DeliverySlip

WHITE PAPER

# Payment Card Industry Data Security Standard (PCI DSS)

## Introduction

As speed of business pushes ever forward, businesses around the world increasingly rely on near instantaneous credit transactions to make sales. In 2011, 135.33 billion transactions were made worldwide involving a credit, debit or prepaid card, up 12 percent over 2010 according to the Nilson Report. With the colossal amount of cardholder data whizzing between merchants, payment processors and banks, it's no wonder that cardholder data is often exchanged unsecured across high volume end user systems, like email.

To prevent cardholders' information from falling into the wrong hands, the Payment Card Industry Data Security Standard (PCI DSS) was established to hold organizations to a common standard for securing cardholder information against unauthorized exposure and exploitation.

First introduced in 2004 by the Card Industry Security Standards Council, The Payment Card Industry Data Security Standard (PCI DSS) is a stringent set of security standards that businesses must meet to transact using card information. Unlike compliance regulations administered by government organizations, PCI DSS defines specific security framework and technologies that businesses must implement to secure cardholder data wherever it resides, including email.

This white paper briefly details how PCI DSS protocols apply to your organization, discusses email security, and outlines what technologies your organization can implement to help ensure secure, PCI DSS-compliant email and file transfer.

## Who is affected by PCI DSS?

PCI DSS applies to all merchants, retailers and other businesses and organizations who transact using major credit, debit and prepaid cards. Additionally, PCI DSS applies to third parties, such as payment card processors, who store and access cardholder information to process transactions on behalf of organizations that accept card payments.

A recent study by the Ponemon Institute showed that 31 percent of respondents terminated their relationship with an organization after receiving notification of a breach of data security.

# Why should my organization comply with PCI DSS?

While businesses bear the burden of meeting multilayered PCI DSS protocols, the cost of compliance is far less than the alternative. Failure to comply with PCI DSS protocols has far reaching consequences that damage your business's bottom line and can cripple your ability to conduct future business. Consequences for non-compliance include:

## FINES

Banks and credit card institutions may, at their discretion, fine offending merchants up to $500,000 per security incident, and up to $50,000 per day for every day a business is operating in violation of security standards.

## SUSPENSION OF MERCHANT ACCOUNTS

Card providers such as Visa and MasterCard can refuse to do business with merchants and organizations who don't meet compliance requirements, reducing your ability to transact down to a cash only basis.

## PUBLIC NOTIFICATION

Currently 38 states have laws requiring that data breaches exposing customer information (including cardholder data) be reported to customers affected.

## LITIGATION

Organizations that fail to secure cardholder information may face civil suits, damages and other costly legal proceedings as a result of cardholder data being exposed without authorization.

## LOSS OF REPUTATION, CUSTOMERS & BUSINESS

It takes years to build a credible reputation but only a few minutes to ruin one, and a loss of credibility translates directly to an organization's bottom line. When consumers lose confidence, they switch to other services or brands, resulting in profit loss. A recent study by the Ponemon Institute showed that 31 percent of respondents terminated their relationship with an organization after receiving notification of a breach of data security.

While not all requirements are relevant to email security, PCI DSS requirements directly impact organizations' messaging security.

## Email security requirements

Unlike the broad framework requirements of government regulations, PCI DSS is broken down into 12 major requirements that additionally specify policies and technologies business must implement to secure cardholder data. While not all requirements are relevant to email security, the following requirements directly impact organizations' messaging security. In short, they charge organizations to:

- Protect stored cardholder data at rest and in transit
- Encrypt transmission of cardholder data across open, public networks including email systems
- Use and regularly update antivirus software on all systems commonly affected by malware
- Restrict access to cardholder data to a need-to-know basis
- Assign a unique ID to each person with computer access
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security

PCI details further requirements and standards, dependent upon organization type and the volume of annual credit transactions, that determine the specific policies and technologies your organization should implement. While a complete list of technical and policy requirements can be viewed on the **Security Standards Council** website, the next section identifies core technologies necessary for all organizations to comply with PCI requirements affecting messaging security.

# How can my organization meet these requirements?

GLBA (Gramm–Leach–Bliley Act) does not explicitly identify specific policies and email technologies organizations should implement as safeguards to achieve compliance; every institution is unique and uses NPI in different forms, for different reasons. Yet, several technologies and policy-best practices stand out as clear solutions to meet GLBA requirements in relation to email:

## END-TO-END ENCRYPTION

To meet regulation requirements that mandate NPI be secured, an end-to-end encryption that can encrypt or block content is often necessary to ensure that data remains confidential and secure between the message sender and the intended recipient, preventing unauthorized access or loss.

## DATA LEAK PREVENTION (DLP)

A DLP solution for email is essential for GLBA compliance, providing enhanced mail security through content filtering, authentication, and permissions rules that limit access and transmission of sensitive information sent within and outside the organization.

## ARCHIVING

An effective email archiving system will enable organizations to meet control objectives for message retention and auditing by capturing, preserving and making all email traffic easily searchable for compliance auditors to evaluate. When encrypted and backed up, archiving provides additional protections for information against loss and unauthorized exposure.

## ANTI-SPAM & ANTI-MALWARE

PCI stipulates that organizations implement appropriate technologies to protect from phishing and malware at the email gateway that could compromise the email system and cardholder data. To protect against advanced malware and zero-day attacks, a firewall is essential but not enough. It becomes necessary to implement, regularly update and audit a firewall, email filter and antivirus software to protect the messaging system from unexpected threats at the email gateway.

## USER TRAINING & AWARENESS

While the right mix of email security technologies is necessary to achieve compliance, technologies are only as smart as the people using them. Educate users on acceptable use policies for email; train them to identify fraudulent email, phishing scams and other pretexting that threatens the security of messaging system and integrity of customer information floating within it.

# Compliance doesn't have to be complex

Despite PCI DSS providing clear direction to the form businesses email security systems should take, many businesses struggle to secure cardholder information exchanged via email, and even when they do, data breaches still happen. The problem is often that the technologies designed to help meet complex compliance requirements are often as complicated as the regulations themselves, posing their own set of challenges to securing email:

## DIFFICULT TO USE, DIFFICULT TO ADOPT

Often technologies created to ensure regulatory compliance inhibit email functionality and workflow, frustrating users. According to a 2011 study by the Ponemon Institute, over half of email encryption users were frustrated with their encryption solutions being inflexible and difficult to use. When technology is difficult to use, managers may have difficulty enforcing policy and users may opt not to use them, which can expose your organization to data leakage and compliance violations.

## PKI KEY MANAGEMENT IS TIME CONSUMING & EXPENSIVE

It's no secret that key management is costly. While a key management solution may be necessary for encryption with outdated technology, the cost and time involved to manage it is more than just an inconvenience—eating into management productivity and your budget. Yet the alternative of selecting a cheap solution could result in unrecoverable data. According to a 2011 study, About 52 percent of the businesses said they have had serious key management problems, with about a third claiming that keys were lost or misplaced keys and another third citing key failure.

## DATA LEAKAGE CAN STILL OCCUR

The understated truth is that compliance does not equal security. Businesses that implement vendors' technologies for secure email, technologies that claim to conform to PCI DSS requirements, don't always have the features necessary to catch user mistakes and policy violations that result in data loss.

---

Solutions for secure email should complement existing email rather than complicate it. It is important to implement a solution that conforms to requirements for PCI DSS and is powerful enough to prevent data loss without compromising the functionality and workflow of existing email that your business depends on. With many out-of-the-box solutions floating around the market, your organization should consider a solution that works well with existing email to simplify complexity of management, and encourages adoption use by end users.

## How DeliverySlip supports compliance

DeliverySlip is a cloud solution for email encryption, secure file transfer and DLP that helps address PCI DSS requirements, and lets you use your email just the way it is. With DeliverySlip, you can:

- Send secure messages right from your existing email client including Microsoft Office 365, Google G-Suite, Outlook, and from any mobile device
- Leverage the Delivery Slip on every message to add controls, authentication, track live updates, true message recall and full audit and eDiscovery capabilities
- Conform to GLBA technical requirements for secure transmission of NPI.
- Automate and securely deliver messages and file attachments decrypted to any email archive database or third party application through a secure API
- Secure communication and collaboration anytime, anywhere, by allowing users to send, track and receive secure email and attachments on any mobile device including iOS, Android and Windows Phone

DeliverySlip

# About DeliverySlip

Powered by 10 patents and stress tests by KPMG, you can trust DeliverySlip to keep your communications safe. DeliverySlip is the leader in email encryption and file security. Used and trusted in virtually every industry with over 5 million users and growing every day.

*Be Productive, Be Collaborative, Be Secure*

**TRY IT FREE | DELIVERYSLIP.COM OR 1.877.404.9964**