

**PAYMENT CARD INDUSTRY (PCI)**

**Background**

Payment Card Industry Data Security Standard was developed by the major credit card companies(Visa and MasterCard) as a guideline to help organizations that process card payments prevent credit card fraud, cracking and various other security vulnerabilities and threats. The global security standard includes requirements for security management, policies, procedures, network architecture, software design, data encryption, auditing/reporting and vulnerability scanning, among other critical protective measures. The standard includes 12 requirements that all businesses that handle credit card data must meet, including the use of firewalls, antivirus software, security audits, network monitoring and others.

Any company processing, storing, or transmitting payment card data must be PCI DSS compliant or risk losing their ability to process credit card payments and being audited and/or fined.

The following diagram explains the logical flow of the process itself:



## Benefits

### Benefits to Business

- Boost customer confidence through a higher level of data security
- Insulate yourself from financial losses and remediation costs
- Maintain customer trust, and safeguard the reputation of your brand
- Provide a complete 'health check' for any business that stores or transmits customer information
- Avoid the severe penalties that may be imposed on your businesses if you suffer a security breach as a result of lack of compliance to the PCI standard

### Benefits to customers

- Protect customers' personal data

## Businesses applying PCI

All members, merchants, and service providers that store, process or transmit cardholder data must comply with the PCI DSS. This includes hospitals, restaurants, insurance companies, government agencies, airlines, utilities and more. While there is no law mandating compliance, the PCI DSS is a contractual obligation. When an organization, on signs up to do business with a payment card vendor, they enter into a contractual obligation to comply with the PCI DSS.

## Statistics

- Visa Inc. announced that as of the end of 2007, more than three-fourths of the largest U.S. merchants and nearly two-thirds of medium-sized merchants have now validated their compliance with the Payment Card Industry Data Security Standard (PCI DSS).
- Visa set compliance deadlines of September 30, 2007 for the largest merchants and December 31, 2007 for middle-sized U.S. merchants.
- Visa recently began levying monthly fines of \$25,000 to U.S. merchant banks (or acquirers) for each of their large merchants that did not validate PCI DSS compliance by the deadline.
- As of January 2008, Visa is levying monthly fines of \$5,000 to U.S. acquirers for non-compliant middle-sized merchants.



## Visa Inc. Cardholder Information Security Program (CISP) PCI DSS Compliance Validation Update as of 12/31/07\*

CISP Validation Category (Visa transactions / year)	Population	Estimated % of Visa Transactions	PCI DSS Compliance Validated***	Initial Validation Submitted / Remediating	Initial Validation In Progress	Pending Commitment
Level 1 Merchants** (> 6M)	326	50%	77%	23%	0%	0%
Level 2 Merchants** (1 – 6M)	709	13%	62%	30%	8%	0%
Level 3 Merchants (e-commerce only 20,000 – 1M)	2596	< 5%	54%	20%	25%	1%

\* Validation statistics are based on merchant compliance reporting provided by acquirers.

\*\* Includes Level 1 and Level 2 merchants identified from 2004 through 2006, which are required to validate by 9/30/07 and 12/31/07 respectively. Level 1 and Level 2 merchants identified as such in 2007 must validate compliance by 9/30/08 and 12/31/08 respectively.

\*\*\* Noteworthy, 99% of Level 1 and 2 merchants confirmed that they do not store prohibited data. Acquirers of Level 1 and 2 merchants that continue to store prohibited data are subject to monthly fines.