Payment Card Industry Data Security Standard (PCI DSS)

Return to Glossary

The **Payment Card Industry Data Security Standard (PCI DSS)** is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. The PCI DSS was created jointly in 2004 by four major credit-card companies: Visa, MasterCard, Discover and American Express.

The PCI DSS specifies and elaborates on six major objectives.

1. A secure network must be maintained in which transactions can be conducted. This requirement involves the use of firewalls that are robust enough to be effective without causing undue inconvenience to cardholders or vendors. Specialized firewalls are available for Wireless Fidelity (Wi-Fi) LANs, which are highly vulnerable to eavesdropping and attacks by malicious hackers. In addition, authentication data such as Personal Identification Numbers (PINs) and passwords must not involve defaults supplied by the vendors. Customers should be able to conveniently and frequently change such data.

2. Cardholder information must be protected wherever it is stored. Repositories with vital data such as dates of birth, mothers' maiden names, Social Security numbers, phone numbers and mailing addresses should be secure against hacking. When cardholder data is transmitted through public networks, that data must be encrypted effectively. Digital Encryption is important in all forms of credit-card Transactions, but particularly in Electronic Commerce (e-Commerce) conducted on the Internet.

3. Systems should be protected against the activities of malicious hackers by using frequently updated anti-virus software, anti-spyware programs, and other anti-Malicious Software (Malware) solutions. All Application should be free of Bugs and Vulnerabilities that might open the door to Exploits in which cardholder data could be stolen or altered. Patches offered by Software (SW) and Operating System (OS) vendors should be regularly installed to ensure the highest possible level of vulnerability management.

4. Access to system information and operations should be restricted and controlled. Cardholders should not have to provide information to businesses unless those businesses must know that information to protect themselves and effectively carry out a transaction. Every person who uses a computer in the system must be assigned a unique and confidential identification name or number. Cardholder data should be Protected Physically as well as electronically. Examples include the use of document shredders, avoidance of unnecessary paper document duplication, and locks and chains on dumpsters to discourage criminals who would otherwise rummage through the trash.

5. Networks must be constantly monitored and regularly tested to ensure that all security measures and processes are in place, are functioning properly, and are kept up-do-date. For example, anti-virus and anti-spyware programs should be provided with the latest definitions and signatures. These programs should scan all exchanged data, all Applications, all Random Access Memory (RAM) and all Storage Media frequently if not continuously.

6. A formal information security policy must be defined, maintained, and followed at all times and by all

participating entities. Enforcement measures such as audits and penalties for non-compliance may be necessary.

Source: URI