PCI COMPLIANCE

Nothing in the American marketplace is more diverse than the Level 4 merchant group. Representing 98% of all U.S. retailers and primarily comprised of small to mid-sized businesses, merchants in this card-brand-defined group number in the millions.

Businesses that fall within the Level 4 merchant group do, however, share one important characteristic with the large retailers that make up the higher volume processing levels: the need to secure the data they capture during the electronic payment process.

Why is PCI necessary?

Gone are the days of small businesses "slipping under the radar" of hackers and thieves. The same technologies that make everyday business efficient also make it easy for hackers to access sensitive information. That's why a business taking "just a handful" of credit cards is no less obligated to protect that card data than the major retailer running thousands of transactions.

To that end, The Payment Card Industry (PCI) Security Standards Council (an organization formed by the card brands) created the PCI Data Security Standard (DSS) to ensure that businesses follow best practices for protecting their customers' payment card information.

What are the PCI requirements?

Build and Maintain a Secure Network

1 | Install and maintain a firewall configuration to protect cardholder data
2 | Do not use vendor-supplied defaults for system passwords and other secure parameters

Protect Cardholder Data

3 | Protect stored cardholder data
4 | Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5 | Use and regularly update anti-virus software or programs
6 | Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7 | Restrict access to cardholder data by business need-to-know
8 | Assign a unique ID to each person with computer access
9 | Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10 | Track and monitor all access to network resources and cardholder data
11 | Regularly test security systems and processes

Maintain an Information Security Policy

12 | Maintain a policy that addresses information security for employees and contractors

FiNet
a network of solutions

7355 California Ave., Boardman, OH 44512 | 800.487.5577 | finetsolutions.com

PCI COMPLIANCE

What should merchants do to remain PCI compliant?

Ultimately, PCI compliance falls on the merchant, not the processor, card issuers or customers. In many cases, adherence to PCI guidelines comes in the form of simple common-sense steps. For example, a merchant should never write down and store credit card numbers. Additionally, merchants should limit access to cardholder data to only those employees that need it.

However, as payment systems become more complex and fully integrated into other business software, some technical security requirements may extend beyond the normal scope of a merchant's expertise. In these cases, it is advisable that merchants secure a third party vendor to conduct network scans to identify potential vulnerabilities. While the process will vary depending upon the provider, many processors have established partnerships with licensed PCI certification vendors. These organizations will require a merchant to undergo a full PCI assessment, which typically includes both a questionnaire and a scan of the merchant's data network. Once successfully completed, the merchant will receive a PCI Compliance certificate valid for one year.

What are the consequences for non-compliance?

PCI is not, in itself, a law. The standard was created by the major card brands (Visa, MasterCard, Discover, AMEX and JCB), not a government agency. However, it is in the best interests of all parties involved (card brands, card issuers, processors, merchants and customers) that a merchant comply with PCI requirements to keep cardholder data secure. Securing data greatly limits the risk of a data breach or other theft of cardholder information, which could result in excessive losses for which the merchant would likely be liable.

While the specifics vary depending upon the vendors involved, most processors have implemented a series of fines for non-compliant merchants to encourage adoption to PCI standards. Some have even gone as far as to discontinue processing services for chronically non-compliant merchants.

Additional PCI information

The full set of PCI requirements can be found on the PCI Security Standards Council's website:
https://www.pcisecuritystandards.org/