

PCI BASICS FOR MERCHANTS

The What, Why, and How

HISTORY OF PCI

The Payment Card Industry Security Standards Council (PCI SSC) was created by the major card brands (MasterCard Worldwide, Discover Financial Services, American Express, JCB International, and Visa Inc.). The PCI Council then created the Payment Card Industry Data Security Standard (PCI DSS) to reduce payment card theft and electronic data loss

WHAT IS THE PCI DSS?

The PCI DSS is a list of card-handling practices merchants must follow to accept payment cards. This standard details how to securely handle, process, and store sensitive payment card data

WHO IS REQUIRED TO COMPLY WITH PCI DSS?

All merchants that accept Visa, MasterCard, Discover, AMEX, or JCB are required to comply with the PCI DSS

WHY SHOULD YOU CARE TO BECOME PCI DSS COMPLIANT?

Data security is more important now than ever as hackers become more prevalent. In 2016 the number of data breaches tracked in the US rose 40% according to a study by the Identity Theft Resource Center (ITRC). Becoming PCI compliant is a great step in preventing these types of attacks

- The FBI reports that socially engineered cyberattacks have cost businesses (including Snapchat and Seagate) more than \$3.1 billion in 2016 alone

PCI DSS COMPLIANCE IS MANDATED BY ALL MAJOR CARD BRANDS

Your merchant processor may require reports on your compliance status to ensure your PCI validation is current

- Failure to comply with the PCI DSS may result in the revocation of the merchant's card processing ability
- You may be charged non-compliance fees by your merchant processor
- PCI DSS compliant merchants stand a greater chance of withstanding attacks
- In the event of a data breach, the merchant is subject to fines, penalties, and associated costs resulting from the breach if the merchant is not PCI DSS compliant. These fees frequently total over \$100,000

**IN 2016 THE
NUMBER OF
DATA BREACHES
TRACKED IN
THE US ROSE
40% ACCORDING
TO A STUDY BY
THE IDENTIFY
THEFT RESOURCE
CENTER (ITRC).**

HOW TO GET COMPLIANT

Validation requirements are based on you handle and process payment cards and the number of transactions they process annually. All merchants are required to complete a Self-Assessment Questionnaire (SAQ). The required SAQ is dependent on how you store, handle, and process card data. Some additional requirements may include:

- External vulnerability scanning
- Internal vulnerability scanning
- Penetration testing
- Security policy implementation

HOW OFTEN IS PCI COMPLIANCE VALIDATION REQUIRED?

Becoming PCI Compliant is not a single event, but an ongoing process. You as a merchant are required to validate your PCI compliance on an annual basis. This includes resubmitting the SAQ and passing the required scans. Although validation is only an annual requirement, you are required and expected to comply with the PCI requirements on a daily basis. This includes monitoring the environment to identify suspicious activity to prevent a data breach

GETTING STARTED WITH PCI DSS COMPLIANCE

SecurityMetrics is a leading provider of merchant data security solutions and will help you understand how to become PCI compliant

SecurityMetrics helps your merchants:

- Understand PCI compliance
- Discover your PCI requirements
- Validate and report franchisee's PCI compliance to franchise HQ

SecurityMetrics provides:

- PCI SAQ
- External vulnerability scans
- Internal vulnerability scans
- Managed firewall
- Data security training
- Security policies and procedures
- Penetration testing
- Card Data Discovery
- Quality service guaranteed

ABOUT SECURITYMETRICS

SecurityMetrics is a global leader in merchant data security and compliance for all business sizes and merchant levels, and has helped secure over 1 million payments systems. SecurityMetrics helps organizations secure their network infrastructure, data communication, other information assets and/or manage PCI DSS compliance. As an Approved Scanning Vendor (ASV), Qualified Security Assessor (QSA), Payment Application Qualified Security Assessor (PA-QSA), Point-to-Point Encryption auditor, Penetration Tester, and Payment Card Industry Forensic Investigator (PFI), SecurityMetrics has the knowledge and tools available to help businesses achieve lasting security and validate accurate PCI compliance.