PCI DSS Overview

What is PCI DSS?

PCI DSS is the standard security framework for the Payment Card Industry. PCI DSS stands for Payment Card Industry Data Security Standards. The core focus of the Standard is developing a process that effectively prevents, detects, and responds to security incidents.

PCI DSS was developed by the PCI Security Standards Council, which is comprised of the five major card brands: Visa International, MasterCard Worldwide, American Express, Discover Financial Services, and JCB.

PCI DSS is not a federal law; it's a regulation standard set forth for the payment card industry. While the consequences of non-compliance are different than with legal matters, they can have drastic effects on a business. Not complying with PCI DSS puts a merchant at risk of having their merchant status revoked by the card brands, leaving them unable to accept payment cards and damaging their business.

The goal of PCI DSS is to enhance the security of payment card data in the United States. PCI DSS includes 12 different requirements for merchants to adhere to along with guidance on meeting the necessary benchmarks.

Who does PCI DSS apply to?

PCI DSS applies to all entities involved in payment card processing. If an entity accepts payment cards, they are required to be compliant with PCI DSS. This includes:

- Merchants
- Processors
- Acquirers
- Issuers
- Service Providers

PCI DSS applies to all other entities that store, process, or transmit cardholder data and/or sensitive authentication data.

Cardholder Data	Sensitive Authentication Data
Primary Account Number (PAN)	Magnetic-Stripe Data
Cardholder Name	Chip Data
Expiration Date	CAV2 / CVC2 / CVV2 / CID
Service Code	PINs / PIN Blocks

Why is PCI DSS Critical to Payment Card Industry?

Payment card fraud, Identity theft, and overall personal data theft are problems that every organization must deal with in the ever-expanding information age. Every year we see major organizations fall victim to security breaches, and millions of victims have their payment card information compromised as a result. Realizing how much revenue these breaches generate in the black market prompted the card brands to develop PCI DSS in order to ensure a safer environment for their consumers.

The credit card industry has the advantage of public dependency on payment cards as a primary means of conducting business. If merchants want to accept credit or debit cards as a payment method, they must comply with the PCI DSS. Non-compliance can result in penalties for the merchants, or even having their merchant status revoked and not being allowed to accept payment cards.

Fines

The table below shows an example of a time-cost schedule which Visa uses as fines for non-compliance:

Month	**Level 1**	**Level 2**
1 to 3	**$10,000 monthly**	**$5,000 monthly**
4 to 6	**$50,000 monthly**	**$25,000 monthly**
7 and on	**$100,000 monthly**	**$50,000 monthly**

Consequences

Compliance does not equal security. A security breach may still occur and cardholder data may become compromised. A breach in cardholder data can result in the following consequences for a merchant:

- Fines for the number of cardholders' data compromised
- Suspension of credit card acceptance by a merchant's credit card account provider
- Loss of reputation with customers, suppliers, and partners
- Possible civil litigation from breached customers
- Loss of customer trust which affects future sales

Ultimately, PCI DSS was developed to reduce the fraud risk of payment card transactions by motivating merchants and service providers to protect cardholder data. It requires merchants and service providers to pay attention to many key aspects of data security including:

- Network security
- System security
- Applications security
- Security awareness
- Incidence response
- Policies

PCI DSS indirectly encourages merchants to drop cardholder data entirely and conduct business in a way that eliminates costly and risky data storage and on-site processing. The focus on security practices and technologies naturally results in a reduction of fraud.