

Credit Cards 101

All About PCI Compliance

What is PCI Compliance?

PCI Compliance is the payment card security standard that all merchants (businesses) and service providers must adhere to or be prohibited from attaining or keeping a merchant account which allows a business to accept credit and debit cards as payment.

PCI Compliance is a Payment Card Industry (PCI) payment acceptance security standard emplaced as a requirement in June, 2008 by the five major card issuing companies (American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc). The standard is multifaceted but basically requires that any merchant handling credit and debit cards begin adhering to certain security considerations or lose their ability to accept and process card payments. These requirements can be trying for many businesses to adhere to.

Fortunately, not all merchants are evaluated the same. The PCI Security Standards Council has established a tiered system for determining compliance based upon transaction types and the annual volume of transactions.

Merchant Level	Description
Level 1	Any merchant-regardless of acceptance channel-processing over 6,000,000 transactions per year.
Level 2	Any merchant-regardless of acceptance channel-processing 1,000,000 to 6,000,000 transactions per year.
Level 3	Any merchant processing 20,000 to 1,000,000 e-commerce transactions per year.
Level 4	Any merchant processing fewer than 20,000 e-commerce transactions or 1,000,000 total transactions per year.

What are the requirements for the merchant to be PCI-DSS compliant?

Each level has different requirements for the merchant to accept credit and debit cards:

- Level 1 Merchant: A full PCI Compliance Audit
- Level 2 Merchant: Annual PCI Self Assessment Questionnaire plus quarterly network security scans
- Level 3 Merchant: Annual PCI Self Assessment Questionnaire plus quarterly network security scans
- Level 4 Merchant: Annual PCI Self Assessment Questionnaire

Furthermore, the PCI Security Standards Council has developed three separate standards that govern the payment industry

- PCI – DSS** Payment Card Industry - Data Security Standard for merchants and processors
- PA - DSS** Payment Application - Data Security Standard for payment application vendors
- PCI – PED** Payment Card Industry - PIN Entry Devices for manufacturers of card payment products

The payment processor is responsible for the most difficult and expensive aspects of compliance. These requirements protect both the merchant and the card holding consumer from fraud, hacking, and threats to card holder data in general. The following relays the goals and requirements which must be met for the payment processor to be PCI – DSS compliant:

What is PCI-DSS?

PCI-DSS stands for Payment Card Industry (PCI) Data Security Standard (DSS). PCI-DSS is the industry security standard to protect card holder data from fraud, hacking, and would be miscreants. The standard is enforced by the collective efforts of the five major card issuing companies (American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc).

What is the purpose of PCI-DSS?

Primarily to protect card holder data by limiting where it can be stored, how it is stored, and



The First Choice in ACH Business Solutions.

www.firstach.com

Credit Cards 101 - Interchange-Plus Explained

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	<ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none"> 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 5. Use and regularly update anti-virus software of programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security for employees and contractors

What if I am not compliant?

If you have not done anything about establishing PCI compliance yet, you are not alone. There are still many merchants that have yet to establish compliance, particularly at compliance levels 3 and 4.

Not attaining compliance is certainly problematic and can lead to costly security issues and/or fines:

- Merchants can be fined for not complying in a timely manner.
- Compromised account data could lead to more and greater fines
- Security breaches
- You can lose your ability to accept credit and debit cards

	Estimated Merchants	Validated Compliance
Level 1	400	81%
Level 2	985	85%
Level 3	2,616	56%
Level 4	6,500,000	<10%

- Identify your merchant compliance level
- Obtain and complete the appropriate self assessment questionnaire for your merchant level.
- Submit your questionnaire to First ACH.
- Provide a solution to each and every area you answered "NO" to.
- Level 1 merchants must undergo a full PCI Compliance audit by a Qualified Security Assessor.
- Level 2 and 3 merchants must hire an approved scanning vendor to obtain quarterly network security scans. A solution must be provided to any area of the scan that failed.
- Level 4 merchant s are not required to complete quarterly scans but must ensure that credit card numbers are not being electronically stored on premises.
- All merchants must ensure that they are operating in a secure manner in general but shredding sensitive documents containing credit card numbers, implementing policies for the creation and use of passwords and user id's, and installing protective software such as anti-virus and anti-phishing applications on office computers can be very helpful in protecting your business from a potential security breach.

So how do I become compliant?

The good news is that by using a payment processor with PCI compliant solutions such as First ACH, you are mostly compliant already. Unless you are a Level 1 merchant, compliance requirements are limited to completing a self assessment questionnaire and undergoing quarterly network scans. Most merchants are Level 4 merchants however and simply required to do an 11 question self-assessment questionnaire if they have compliant solutions through their processor. Note that no merchant should store sensitive card holder data electronically.

First ACH
9693 Gerwig Lane Suite A
Columbia, MD 21046
800-356-2429

Better payments.