

# GUIDE TO PCI COMPLIANCE MERCHANT LEVELS

PCI compliance is an important step for your business to process credit cards securely, but how do you know if you're validating correctly for your business? PCI requirements vary based on transactions processed annually, which determines your merchant level. This guide provides you with an overview of the varying merchant levels and lists key PCI requirements for each level.

## DEFINITION OF A MERCHANT

For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.

## LEVEL 1 MERCHANT

Merchants processing more than 6,000,000 Visa transactions annually.

### PCI Requirements

- Annual Report on Compliance (ROC) by Qualified Security Assessor (QSA)
- Quarterly network scan by Approved Scanning Vendor (ASV)
- Penetration Test
- Internal Scan
- Attestation of Compliance Form

## LEVEL 2 MERCHANT

Merchant processing 1,000,000 - 6,000,000 Visa transactions annually.

### PCI Requirements

- Annual Self-Assessment Questionnaire (SAQ) if organization has a certified Internal Security Assessor (ISA) on staff\*
- Onsite Assessment conducted by a PCI SSC approved Qualified Security Assessor (QSA)\*
- Quarterly network scan by ASV
- Attestation of Compliance Form
- Additional requirements depending on SAQ type (e.g. Penetration Test, Internal Scan)

## LEVEL 3 AND 4 MERCHANTS

Level 3 merchants process 20,000 - 1,000,000 Visa e-commerce transactions annually. Level 4 merchants process less than 20,000 Visa e-commerce transactions annual and all other merchants processing up to 1 million Visa transactions annually.

### PCI Requirements

- Annual SAQ
- Quarterly network scan by ASV
- Attestation of Compliance Form
- Additional requirements depending on SAQ type (e.g. Penetration Test, Internal Scan)

\*Effective 30 June 2012, Level 2 merchants that choose to complete an annual self-assessment questionnaire must ensure that staff engaged in the self-assessment attend PCI SSC ISA Training and pass the associated accreditation program annually in order to continue the option of self-assessment for compliance validation. Alternatively, Level 2 merchants may, at their own discretion, complete an annual onsite assessment conducted by a PCI SSC approved Qualified Security Assessor (QSA) rather than complete an annual self-assessment questionnaire.

[READ MORE](#)

## 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.