

**PCI
COMPLIANCE:**

**IS YOUR
BUSINESS
PROTECTED?**

directtec.com



PCI APPLIES TO ALL ORGANIZATIONS OR MERCHANTS, THAT ACCEPTS, TRANSMITS OR STORES ANY CARDHOLDER DATA.

Payment Card Industry (PCI) Compliance: Safety First

The major card associations, including Discover, American Express, Visa and MasterCard, have mandated compliance standards to ensure cardholder data (e.g. cardholder name, account number, expiration date) is processed, transmitted, stored and/or retained in a secure manner. Under NO circumstance should card track data be stored.

Who Must Comply with PCI Standards?

All merchants accepting credit and debit card transactions must comply with PCI standards.

What if a Merchant Does Not Comply?

This is the new mandated standard for data security. Merchants not in compliance could face significant fines and be financially responsible for any transactions that are compromised. Non-compliance fines begin at \$5000 per month.

Where Can My Business Find Out More information?

Do a Google Search on "PCI Compliance" and you will get over 1.6 Million Results. A recent survey conducted by the **Institute of Internal Auditors** revealed that nearly 90% of businesses are trying to implement a PCI Compliance process. For the latest information, please refer to these websites:

www.mastercard.com/sdp
www.pcisecuritystandards.org
www.salesynergy.com
www.themerchantmaven.com

PCI DATA SECURITY IS MANDATED BY ALL MAJOR CREDIT CARD ASSOCIATIONS.

PCI Fines Getting Stiffer

MasterCard recently updated their requirements and non-compliance fines for the Payment Card Industry Data Security Standards (PCI DSS). MasterCard requires Level 3 businesses to validate compliance and have a passing scan on record. Level 3 businesses that have not validated compliance and/or do not have a passing scan on record will be penalized.

MasterCard's updated penalty structure is below. Level 3 Merchants (See back for Level Descriptions)

\$10,000 - First Violation
\$20,000 - Second Violation
\$40,000 - Third Violation
\$80,000 - Fourth Violation

Things to Consider if Your Business is Breached

- Potential loss of customers
- Loss of reputation
- Litigation & financial damage
- Permanent inability to accept credit cards

Call DTI Today to Find Out More About PCI Compliance

Let Direct Technology Innovations provide you with a complete, secure PCI Compliance program which includes PCI Insurance. For a nominal monthly fee your business and your cardholder data will form an important alliance with compliance.



800.724.7000 ext. 456

PCI FAQ

Q: What is PCI DSS (Payment Card Industry Data Security Standard)?

A: PCI DSS (Payment Card Industry Data Security Standard) has been established through the formation of the Security Standards Council (American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. are represented on this council) to govern the acceptance, storage and transfer of credit card information in the United States. "PCI Compliant" is the typical terminology used in the credit card industry for complying with the standards established by the Security Standards Council. More information can be found at the PCI Security Standards Council website: www.pcisecuritystandards.org/.

Q: When does PCI Compliance go into effect?

A: PCI compliance has been in effect for several years, but Visa and MasterCard have only recently increased their capability to fine merchants for PCI Non-compliance and/or data compromises.

Q: How does PCI Compliance affect me and what are my responsibilities as a merchant?

A: The standard applies to all parties involved in the handling of credit cards, including merchants, Property Management Systems (PMS), Point of Sale (POS) providers, middleware companies, and credit card processors. Failure to become PCI Compliant can result in significant fines levied by Visa, MasterCard, American Express, JCB and/or Discover. The merchant's responsibility is for the merchant itself to become PCI Compliant and for all payment applications used by the merchant to be PCI Compliant.

Merchant Level Description

Level 1. Any merchant – regardless of acceptance channel — processing over 6M Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.

Level 2. Any merchant – regardless of acceptance channel — processing 1M to 6M Visa transactions per year.

Level 3. Any merchant processing 20,000 to 1M Visa e-commerce transactions per year.

Level 4. Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants — regardless of acceptance channel — processing up to 1M Visa transactions per year.

Q: How do I become PCI Compliant?

A: As a merchant, you must complete the Self Assessment Questionnaire (SAQ) and answer each question in the affirmative. There are different SAQ's specific to your merchant category. If you cannot answer "yes" to each question on the SAQ, the issue must be corrected before becoming PCI Compliant. Answers are attested to at the end of the SAQ. The SAQ must be completed annually.

Q: What is my responsibility as a merchant for the payment applications or terminals that I use?

A: The merchant is responsible for ensuring that the payment applications and terminals used are PCI Compliant. Beginning July, 2010, the Security Standards Council has mandated that all payment applications and terminals must be PCI Compliant. Failure at that time to be compliant could result in discontinuation of the merchant's ability to process credit cards and/or severe fines.

Q: Am I required to perform periodic vulnerability scanning?

A: Vulnerability scanning (computer scan for known vulnerabilities on your network) is only required for merchants utilizing Point of Sale credit card interfaces. The SAQ will inquire about the specific payment application(s) that the merchant is using and if a Point of Sale System is being used, the merchant will be notified that scanning is required on a quarterly basis. Only Security Standards Council third party approved scanning vendors may be used. Once a merchant has been successfully scanned, the merchant will receive a record of approval.

Q: What are the penalties for a merchant that is not PCI Compliant?

A: PCI Non-compliance fines begin at \$5000 per month and can be significantly higher. Additionally, a data compromise could result in Account Data Compromise Recovery (ADCR) fines, which cover partial collection of losses by credit card issuers affected by the breach. ADCR fines cover a percentage of the issuers' losses.

Q: Should I experience a security breach, and card data is compromised, what is my exposure as a merchant?

A: More significant than PCI Non-compliance fines, a data compromise could result in an Account Data Compromise Recovery (ADCR) fines. Fines can run to the hundreds of thousands of dollars.

This PCI mini - book
available as pdf file at
directtec.com