PCI COMPLIANCE

WHAT IT IS AND HOW TO MAINTAIN IT

INTRODUCTION

Payment Card Industry Security Standard Council (PCI SSC) was founded in 2009 by American Express, Discover, JCB International, MasterCard, and Visa Inc. to set, uphold, evolve, and promote the safety of cardholder data through mandatory requirements that every merchant must abide by. The global council works with millions of organizations, including merchants, financial institutions, point-of-sale vendors, and software and hardware developers, to focus on two main objectives. The first is to assist merchants and financial institutions with understanding what the security standards are. The council also provides critical tools for implementing these security standards and technologies that protect the merchants' systems from a security breach. The second focus is helping vendors who create payment solutions understand and implement these standards in their technologies.

WHY IS IT IMPORTANT?

A breach involving payment card data can affect every party involved. As a cardholder, the risks include identity theft and fraudulent charges. In addition, cardholders may have to report unauthorized charges and request a new payment card from their provider, which can cause delay and inconvenience. From the merchant's side, the effects are less conspicuous, but can be even more costly. Some of the potential risks to merchants include…

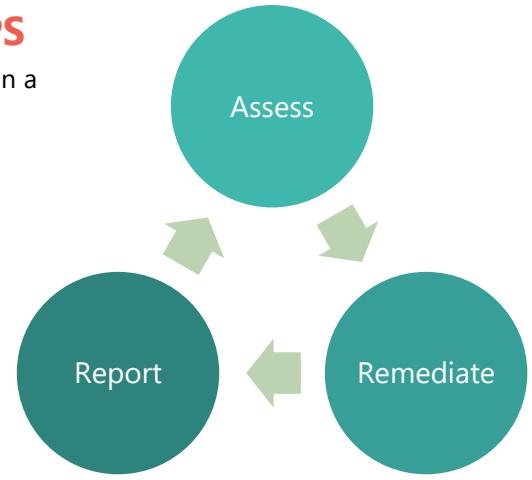
- Fines and penalties
- Loss of ability to accept payment cards
- Cost of reissuing new payment cards
- Higher costs of trying to achieve/maintain compliance
- Legal costs including settlements
- Loss of credibility and business

HOW IS CARDHOLDER DATA STOLEN?

Cardholder data can be stolen from multiple locations: databases, filling cabinets, compromised card readers, cameras recording entry of authentication data, and secret taps inserted into a store's wireless or wired network. Cardholder data should be secured at the point-of-entry (when it is captured), during processing, and when it is stored for future processing.



ACHIEVING PCI COMPLIANCE – 3 STEPS



Most businesses don't realize that PCI compliance is more than a once-a-year event, which can create a false sense of security. Continuously monitoring and enforcing the Payment Card Industry's Data Security Standards (PCI DSS) is the greatest way to maximize security of cardholder data. Here are three steps for getting started on achieving PCI Compliance:

1

The first step of implementing PCI DSS is to **Assess**. This is an annual process that involves identifying all system components that are located within or linked to the cardholder data environment. This includes environments comprised of people, processes, and technology that deal with cardholder data or sensitive authentication data.

The processes involved in the Assess step include:

- Identifying cardholder data
- Taking inventory of IT assets
- Taking inventory of business processes for payment processing
- Analyzing the first three for vulnerabilities

2

The second step is **Remediate**, or fixing any vulnerabilities within your software or business practices.

The processes involved in the Remediate step include:

- Securing any vulnerable business processes
- Removing any unnecessary cardholder data storage

Removing Cardholder Data from Local Storage

Merchants can choose to store cardholder data off-premises using methods like tokenization and cloud-based storage. Tokenization stores the actual cardholder data at the merchant's payment gateway and sends only a token back to the payment software application for processing. A cloud-based processing method uses iframes to process credit cards through locally installed applications without actually storing credit card data in the local database.

3

The third step is **Report**. One requirement of PCI compliance is to submit regular reports to your acquiring bank and payment card brands that you do business with if you fall within merchant levels 1 -3. Here is a chart to use as a guideline on how the levels are determined. However, it is best to contact your acquiring bank for assistance in determining exactly which merchant level you fall under.

Merchant Levels for PCI

Level	MasterCard	Visa	American Express	Discover
1	Over 6 million combined MasterCard and Maestro Transactions; suffered from a hack	Over 6 Million Transactions per year	2.5 million or more transactions per year	Over 6 Million Transactions per year
2	1-6 million combined MasterCard and Maestro transactions	1-6 Million Transactions per year	50,000 to 2.5 million transactions per year	1-6 Million Transactions per year
3	Over 20,000 combined MasterCard and Maestro	20,000 to 1 Million ecommerce transactions per year	Less than 50,000 transactions per year	20,000 to 1 Million transactions per year
4	All other merchants	Less than 20,000 ecommerce transactions per year	--	Less than 20,000 transactions per year
EMV	--	--	50,000 Transactions or more per year, of which total Transactions at least 75% are made by the Card member with the physical Card present at a Point of Sale System	--

MAINTAINING PCI COMPLIANCE

Maintaining the PCI Security Standards is a requirement for every organization that processes and/or stores cardholder data. Below is a list of goals and requirements according to the PCI compliance website (https://www.pcisecuritystandards.org/):

Secure Your Network

- Use and regularly update anti-virus software or programs
- Create strong passwords instead of using vendor-supplied default passwords

REMEMBER

The PCI DSS applies to ALL organizations and entities that process, transmit, and store cardholder and/or authentication data.

Protect Payment Card Data

- Only use payment software that has been validated by the PCI SSC
- Install and maintain proper firewalls
- Encrypt the transmission of payment card data across any open networks

Restrict Unnecessary Access to Sensitive Data

- Provide access to cardholder data only to those that need it
- Assign a unique ID to personnel with computers to track/monitor access to data
- Restrict physical access to cardholder data
- Regularly monitor and test networks and business processes

Create Security Policies

- Share and enforce security policies with all internal personnel and contractors

PCI SSC Overview

The PCI Security Standards Council oversees cardholder security and offers standards and supporting materials to ensure that security. They offer information and training on safe handling of cardholder information, prevention, detection, and appropriate reaction to security breaches. Becoming PCI compliant is necessary because preventing a breach or hack of sensitive information is vital to the success of an organization. In order to achieve the PCI Security Standards, an organization must follow specific compliance procedures. Once PCI compliance is achieved, it must be maintained. This is done by continuously monitoring security, sending follow up reports, and completing compliance questionnaires.

"Payment security is a paramount for every merchant, financial institution or other entity that stores, processes or transmits cardholder data" (www.pcisecuritystandards.org).

Nodus Technologies, Inc.

Nodus Technologies provides businesses and developers with integrated payment solutions for Microsoft Dynamics ERPs and CRM, on-premises or in the cloud. Our expertise in electronic payment processing, B2B & B2C eCommerce, online bill pay, and cloud payment solutions assists organizations of any size and industry with achieving PCI compliance while automating accounts receivables, expediting funding, and improving the customer experience.

Nodus can help merchants obtain PCI Compliance by providing certified payment applications, P2PE and EMV-supported devices, and cloud-based processing and storage technology.

Contact Us

(909)-482-4701

sales@nodus.com

www.nodus.com

MERCHANT ECOMMERCE
EMV
CREDIT CARD
PAYMENT
P2PE
ONLINE BILL PAY
PA-DSS
ECHECK
PROCESSING
SECURITY
GATEWAY