



PCI DSS Quick Reference Guide

Understanding the Payment Card Industry
Data Security Standard version 3.2.1

For merchants and other entities involved in payment card processing



PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1.

Copyright 2009-2018 PCI Security Standards Council, LLC. All Rights Reserved.

This Quick Reference Guide to the PCI Data Security Standard (PCI DSS) is provided by the PCI Security Standards Council (PCI SSC) to inform and educate merchants and other entities involved in payment card processing. For more information about the PCI SSC and the standards we manage, please visit www.pcisecuritystandards.org.

The intent of this document is to provide supplemental information, which does not replace or supersede PCI Standards or their supporting documents.

July 2018

Contents

Introduction: Protecting Cardholder Data with PCI Security Standards	4
Overview of PCI Requirements.....	6
The PCI Data Security Standard	9
Security Controls and Processes for PCI DSS Requirements	11
Build and Maintain a Secure Network and Systems	12
Protect Cardholder Data	14
Maintain a Vulnerability Management Program.....	16
Implement Strong Access Control Measures	18
Regularly Monitor and Test Networks.....	21
Maintain an Information Security Policy.....	24
Compensating Controls for PCI DSS Requirements	26
How to Comply with PCI DSS	27
Choosing a Qualified Security Assessor	28
Choosing an Approved Scanning Vendor.....	29
Scope of PCI DSS Requirements	30
Using the Self-Assessment Questionnaire	33
Reporting	35
Implementing PCI DSS into Business-as-Usual Processes.....	36
Web Resources	37
About the PCI Security Standards Council	39

Introduction: Protecting Cardholder Data with PCI Security Standards

The twentieth century U.S. criminal Willie Sutton was said to rob banks because “that’s where the money is.” The same motivation in our digital age makes merchants the new target for financial fraud. Occasionally lax security by some merchants enables criminals to easily steal and use personal consumer financial information from payment card transactions and processing systems.

It’s a serious problem – more than 10.9 billion records with sensitive information have been breached according to public disclosures between January 2005 and July 2018, according to PrivacyRights.org. As you are a key participant in payment card transactions, it is imperative that you use standard security procedures and technologies to thwart theft of cardholder data.

Merchant-based vulnerabilities may appear almost anywhere in the card-processing ecosystem including:

- point-of-sale devices;
- mobile devices, personal computers or servers;
- wireless hotspots;
- web shopping applications;
- paper-based storage systems;
- the transmission of cardholder data to service providers;
- in remote access connections.

Vulnerabilities may also extend to systems operated by service providers and acquirers, which are the financial institutions that initiate and maintain the relationships with merchants that accept payment cards (see diagram on page 5).

Compliance with the PCI DSS helps to alleviate these vulnerabilities and protect cardholder data.

DATA TYPES COMPROMISED IN BREACHES

22% card track data

18% card-not-present (e-commerce)

16% financial/user credentials

Source: 2018 Trustwave Global Security Report, p. 30
<https://www2.trustwave.com/GlobalSecurityReport.html>
(form to access report)



The intent of this PCI DSS Quick Reference Guide is to help you understand how the PCI DSS can help protect your payment card transaction environment and how to apply it.

There are three ongoing steps for adhering to the PCI DSS:

Assess — identifying all locations of cardholder data, taking an inventory of your IT assets and business processes for payment card processing and analyzing them for vulnerabilities that could expose cardholder data.

Repair — fixing identified vulnerabilities, securely removing any unnecessary cardholder data storage, and implementing secure business processes.

Report — documenting assessment and remediation details, and submitting compliance reports to the acquiring bank and card brands you do business with (or other requesting entity if you're a service provider).

PCI DSS follows common-sense steps that mirror security best practices. The PCI DSS globally applies to *all* entities that store, process or transmit cardholder data and/or sensitive authentication data. PCI DSS and related security standards are administered by the PCI Security Standards Council, which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Participating Organizations include merchants, payment card issuing banks, processors, developers and other vendors.

PCI DSS COMPLIANCE IS A CONTINUOUS PROCESS

