# PCI Compliance Facts For SMBS

agj
your IT department


The Payment Card Industry Data Security Standard (PCI DSS) is a compliance standard designed to protect credit card information. Small businesses, including professional services, are required by law to comply with the requirements which has been a significant source of concern for small- and mid-sized businesses in the Gulfport, Mississippi, and surrounding areas.

The concern for many small businesses is navigating and understanding how to put compliance standards in place. The first step is to know what level of compliance your business fits into. There are four levels that are dependent on how many credit card transactions a business processes per year and the dollar amount of those transactions.

Level 1 – Businesses that do $6 million or more in transactions, accept global transactions, or have experienced a serious data breach in the past

Level 2 – $1 to $6 million in transactions

Level 3 – $20,000 to $1 million in e-commerce transactions

Level 4 – Less than $20,000 in e-commerce transactions and up to $1 million in transactions for other businesses .

Level 1 certification is the most rigorous, requiring yearly compliance checks with security professionals who are trained PCI Qualified Security Assessors (QSA). Most SMBs fall into Level 3 or Level 4. Businesses in those categories can perform their own PCI-DSS audits and self-report their compliance.

Some businesses think self-assessment means "no assessment" for compliance. That is NOT the case. Any business caught being noncompliant faces thousands of dollars in fines per day and might lose the right to process credit card transactions entirely.


## 3 Steps To Reliable PCI Compliance

Building a secure PCI compliance system requires three phases: assessment, remediation and reporting. Each step of the process raises some central concerns. Are you running a secure network and adequately protecting cardholder data? Do you have a strong vulnerability program and access controls in place? Do you have a coherent information security policy and are you regularly testing that policy?

## 1. Assess

This involves identifying what credit card data you're responsible for protecting, creating a detailed inventory of IT assets and business processes related to receiving credit card payments, and then carefully analyzing each system for security weakness. While the assessment should prioritize risks in the systems within the scope of your PCI-DSS compliance, you should evaluate the security throughout your entire company to get a comprehensive view of your organizations vlunerabilities.

## 2. Remediate

This is the time to address vulnerabilities you discovered during the assessment stage. This process begins by building a list of items that need remediation, interpreting compliance requirements to make sure you're using the correct remediation methods and gathering the evidence you'll need for PCI reporting.

## 3. Reports

Compile and submit remediation validation records, along with the compliance reports, to your banks and card brands. This process often involves submitting a completed self-assessment questionnaire (SAQ), Attestation of Compliance (AOC), along with supporting documentation - such as an approved scanning vendor (ASV) scan report.gathering the evidence you'll need for PCI reporting.

## Common SMB Struggles With PCI DSS Compliance

Small businesses most commonly struggle with the technical aspects of PCI DSS compliance, failing to maintain security software, data encryption, anti-malware software and controls to ensure data security.

One area where SMBs often have difficulty is with network segmentation. Segmentation should enable a company to isolate the Cardholder Data Environment (CDE), the portion of your network that contains or processes credit card information. In theory, this reduces the scope of your PCI implementation and makes compliance easier, but the process is much more difficult than most businesses realize. A firewall or router alone does not sufficiently separate sensitive information from the rest of your network. Hardware and software used to segment sensitive data must be hardened and configured to provide the proper level of security.

Unfortunately, businesses that fail to make themselves 100% compliant are entirely out of compliance. With no room for error, it's easy to understand why many companies choose to outsource PCI DSS compliance work to a trusted technology partner.

If you find your business has been struggling with PCI compliance or if you haven't had a PCI Assessmentin the last year –reach out to Gulfport, Mississippi's, AGJ Networks team today.

Learn more about how we can help your organization grow with a free, no-obligation IT consultation.

Call us: 228-641-4688
Email: info@agjsystems.com
14257 Dedeaux Rd. | Gulfport, MS 39503
www.agjsystems.com