



## PROTECTING CREDIT CARD DATA

# PCI Compliance: What It Is and Why It Matters

## What is Payment Card Industry Data Security Standard (PCI DSS)?

PCI DSS is a set of technical and operational mandates designed to ensure that all organizations that process, store or transmit credit card information maintain a secure environment and safeguard sensitive credit card data.

## Who Does It Impact?

PCI compliance applies to ALL organizations, regardless of size or number of transactions, that accept, transmit, or store any cardholder data.

## What is the Purpose of PCI Compliance?

When customers provide their credit cards at point-of-sale systems, over the Internet, on the phone, or through the mail, they want assurance that their account information is safe. These standards were established to provide guidelines to ensure that the best information security practices are implemented and maintained.

## PCI DSS Overview



## What Happens If You're Not Compliant?

According to a Gartner study, failure to comply with the PCI security standards may result in heavy fines, increased processing fees, or suspension of credit card transaction processing services.

## Compliance Levels

There are typically four levels of compliance based on the number of transactions being processed, the credit card brand, and other scenarios within your organization. Level 1 can have more than 250 sub-requirements, including an on-site audit. Levels 2, 3, and 4 need to complete a Self Assessment Questionnaire (SAQ) and sign up for a quarterly scan to check vulnerabilities on all outward-facing IP addresses. Each credit card brand has established their own levels.

## PROTECTING CREDIT CARD DATA

Below is an example from Visa

<b>Level 1</b>	Processing > 6 million Visa transactions annually
<b>Level 2</b>	Processing 1 million to 6 million Visa transactions annually
<b>Level 3</b>	Processing 20,000 to 1 million Visa e-commerce transactions annually
<b>Level 4</b>	Processing < 20,000 e-commerce transactions and all other processing up to 1 million Visa transactions

\*Level 1 compliance is the strictest and most difficult certification to hold. Level 1 is validated by a third party auditor approved by the Payment Card Industry. Source: Visa CISP

### What is ACTIVE Network Doing to Meet PCI DSS?

With ACTIVE's hosted solutions, we take on the role of both applications provider and merchant, eliminating much of your PCI requirements and financial risk. We have also successfully completed a PA DSS certification. Customers can contact their account manager for further proof of compliance.

### How ACTIVE Network Can Help You with PCI Compliance

ACTIVE Network can help significantly mitigate the risks, reduce the requirements and costs, and ease some of the pains associated with PCI DSS compliance through our hosted solutions. We take on the burden of complying and ensure that the bulk of the required data security standards for credit card processing are met through our hosted network and applications.

- Mitigate Your Risks associated with Credit Card Processing – You achieve the same level of customer service without storing or processing the data yourself!
- Reduce Your Costs, Time and Resources Required for Compliance Mandates
- Reduce Your Reporting Requirements for PCI Compliance

Note: This document is intended as a basic overview only and is not a definitive guide to PCI Compliance. Resources for this information include PCI SSC and Visa CISP. Please refer to PCI SSC, credit card companies, merchant banks, and processors for specific requirements. Standards and requirements evolve and change based on the latest security best practices. Website links are subject to change. Contact us for the latest resources.

## Common PCI Acronyms

### PCI

Payment Card Industry

### PCI SSC

PCI Security Standards Council

Independent body founded by major payment card companies – American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa, Inc. – to establish security standards.

### PCI DSS

PCI Data Security Standard

Technical and operational requirements set by the Payment Card Industry Security Standards Council to protect cardholder data. See

[www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

Source: PCI SSC