

Compliance Brief: PCI DSS



Secure and Protect Credit Card Information

In 2004, five major credit card companies joined forces to align their individual security policies and form a single set of mandatory requirements for all merchants and credit card payment processors. The result, known as the Payment Card Industry Data Security Standard (PCI DSS), was a cohesive policy designed to help merchants protect credit card account information and prevent credit card fraud.

Applicability

Security breaches and fraudulent credit card purchases have been rising dramatically over the past decade, and any business that processes, stores or transmits credit card information inherently runs the risk of mishandling or losing their customers' account data. PCI DSS affects any merchant that accepts MasterCard, Visa, American Express, Discover or JCB cards, and no matter how many credit card transactions a merchant makes, they must be in compliance with PCI DSS.

The Impact on Your Business

PCI DSS is a multifaceted security standard that includes 12 requirements for security management. Individual credit card brands enforce the regulations and have their own compliance consequences, which can include audits, fines of up to \$500,000 per incident and losing the ability to process credit card payments. Retailers face increased financial liability for lost credit card information and find themselves in courtrooms arguing over lost data, meanwhile losing important business partners, customer confidence and loyalty. PCI DSS requirements force merchants to redefine their policies and procedures for:

- Building and maintaining a secure computer network.
- Protecting cardholder data.
- Testing systems and managing vulnerability.

A survey conducted by Javelin Strategy & Research studying retailers and credit card security found that 78% of consumers would be unlikely to continue shopping at a store if they learned it had a breach that may have compromised their credit account information. On the other hand, 85% of customers would be likely to increase their shopping at a store if they knew it was a leader in devoting resources and technology to protecting its customers' personal credit and or debit card account information.

ECM Enables PCI DSS Compliance

Enterprise Content Management (ECM) technology provides merchants and retailers with a secure information management system that can enhance PCI DSS compliance strategies and improve operational efficiency. PaperVision® Enterprise, the on-premise ECM system, and ImageSilo®, the world's most trusted on-demand ECM service, are affordable, easy-to-implement systems that can also help companies reduce information management costs. Many businesses with limited IT resources prefer to outsource their data storage with ImageSilo and rely on its ultra-secure network to address PCI DSS requirements.

PaperVision Enterprise and ImageSilo capabilities assist merchants in building and maintaining compliant practices, while saving money and time.

Reliable Network Security

PCI DSS requires merchants to build a firewall configuration that denies all traffic from “untrusted” networks and hosts. Additionally, retailers cannot use vendor-supplied defaults for system passwords and other security parameters. PaperVision Enterprise and ImageSilo provide comprehensive systems, features and settings to safeguard information and control application security.

- ImageSilo stores and protects customer data on an ultra-secure, closed network that is monitored 24 hours a day, 365 days a year.
- Security access rights are verified each time a request is made to the ECM system to protect against unauthorized traffic.
- Password settings and other detailed security options give merchants complete control over user access, including password complexity, password expiration, invalid login attempts and more.

Protected Credit Card Information

Key elements of PCI DSS compliance include data encryption, hidden account numbers, as well as secure information transmission and storage. Digitech Systems’ ECM technology can enhance security and make credit card information unreadable anywhere it is stored.

- 256-bit AES encryption can occur both during transmission and when data is stored, protecting credit card numbers throughout the entire ECM system.
- Multiple levels of security enable merchants to limit access to sensitive information and customize security rights for each employee.
- Redaction hides specific account information within a credit card authorization form and restricts the viewing or disclosing of sensitive information even if the document is shared.

Simple Vulnerability Management

PCI DSS was designed to protect against exploitation and forces businesses to detect and manage any network vulnerabilities. Specifically, retailers must track all access to cardholder data, have the most recently released software patches and regularly test security systems. PaperVision Enterprise and ImageSilo include tools that can track system activity and verify security. Plus, ImageSilo frees merchants from managing software updates.

- Both PaperVision Enterprise and ImageSilo track all system access, including successfully completed, attempted or suspicious activities, such as trying to open a record without proper security clearance.
- As an on-demand ECM service, ImageSilo never requires retailers to update their software, because the system is maintained for them.
- Digitech Systems employs a third party to scan the ImageSilo network daily and verify merchant information stored in the system is immune to the latest security threats.

For more information, please visit www.digitechsystems.com or call toll free at 888.374.3569.