



Mphasis PCI Compliance Solutions

The fastest, safest and most cost-effective means to PCI DSS Compliance

/// WHITE PAPER



Introduction

The PCI DSS standards require companies to adhere to 12 requirements in managing their systems that either store, process or transmit card data. These set specific security standards that are obligatory in order to carry on business as usual and companies found to abandon these can find themselves incurring enormous PCI and government fines in the case of any consumer compromised by their data being hacked.

Recently, a leading US wholesaler publicly disclosed in a regulatory filing that they had experienced an unauthorized intrusion into the electronic credit/debit card processing system. As many as 45 million credit/debit card account numbers and over 455,000 records containing customer names and driver's license numbers had been stolen from the company's IT system. This resulted in major financial losses and lawsuits were filed against the merchant that in turn eroded their reputation.

What is the PCI directive?

To recount, PCI-DSS is a set of 12 high-level requirements that apply to all organizations that store, process, and transmit card data.

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 password 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 or programs.

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 systems and processes

Maintain an information security policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors

Why PCI Compliance is Required?

- To protect brand reputation of banks and merchants (Millions of card holder data has been compromised in the past few years.)
- Avoid card company PCI fines ranging from US \$50,000 to US \$1M.
- Avoid government PCI fines ranging from US \$1M to US \$20M in addition to 20 years of compliance audits.
- Avoid regulatory actions, insurance claims, class Action, litigation.
- Avoid card acceptance being revoked by card companies. (Card Systems Solutions is out of business after experiencing a breach)

PCI compliance is not a one time task!

At first glance, PCI compliance may seem simple; after all, the focus and intent is to either eliminate credit card data from systems or to encrypt the data if it is stored, and to form a policy framework that protects card processing systems and their data. However, PCI DSS is a comprehensive risk management strategy that covers people, systems, and process. PCI DSS Compliance is not a one-time task. It is a continuous process with continuous assessment. Thus, any solution for compliance must handle the complexity of managing data privacy and system integrity over time, and across multiple business domains and boundaries.

Encryption has traditionally been very complex. Requirements such as support for aging legacy systems, managing encryption keys, encryption key rollover, dual controls, and the need to have separate views of card data on a "need to know" basis between customer service representatives, fraud investigators and

administrators can make the task for compliance daunting. Consequently (and this is especially true for legacy systems), many organizations resort to costly and complex compensating controls, which increase costs and inhibit business through the need for dedicated human resources and changes to business processes

How does MphasiS/EDS Application Remediation platform solve these problems?

A particularly challenging requirement is PCI DSS Section 3: Encryption and Key Management. Since any non-compliance can result in substantial fines and re-work, as well as additional audit scrutiny - all of which are invasive and costly, it is imperative that organizations requiring PCI DSS compliance review technologies such as our Remediation Services to:

- Avoid any risk of failure.
- Fast track compliance at minimal cost.
- Eliminate substantial IT change and business disruption.
- Avoid fines and increased PCI audit scope.
- Quickly enable best practices in encryption today, avoiding future change.

This solution has been developed to address the Payment Card Industry (PCI) compliance requirements 3, 6, and 7. This solution ensures secure storage of sensitive data like Credit Card Number, Bank Account Number, and Social Security Number (SSN).

The solution is a flexible building block and it is a well-defined, self-contained and stateless service. It is a data-centric persistence mechanism used to store sensitive information in the isolated database.

Both Online and Batch processes can invoke this service to recognize sensitive data and transform sensitive data into nonsensitive reference id. The sensitive data will be moved into a secure, isolated PCI compliant database and will reside on a separate network subnet with stringent firewall configuration, while nonsensitive reference id will be used for processing of payment transactions within the system and this reference id will be stored in the Domain application database. The nonsensitive reference id generation process has the capability to process multiple cards in a single request and generate a unique reference id for each card number

within a customer database and store each card number, associated data and nonsensitive reference id in a secure database. This solution also provides an audit trail of all user access of credit card data in PCI compliant zone as per PCI requirements.

Comparison of MphasiS/EDS solution and In-House Solutions

	MphasiS/EDS Approach	In House Approach
Time to become PCI compliant	Under 3 months**	6 to 18 months
Assessment costs to determine 'scope'	50% reduced as compared to other in-house	USD 135,000 to USD237,000*
PCI Compliance cost	50% reduced as compared to other in-house	USD155,000 to USD 2.7M
Ongoing expenses	Fixed	Variable

* Gartner estimates merchant Level 1-3

** The above figures apply to Low - medium complex systems

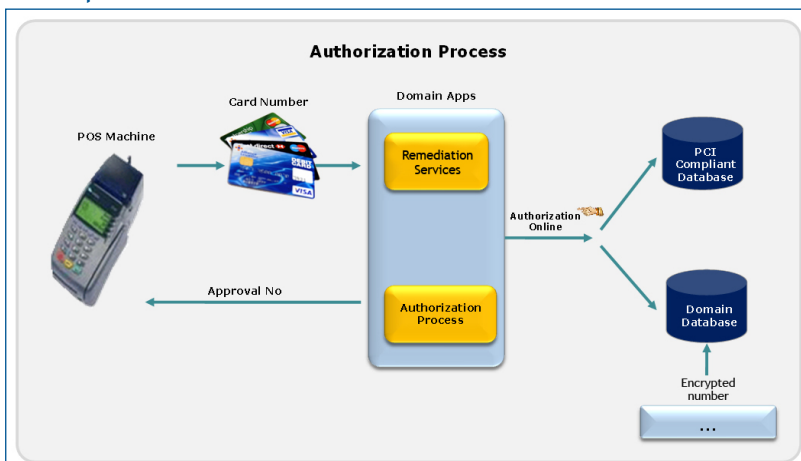
For a practical example of the impact of PCI regulations, consider that many companies have a need to maintain payment details on their systems for a variety of business needs. Memberships, subscriptions, services and payments that are accrued are all fundamental components of sales revenue. Understanding, measuring the impact and ultimately changing all the systems that manage the present process to an architecture that meets the PCI DSS compliance is a substantial task in itself. Then consider the impact of the time and money that managing this will have against delivering the things that the business really employs the development team to deliver, and the true cost of compliance can be calculated.

MphasiS/EDS Application Remediation Platform has been developed to address the core requirements of PCI DSS compliance. These requirements correspond to up to 80% of the re-engineering and maintenance effort needed to maintain the appropriate levels of security across card payment systems.

MphasiS/EDS Application Remediation Platform is an industry proven solution that simplifies the management of these requirements, that means huge savings in terms of time, money and security resources. EDS have extensive experience developing, implementing and managing systems throughout the cards payment industry, and offer complementary services to manage your compliance solution including pre compliance audit assessments, gap analysis and other remediation services.

Online and Batch Process Flow

Online process flow



This service helps remove sensitive data from the entire application and ensures uninterrupted secure processing of transactions without the sensitive data being present in the domain database. Clients have the option of storing the PCI compliant database in-house or at EDS data center that is already PCI compliant.

Benefits of Mphasis/EDS Application Remediation Platform

- With the above approach, in case of hacking or theft of nonsensitive reference id, the data is of no commercial value to the hacking community because this reference id cannot be reverse-engineered into a valid card number. This reference id also cannot be used for fraudulent payment processing outside of our system.
- Business users and card holders' experience will remain the same. The application remediation changes would be transparent to the users.
- Seamless integration into existing IT environment
- Requires minimum changes to underlying data schemas and applications
- Mphasis/EDS Application Remediation Platform services can be easily plugged into existing system. Administration toolkit gives client the flexibility to setup capture options of sensitive data, choose reference id generation option, etc.
- Least cost, time and most secure solution available

Other EDS/ Mphasis PCI Offerings

EDS is a major payment cards service provider processing millions of cards across the globe and has its own Cards processing solution (ACF). This means we understand all the PCI DSS requirements and the need to become compliant. Mphasis/EDS solutions are scalable and can be implemented with no disruption to ongoing business.

EDS offers a comprehensive suite of services and solutions to become PCI compliant. Our unique Application Remediation platform along with solutions for database and application monitoring, network management, access management and Event/Incident Management provide a complete set of solutions for PCI compliance. EDS' service offerings focus on cost

control, process improvement and compliance. The offerings include pre compliance assessment, gap analysis and solution implementation. Additionally, EDS supports compliant consumer card services. We also help third party vendors like embosser, PIN generation, statement printing, etc, become PCI compliant. Our services and solutions can be consumed by a variety of industries - Banking, Insurance, Retail, Transportation, Travel & Hotels, etc.

Security Solutions

- Database Activity Monitoring
- Application Activity Monitoring
- Data-At-Rest Encryption
- Network Management
- Vulnerability Assessment and Management
- Access Management
- Event / Incident Management

Service Offerings

- PCI DSS Pre Compliance Assessment
- PCI DSS Gap Analysis
- PCI DSS Implementation (Custom solutions, Point Solutions)
- PCI DSS Complaint Consumer Card Services support

For further information contact;
PCI-Experts@mphasis.com

Contact us

USA

Mphasis
460 Park Avenue South
Suite # 1101, New York
NY 10016, U.S.A.
Tel: +1 212 686 6655
Fax: +1 212 686 2422

UK

Mphasis
100 Borough High Street
London SE1 1LB
Tel: +44 20 30 057 660
Fax: + 44 20 30 311 348

Mphasis
Edinburgh House
43-51 Windsor Road
Slough SL1 2EE, UK
Tel: +44 0 1753 217 700
Fax: +44 0 1753 217 701

INDIA

Mphasis
Bagmane Technology Park
Byrasandra, C.V. Raman Nagar
Bangalore 560 093, India
Ph.: +91 80 4004 0404
Fax: +91 80 4004 9999

About Mphasis

Mphasis, an EDS company, delivers Applications Services, Infrastructure Services, BPO and KPO services through a combination of technology know-how, domain and process expertise. We service clients in Financial Services & Insurance, Manufacturing, Communications, Media & Entertainment, Healthcare, Transportation & Logistics, Consumer & Retail industries and to Governments around the world. We are certified with ISO 9001:2000, ISO/IEC 27001:2005 (formerly known as BS 7799), assessed at CMMI v 1.2 Level 5 and are undergoing SAS 70 certification. We also provide SEI CMMI, ISO and Six Sigma related services support.

Mphasis is a performance based company, dedicated to outstanding customer service. We offer capabilities to provide innovative solutions by sustainable cost savings and improved business performance through flexible engagement models. Customer centricity, transparency in operations, result-oriented activity and flexibility are the values on which we build long-term relationships with our clients.