to-host terminal emulation solution. Whether it is used traditionally on the desktop or as a browser-based solution, HostExplorer consistently delivers the same features, power, and administrative functions. HostExplorer provides a seamless transition from a fat to a thin client as the enterprise needs continue to evolve.

In addition, HostExplorer offers a powerful migration path from many other terminal emulation software products currently available. To ensure a smooth conversion and migration with no disruption of business, HostExplorer offers powerful features, such as macro conversion and user interface themes.



HostExplorer offers significant security capabilities which will help organizations in their effort to become PCI compliant. Some of these capabilities are:

- SSL encryption and authentication support
- Kerberos authentication support
- Support for PKI based cryptography
- FIPS 140-2 certified encryption module
- Extensive desktop lock-down capabilities
- Ability to configure session lock-down period

While Mainframe systems still represent a significant element of many corporate application infrastructures, it is important for organizations to ensure maximum security of their terminal emulation solution. HostExplorer offers a set of security migration and productivity benefits that can help enterprise improve their PCI compliance profile.

## High-End UNIX Applications Access

Credit card data are not restricted to client server applications or Mainframe systems they can also be manipulated from graphical UNIX applications which in most cases rely on the X11 network protocol to interact with the user.

Exceed is Open Text Connectivity's flagship product. For over 20 years, Open Text Exceed has set the standard for the PC X Server market and has earned the highest scores against the X11 performance benchmarks. The Exceed family is ideally complemented by:

- Exceed: The gold standard for PC X Server
- Exceed Freedom: security, mobility and collaboration add-on for Exceed
- Exceed onDemand: centralized remote application delivery solution
- Exceed PowerSuite: X window, terminal emulation and NFS connectivity in one convenient software package
- Exceed 3D: OpenGL extension add-on for Exceed
- Exceed XDK: X Window software development kit for Windows.



True enterprise software, Exceed has been designed with many unique features that ease administrative burden and increase user productivity. With a strong presence in the engineering, banking, and government sectors, Exceed has proven that it can meet the most complex applications in the most demanding environments.

When it comes to PCI, Exceed will help organizations along their PCI compliance effort by offering them strong security capabilities through:

- Integration with the optional Open Text Secure Shell add-on
- Host-based and client-based access control lists
- MIT-Magic Cookie extension support
- Integration with smartcards from ActivCard, Axalto or Safenet
- Built-in Kerberos and FIPS 140-2 Validated SSL support

## Next Step

If your organization hosts or interacts with credit card data, there is no doubt that you will be impacted by the PCI standard sooner or later. Contact Open Text Connectivity Solutions Group today to find out how we can help you along the way of PCI compliance. We will assess your connectivity PCI requirements and propose you the solutions that best suit your needs.



## About Open Text Connectivity Solutions Group

Open Text's leading Connectivity Solutions connect people, data and applications in mission-critical environments through a complete line of remote application access and data integration solutions. With 90 percent of Global 2000 companies relying on its award-winning solutions for over 20 years, Open Text understands the financial and operational challenges that most organizations face, whether they are multiple systems, disparate data sources, or geographically dispersed teams.

## About Open Text

Open Text is a leader in Enterprise Content Management (ECM). With two decades of experience helping organizations overcome the challenges associated with managing and gaining the true value of their business content, Open Text stands unmatched in the market.

Together with our customers and partners, we are truly The Content Experts™, supporting 46,000 organizations and millions of users in 114 countries around the globe. We know how organizations work. We have a keen understanding of how content flows throughout an enterprise, and of the business challenges that organizations face today.

It is this knowledge that gives us our unique ability to develop the richest array of tailored content management applications and solutions in the industry. Our unique and collaborative approach helps us provide guidance so that our customers can effectively address business challenges and leverage content to drive growth, mitigate risk, increase brand equity, automate processes, manage compliance, and generate competitive advantage. Organizations can trust the management of their vital business content to Open Text, The Content Experts.

<http://connectivity.opentext.com>

**Sales:**            connsales@opentext.com  
                         +1 905 762 6400

To contact our international sales offices:

<http://connectivity.opentext.com/contact-us.aspx>

**www.opentext.com**