

# ei Ecom Infotech Inc

## Governance Risk Compliance Solutions



Data Assurance  
Governance Risk Compliance  
COBIT , ISO 27001 , ITIL  
IBM Tivoli  
Identity and Access MGMNT  
IT Infrastructure Managemant  
Business Continuity and Resilience  
Enterprise Security Managemant

## Information Security Governance Risk Compliance Solutions

[Click here for more details >>](#)

[Corporate Training](#)

Holistic Approach to Your Security

# PCI DSS Services

## Overview

Credit cards are widespread and their use for online payments is increasing dramatically. However this increase has also brought about a growth in credit card fraud. In March 2007, TJX Companies Inc. disclosed that at least 45.6 million credit and debit card numbers were stolen by hackers who broke into its network. Another case involved Card Systems Solutions in a theft of 40 million card holder data.



On August 18, in 2009 as reported by [US News Today](#), Three men have been charged with stealing the numbers of more than 134 million credit and debit cards in what the US Justice Department said was the largest case of identity theft in US history.



Alberto Gonzalez, 28, from Miami, and two unnamed computer hackers, based in or near Russia, allegedly targeted 7-Eleven and other large corporations by uploading millions of customers' details from internal computer systems onto servers that worked as hacking platforms.

They allegedly breached the firewall of Heartland Payment Systems, a New Jersey-based bank card payment processor, stealing 130 million numbers. They allegedly stole 4.2 million card details from Hannaford Brothers, a Maine-based supermarket chain. An undisclosed number of card details were hacked from 7-Eleven, the Texas-based convenience store chain with outlets around the world,.

There could be many more such instances, which are not reported for the risk of brand image and reputation loss. Since companies are constantly at risk of losing sensitive cardholder data, which could result in fines, legal action and bad publicity, achieving compliance with the PCI DSS is now on a high on the agenda of companies who store, transmit or process credit card data. Furthermore, PCI DSS compliance **needs** to be achieved. Organizations that fail to comply face severe fines if the data is lost or stolen and risk not being allowed to handle cardholder data.

## The Payment Card Industry Data Security Standard ( PCI DSS)

The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.



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 organizations proactively protect customer account data.

Any entity that stores, process and/ or transmits cardholders' data, it is mandatory to comply with PCI DSS. Entities include but not limited to:

- ⇒ Merchants
- ⇒ Acquirers
- ⇒ Service Providers
- ⇒ Trusted Third Parties

This applies to all payment channels including physical card presence, mail or telephone order, and e-commerce.

### PCI DSS Requirements

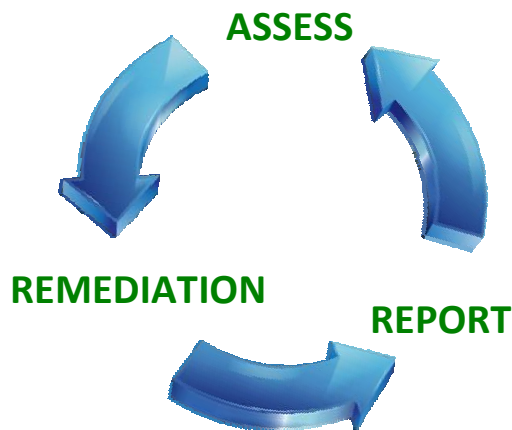
The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	<ol style="list-style-type: none"> <li>1. Install and maintain a firewall configuration to protect cardholder data</li> <li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ol>
Protect Cardholder Data	<ol style="list-style-type: none"> <li>3. Protect stored cardholder data</li> <li>4. Encrypt transmission of cardholder data across open, public networks</li> </ol>
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> <li>5. Use and regularly update anti-virus software</li> <li>6. Develop and maintain secure systems and applications</li> </ol>
Implement Strong Access Control Measures	<ol style="list-style-type: none"> <li>7. Restrict access to cardholder data by business need-to-know</li> <li>8. Assign a unique ID to each person with computer access</li> <li>9. Restrict physical access to cardholder data</li> </ol>
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> <li>10. Track and monitor all access to network resources and cardholder data</li> <li>11. Regularly test security systems and processes</li> </ol>
Maintain an Information Security Policy	<ol style="list-style-type: none"> <li>12. Maintain a policy that addresses information security</li> </ol>

## ECOM's PCI DSS Compliance Program

PCI DSS Compliance Services are among the core competencies of ECOM . ECOM is the approved Qualified Security Assessor (QSA) for India by PCI DSS Council. Our PCI compliance services include:

- ⇒ Pre Audit checks and Technical Auditing
- ⇒ GAP Analysis
- ⇒ Compliance Audits / ROC & SAQ Completion
- ⇒ Consultation on payment process and architectural design.
- ⇒ Education & Assessment Preparation
- ⇒ Compliance Advisory & Support
- ⇒ Onsite QSA Audits
- ⇒ Remediation and Managed Services (Consulting as well as SAAS)



### Advantage ECOM

**Proven track record** in Information Security Domain with offices in Mumbai India and IL, USA. Our Consultants are SME's (Subject Matter Experts) with multiple certifications such as CISA, CISM, CGEIT, CISSP, CEH, PCI QSA, ISO 27001/20000 LA, ITIL PMP etc. ECOM has been in existence since 1983 and is listed on BSE (Mumbai Stock Exchange) since 1996.

**Structured approach for timely compliance** ECOM uses Project Management Methodology for enabling our clients to get PCI DSS Compliance as quickly, systematically and painlessly as possible, thus reducing your costs.

**Remediation and Managed Services** ECOM is also a business partner of many technology solutions companies such as IBM and is updated in the automated compliance market space. ECOM provides remediation solutions for Log Management, SIEM, Enterprise Security Management, IT GRC Tools (with PCI DSS Controls out of the box), Single Sign On, Identity and Access Management etc. ECOM offers SAAS for Log /SIEM and for IT GRC.

**Expertise** ECOM has worked on core IT Controls for many compliance requirements and framework implementations/ best practices such as ISO27001/2, ISO 20000, COBIT, SOX, HIPAA, GLBA, PCI DSS etc in most verticals.

## PCI FAQ

1. Is PCI DSS applicable to us?
2. What should we do to prepare for a PCI audit?
3. What are some common challenges that companies face in trying to become compliant with PCI?
4. How much time does it take for PCI Compliance?
5. Our servers are in hosted environment, do we need PCI ?
6. We are performing scanning from a Authorized Scan Vendor, are we PCI compliant ?
7. We are ISO 27001 certified , are we straight away compliant with PCI ?
8. What is ECOM's specific methodology ?
9. Do you have a list of Do's and Don't's for PCI DSS?

### 1. Is PCI DSS applicable to us?

If your organization touches or sees credit card information and cardholder data, either directly or as a service provider to another company, then you are subject to PCI DSS compliance. As an executive charged with PCI DSS compliance, you are not only managing the risk of financial liability for penalties and fraud conducted on your systems, but increasingly it is a matter of law. In the US and worldwide, PCI DSS is evolving from industry compliance to government mandate.

Depending on your company's role in cardholder data handling and the number of transactions you conduct yearly, your company may be classified as **Merchant - Level 1, 2, 3, or 4** or **Service Provider - Level 1, 2, or 3** and be required to either conduct a self-assessment or have one performed by a PCI DSS Qualified Security Auditor (QSA) such as ECOM. In all cases, PCI DSS requires that an executive officer of your company sign-off on any assessment statements and results highlighting the accountability and liability inherent in the process.

### 2. What should we do to prepare for a PCI audit?

At a high level, designate a person responsible for the project (Project Manager) first. Then seek out the required documentation as mandated by PCI DSS and prepare a project plan based on the requirements and applicability. ECOM can help you with this.

The plan should detail all activities and personnel with tentative dates of completion for activities. If you are using a project management methodology you can create WBS or Work Breakdown

Structure. Regular communication with ECOM via conference calls and e-mail is required. Steps that will help guide you through the preparation process could include the following:

- Step 1:** Establish PCI DSS Compliance team under the Project Manager. The team should comprise of members that represent management to review the PCI DSS compliance policies and procedures and members of the core IT group who are responsible for implementing the IT controls.
- Step 2:** Based on PCI DSS controls make a GAP Analysis.
- Step 3:** Complete a detailed scoping study to restrict PCI DSS implementation to only the cardholder network environment.
- Step 4:** Once scoped, start distributing responsibilities for implementation of individual controls.
- Step 5:** Conduct a weekly review meeting with the team. Once a control objective has been documented, implemented and put into working order, mark it in the GAP Analysis.
- Step 6:** Once all the controls are in place, invite an ECOM's QSA team to conduct a pre-certification audit. Any controls identified as being not compliant or partially compliant should be documented and marked pending in the GAP Analysis.
- Step 7:** Once all control objectives are implemented you should now invite the ECOM'QSA team for the final certification audit.

### 3. What are some common challenges that companies face in trying to become compliant with PCI?

Some common challenges that companies face when attempting to become compliant with PCI include:

- No Intrusion Detection/Prevention System (IDS/IPS) in place.
- Logging and Analyzing of logs or SIEM solution is not in place.
- No periodic Application Security reviews for applications that are used in the processing of credit card transactions.
- Administrative access to too many users without ability to pin point specific activity to a particular admin.
- No segregation between PCI and non-PCI networks.

- Not properly prepared for financial resources for **People, Process and Technology** to become PCI compliant.
- No unique login/passwords for all users.
- No network DMZ in place.

#### 4. How much time does it take for PCI Compliance?

If an organization has segregated the PCI DSS and other environment, it will take much lesser time to become PCI DSS compliant. Secondly, organization has to put all controls as per PCI DSS standard 1.2 in place and should be in a position to exhibit the evidence of the same to QSA. Approximately it may take about 3 to 6 months to become PCI DSS compliant.

#### 5. Our servers are in hosted environment, do we need PCI?

Whether data resides in your own corporate environment or a hosted environment, all remote accessing and shared servers should also follow PCI DSS standards.

#### 6. We are performing scanning from an Authorized Scan Vendor, are we PCI compliant?

No. PCI DSS has two components: Scans and On-site Audits. Although getting the organization's perimeter network scanned from an Authorized Scan Vendor (ASV) every quarter, is a mandatory requirement but it is only one of the requirements for PCI DSS. Only getting the organization's perimeter network scanned by an Approved Scanning Vendor (ASV) will not make the organization compliant.

#### 7. We are ISO 27001 certified, are we straight away compliant with PCI?

No. ISO27001 (formerly BS7799) is primarily an IT Governance Framework. It does not give actual PCI DSS audit procedures. PCI is specific data security standards to protect credit card data, which gives 12 specific requirements/ controls that are mandated. Unlike ISO 27001, **Acceptance of Risk** does not constitute PCI DSS compliance. ISO27001 certification will not lead you to automatically achieve PCI DSS compliance.

## 8. What is ECOM's specific methodology?

### ECOM's PCI DSS Methodology

ECOM follows a 4 Step process to achieve PCI DSS Compliance

#### Step 1: Identify Cardholder Data and Reduce Scope

ECOM's team will first identify how cardholder data flows, where it resides, and how to design networks to properly manage the card-holder data, this phase focuses on reducing what is considered in-scope for PCI DSS in order to minimize "wasted motion" and reduce costs. The step will include **Data Flow Analysis, Mapping Cardholder Data, PCI Data Segmenting and Scope Classification.**

#### Step 2: Assess Current State

This step reviews an organization's current state, identifies any areas of potential non-compliance and creates remediation plans to achieve compliance. It includes **Gap Analysis, Self-Assessment Questionnaire (SAQ), Developing Remediation Plans**

#### Step 3: Implement Requirements and Solutions

This step focuses on implementing solutions that help organizations meet specific DSS requirements. In some cases, this would be in the form of consulting services to develop specific policies or procedures. In others, it would involve performing consulting services to fulfill specific requirements such as penetration testing and web application assessments. ECOM also provides Managed Security Services (Consulting as well as SAAS) to meet other PCI DSS requirements.

#### Step 4: Assess for Compliance

This step involves performing the required PCI DSS compliance assessments in the form of annual PCI DSS audits as a Qualified Security Assessor (QSA). ECOM can audit organizations for compliance, assist in their remediation efforts and submit all required paperwork to the appropriate stakeholders.



## 9. Do you have a list of Do's and Don'ts for PCI DSS?

Yes it is given as below:

Data Do's	Data Don'ts
Do understand where payment card data flows for the entire transaction process	Do not store cardholder data unless it's absolutely necessary
Do verify that your payment card terminals comply with the PCI personal identification number (PIN) entry device (PED) security requirements	Do not store sensitive authentication data contained in the payment card's storage chip or full magnetic stripe, including the printed 3-4 digit card validation code on the front or back of the payment card after authorization
Do verify that your payment applications comply with the Payment Application Data Security Standard (PA-DSS)	Do not have PED terminals print out personally identifiable payment card data; printouts should be truncated or masked
Do retain (if you have a legitimate business need) cardholder data only if authorized, and ensure it's protected	Do not store any payment card data in payment card terminals or other unprotected endpoint devices, such as PCs, laptops or smart phones
Do use strong cryptography to render unreadable cardholder data that you store, and use other layered security technologies to minimize the risk of exploits by criminals	Do not locate servers or other payment card system storage devices outside of a locked, fully – secured and access-controlled room
Do ensure that third parties who process your customers' payment cards comply with PCI DSS, PED and/or PA-DSS as applicable. Have clear access and password protection policies	Do not permit any unauthorized people to access stored cardholder data

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Card Holder 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 Data	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

**Contact us for more details**

**Ecom Infotech Inc**

**Call India +91 9869436685 US 1-312-224-1657**

[www.ecominfotech.biz](http://www.ecominfotech.biz) <mailto:ac@ecominfotech.biz>