



PCI Basics For Acquirers

Never have a false
sense of security.™

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 your 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 if your portfolio is PCI DSS compliant?

Data security is more important now than ever as hackers become more prevalent. In 2021, the number of data breaches tracked in the US rose 16.5% according to a study by the Identity Theft Resource Center (ITRC). Becoming PCI compliant is a great step in preventing these types of attacks.

In 2021, the number of data breaches tracked in the US rose 16.5% according to a study by The Identify Theft Resource Center (ITRC).

PCI DSS compliance is mandated by all major card brands.

- The major card brands may require reports on the compliance status of merchants in your portfolio to ensure your PCI program is being effective.
- Failure to comply with the PCI DSS may result in the revocation of the merchant's card processing ability.
- A PCI program can help defend merchants against hacks/breaches, and also notify merchants of potential weaknesses so they can be proactive and prevent disasters before they happen.
- In the event of a data breach, both the merchant and you, the acquirer, are 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.

How to get compliant

Validation requirements are based on how merchants handle and process payment cards and the number of transactions that are processed annually. All merchants are required to complete a Self-Assessment Questionnaire (SAQ). The SAQ they are required to complete is dependent on how they 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. However, merchants are required to validate their PCI compliance on an annual basis. This includes resubmitting their SAQ and passing the required scans.

Although validation is only an annual requirement, merchants are required and expected to comply with the PCI requirements on a daily basis. This includes monitoring their 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.

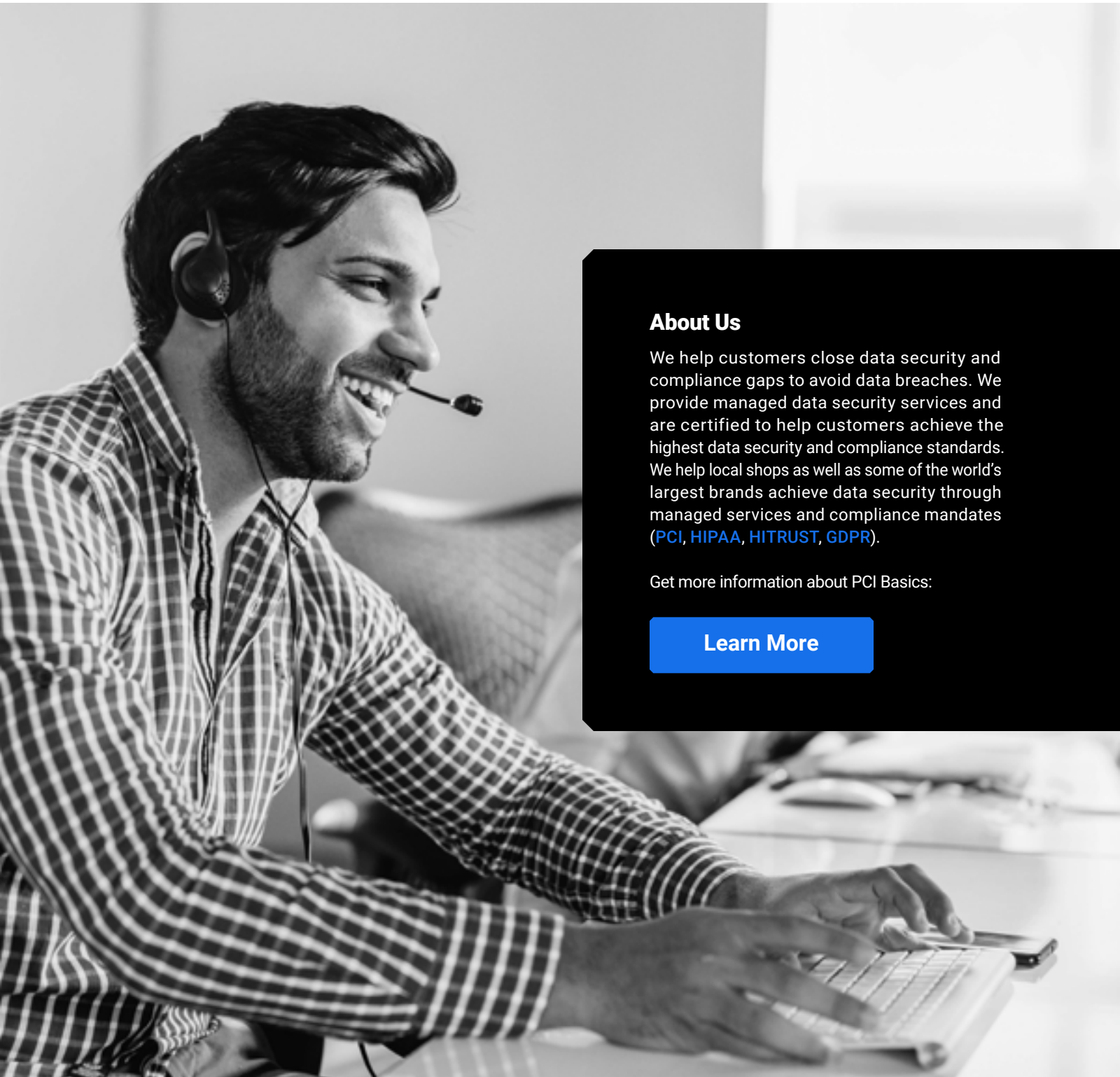
SECURITYMETRICS HELPS MERCHANTS:

- Understand PCI compliance
- Discover each business' PCI requirements
- Report PCI compliance validation to you directly

SECURITYMETRICS PROVIDES:

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





About Us

We help customers close data security and compliance gaps to avoid data breaches. We provide managed data security services and are certified to help customers achieve the highest data security and compliance standards. We help local shops as well as some of the world's largest brands achieve data security through managed services and compliance mandates ([PCI](#), [HIPAA](#), [HITRUST](#), [GDPR](#)).

Get more information about PCI Basics:

[Learn More](#)