# What are the PCI compliance levels and how are they determined?

There are four PCI compliance levels and their compliance requirements vary. Merchants are assigned to a level based on their combined transaction volume — including credit, debit and prepaid cards — over a 12-month period. The four levels (from fewest to most transactions) and their requirements are:

- **Level 4:** Small businesses that process less than 20,000 eCommerce trans- actions and less than 1 million other transactions annually. Level 4 busi- nesses must complete an annual risk assessment using the appropriate PCI Self-Assessment Questionnaire (SAQ). Quarterly PCI scans, administered by an approved scanning vendor, may also be required.
- **Level 3:** Mid-sized companies — those with between 20,000 and 1 million transactions annually — fall into this level. Level 3 companies are required to complete an annual risk assessment using the appropriate SAQ. Quar- terly PCI scans, administered by an approved scanning vendor, may also be required.
- **Level 2:** Level 2 companies conduct between 1 million and 6 million trans- actions yearly. These companies are required to undergo a risk assessment every year, using the appropriate SAQ. Quarterly PCI scans, administered by an approved scanning vendor, may also be required.
- **Level 1:** “Big box” stores and major corporations are Level 1 companies, which are de ned as having a minimum of 6 million transactions per year. In addition to an annual internal audit conducted by a quali ed PCI audi- tor, Level 1 companies may also be required to undergo quarterly PCI scans administered by an approved scanning vendor.