# PCI DSS Glossary

| Name | Description |
|---|---|
| **Account Data** | Account data consists of cardholder data and/or sensitive authentication data. See *Cardholder Data* and *Sensitive Authentication Data.* |
| **Account Number** | See *Primary Account Number (PAN).* |
| **Acquirer** | Also referred to as “merchant bank,” “acquiring bank,” or “acquiring financial institution”. Entity, typically a financial institution that processes payment card transactions for merchants and is defined by a payment brand as an acquirer. Acquirers are subject to payment brand rules and procedures regarding merchant compliance. See also *Payment Processor.* |
| **Anti-Virus** | Program or software capable of detecting, removing, and protecting against various forms of malicious software (also called “malware”) including viruses, worms, Trojans or Trojan horses, spyware, adware, and rootkits. |
| **AOC** | Acronym for “attestation of compliance.” The AOC is a form for merchants and service providers to attest to the results of a PCI DSS assessment, as documented in the Self-Assessment Questionnaire or Report on Compliance. |
| **Application** | Includes all purchased and custom software programs or groups of programs, including both internal and external (for example, web) applications. |
| **ASV** | Acronym for “Approved Scanning Vendor.” Company approved by the PCI SSC to conduct external vulnerability scanning services. |
| **Audit Log** | Also referred to as “audit trail.” Chronological record of system activities. Provides an independently verifiable trail sufficient to permit reconstruction, review, and examination of sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from inception to final results. |
| **Audit Trail** | See *Audit Log.* |
| **Authentication** | Process of verifying identity of an individual, device, or process. Authentication typically occurs through the use of one or more authentication factors such as:<br> Something you know, such as a password or passphrase<br> Something you have, such as a token device or smart card |
| **Backup** | Duplicate copy of data made for archiving purposes or for protecting against damage or loss. |
| **Card Skimmer** | A physical device, often attached to a legitimate card-reading device, designed to illegitimately capture and/or store the information from a payment card. |
| **Card Verification Code or Value** | Also known as Card Validation Code or Value, or Card Security Code. Refers to either: (1) magnetic-stripe data, or (2) printed security features.<br>(1) Data element on a card's magnetic stripe that uses secure cryptographic processes to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. The following list provides the terms for each card brand:<br> CAV – Card Authentication Value (JCB payment cards)<br> CVC – Card Validation Code (MasterCard payment cards)<br> CVV – Card Verification Value (Visa and Discover payment cards)<br> CSC – Card Security Code (American Express)<br>(2) For Discover, JCB, MasterCard, and Visa payment cards, the second type of card verification value or code is the rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit un-embossed number printed above the PAN on the face of the payment cards. The code is uniquely associated with each individual piece of plastic and ties the PAN to the plastic. The following list provides the terms for each card brand:<br> CID – Card Identification Number (American Express and Discover payment cards) |
| **Cardholder** | Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card. |
| **Cardholder Data** | At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code |
| | See *Sensitive Authentication Data* for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction. |
| **CDE** | Acronym for “cardholder data environment.” The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data. |
| **Cellular Technologies** | Mobile communications through wireless telephone networks, including but not limited to Global System for Mobile communications (GSM), code division multiple access (CDMA), and General Packet Radio Service (GPRS). |

| Name | Description |
|---|---|
| **Change Control** | Processes and procedures to review, test, and approve changes to systems and software for impact before implementation. |
| **Compensating Controls** | Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must:<br>(1) Meet the intent and rigor of the original PCI DSS requirement;<br>(2) Provide a similar level of defense as the original PCI DSS requirement; (3) Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and<br>(4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.<br>See "Compensating Controls" Appendices B and C in PCI DSS Requirements and Security Assessment Procedures for guidance on the use of compensating controls. |
| **Compromise** | Also referred to as "data compromise," or "data breach." Intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected. |
| **Data-Flow Diagram** | A diagram showing how data flows through an application, system, or network. |
| **Database** | Structured format for organizing and maintaining easily retrievable information. Simple database examples are tables and spreadsheets. |
| **Database Administrator** | Also referred to as "DBA." Individual responsible for managing and administering databases. |
| **Default Password** | Password on system administration, user, or service accounts predefined in a system, application, or device; usually associated with default account. Default accounts and passwords are published and well known, and therefore easily guessed. |
| **DSS** | Acronym for "Data Security Standard." See PA-DSS and PCI DSS. |
| **Dual Control** | Process of using two or more separate entities (usually persons) operating in concert to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person is permitted to access or use the materials (for example, the cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires dividing knowledge of the key among the entities. (See also Split Knowledge.) |
| **Encryption** | Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure. See Strong Cryptography. |
| **End to End Encryption (E2EE)** | The information is encrypted by the sender (at read head of terminal) and is not decrypted until end point. The cryptographic keys needed to decrypt the information is housed at end point receiver. |
| **File Integrity Monitoring** | Technique or technology under which certain files or logs are monitored to detect if they are modified. When critical files or logs are modified, alerts should be sent to appropriate security personnel. |
| **File-Level Encryption** | Technique or technology (either software or hardware) for encrypting the full contents of specific files. Alternatively, see Disk Encryption or Column-Level Database Encryption. |
| **Firewall** | Hardware and/or software technology that protects network resources from unauthorized access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria. |
| **Forensics** | Also referred to as "computer forensics." As it relates to information security, the application of investigative tools and analysis techniques to gather evidence from computer resources to determine the cause of data compromises. |
| **FTP** | Acronym for "File Transfer Protocol." Network protocol used to transfer data from one computer to another through a public network such as the Internet. FTP is widely viewed as an insecure protocol because passwords and file contents are sent unprotected and in clear text. FTP can be implemented securely via SSH or other technology. See S-FTP. |
| **GSM** | Acronym for "Global System for Mobile Communications." Popular standard for mobile phones and networks. Ubiquity of GSM standard makes international roaming very common between mobile phone operators, enabling subscribers to use their phones in many parts of the world. |

| Name | Description |
|---|---|
| **HECVAT** | Acronym for Higher Education Cloud Vendor Assessment Tool |
| **HTTP** | Acronym for “hypertext transfer protocol.” Open internet protocol to transfer or convey information on the World Wide Web. |
| **HTTPS** | Acronym for “hypertext transfer protocol over secure socket layer.” Secure HTTP that provides authentication and encrypted communication on the World Wide Web designed for security-sensitive communication such as web-based logins. |
| **ID** | Identifier for a particular user or application. |
| | |
| **IDS** | Acronym for Intrusion  Detection System. An intrusion detection system is a type of security software designed to automatically alert administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations |
| **Incident Response** | An organized approach to addressing and managing the aftermath of a security breach or cyberattack.  The goal is to handle the situation in a way that limits damage and reduces recovery time and costs. |
| **Index Token** | A cryptographic token that replaces the PAN, based on a given index for an unpredictable value. |
| **Information Security** | Protection of information to ensure confidentiality, integrity, and availability. |
| **IP** | Acronym for “internet protocol.” Network-layer protocol containing address information and some control information that enables packets to be routed and delivered from the source host to the destination host. IP is the primary network-layer protocol in the Internet protocol suite. See TCP. |
| **ISA** | Internal Security Assessor Designation- a program that teaches you how to perform internal assessments and recommend solutions to remediate issues related to PCI DSS compliance.  Assessors are sponsored by their companies and will be able to act as a liaison with external PCI auditors and QSA’s. |
| **Issuer** | Entity that issues payment cards or performs, facilitates, or supports issuing services including but not limited to issuing banks and issuing processors. Also referred to as “issuing bank” or “issuing financial institution.” |
| **LAN** | Acronym for “local area network.” A group of computers and/or other devices that share a common communications line, often in a building or group of buildings. |
| **Magnetic-Stripe Data** | See Track Data. |
| **Malicious Software / Malware** | Software or firmware designed to infiltrate or damage a computer system without the owner's knowledge or consent, with the intent of compromising the confidentiality, integrity, or availability of the owner’s data, applications, or operating system. Such software typically enters a network during many business-approved activities, which results in the exploitation of system vulnerabilities. Examples include viruses, worms, Trojans (or Trojan horses), spyware, adware, and rootkits. |
| **Masking** | In the context of PCI DSS, it is a method of concealing a segment of data when displayed or printed. Masking is used when there is no business requirement to view the entire PAN. Masking relates to protection of PAN when displayed or printed. See Truncation for protection of PAN when stored in files, databases, etc. |
| **Merchant** | For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers. |
| **MO/TO** | Acronym for “Mail-Order/Telephone-Order.” |
| **Mobile Payments** | In PCI, it is generally used as a wireless payment terminal with payment middleware that may be sent via internet or cellular technology. A mobile payment is money paid for a product through a portable electronic device such as a tablet or cell phone. |
| **Network** | Two or more computers connected via physical or wireless means. |
| **Network Security Scans (Internal and External)** | Process by which an entity’s systems are remotely checked for vulnerabilities through use of manual or automated tools. Security scans that include probing internal and external systems and reporting on services exposed to the network. Scans may identify vulnerabilities in operating systems, services, and devices that could be used by malicious individuals. |

| Name | Description |
|---|---|
| **Network Administrator** | Personnel responsible for managing the network within an entity. Responsibilities typically include but are not limited to network security, installations, upgrades, maintenance and activity monitoring. |
| **P2PE** | Acronym for Point to Point Encryption.  Point to point encryption solution is a council validated solution.  A solution must be validated to be able for the merchant to utilize the Self-Assessment Questionnaire P2PE. |
| **PA-DSS** | Acronym for “Payment Application Data Security Standard.” |
| **PA-QSA** | Acronym for “Payment Application Qualified Security Assessor.” PA-QSAs are qualified by PCI SSC to assess payment applications against the PA-DSS. Refer to the *PA-DSS Program Guide* and *PA-QSA Qualification Requirements* for details about requirements for PA-QSA Companies and Employees. |
| **PAN** | Acronym for “primary account number” and also referred to as “account number.” Unique payment card number (typically for credit or debit cards) that identifies the issuer and the cardholder account. |
| **Password / Passphrase** | A string of characters that serve as an authenticator of the user. |
| **Payment Application** | In the context of PA-DSS, a software application that stores, processes, or transmits cardholder data as part of authorization or settlement, where the payment application is sold, distributed, or licensed to third parties. Refer to *PA-DSS Program Guide* for details. |
| **Payment Cards** | For purposes of PCI DSS, any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or Visa, Inc. |
| **Payment Processor** | Sometimes referred to as “payment gateway” or “payment service provider |
|  | (PSP)”. |
|  | Entity engaged by a merchant or other entity to handle payment card transactions on their behalf. While payment processors typically provide acquiring services, payment processors are not considered acquirers unless defined as such by a payment card brand. See also *Acquirer.* |
| **PCI** | Acronym for “Payment Card Industry.” |
| **PCI DSS** | Acronym for “Payment Card Industry Data Security Standard.” |
| **PCIP** | Payment Card Industry Professional- An individual, entry-level qualification in payment security information.  This designation demonstrates a level of understanding that can provide a strong foundation for a career in the payments security industry. |
| **Personally Identifiable Information** | Information that can be utilized to identify or trace an individual’s identity including but not limited to name, address, social security number, biometric data, date of birth, etc. |
| **PIN** | Acronym for “personal identification number.” Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder’s signature. |
| **POI** | Acronym for “Point of Interaction,” the initial point where data is read from a card. An electronic transaction-acceptance product, a POI consists of hardware and software and is hosted in acceptance equipment to enable a cardholder to perform a card transaction. The POI may be attended or unattended. POI transactions are typically integrated circuit (chip) and/or magnetic-stripe card-based payment transactions. |
| **Policy** | Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures |
| **POS** | Acronym for “point of sale.” Hardware and/or software used to process payment card transactions at merchant locations. |
| **Privileged User** | Any user account with greater than basic access privileges. Typically, these accounts have elevated or increased privileges with more rights than a standard user account. However, the extent of privileges across different privileged accounts can vary greatly depending on the organization, job function or role, and the technology in use. |
| **PTS** | Acronym for “PIN Transaction Security,” PTS is a set of modular evaluation requirements managed by PCI Security Standards Council, for PIN acceptance POI terminals. Please refer to www.pcisecuritystandards.org. |

| Name | Description |
|---|---|
| **Public Network** | Network established and operated by a third-party telecommunications provider for specific purpose of providing data transmission services for the public. Data over public networks can be intercepted, modified, and/or diverted while in transit. Examples of public networks include, but are not limited to, the Internet, wireless, and mobile technologies. See also *Private Network* . |
| **QSA** | Acronym for “Qualified Security Assessor.” QSAs are qualified by PCI SSC to perform PCI DSS on-site assessments. Refer to the *QSA Qualification Requirements* for details about requirements for QSA Companies and Employees. |
| **Remote Access** | Access to computer networks from a location outside of that network. Remote access connections can originate either from inside the company’s own network or from a remote location outside the company’s network. An example of technology for remote access is *VPN* . |
| **Risk Analysis / Risk Assessment** | Process that identifies valuable system resources and threats; quantifies loss exposures (that is, loss potential) based on estimated frequencies and costs of occurrence; and (optionally) recommends how to allocate resources to countermeasures to minimize total exposure. |
| **ROC** | Acronym for “Report on Compliance.” Report documenting detailed results from an entity’s PCI DSS assessment. |
| **SAQ** | Acronym for “Self-Assessment Questionnaire.” Reporting tool used to document self-assessment results from an entity’s PCI DSS assessment. |
| **Scoping** | Process of identifying all system components, people, and processes to be included in a PCI DSS assessment. The first step of a PCI DSS assessment is to accurately determine the scope of the review. |
| **Security Officer** | Primary person responsible for an entity’s security-related matters. |
| **Sensitive Area** | Any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present such as the cashier areas in a retail store. |
| **Separation of Duties** | Practice of dividing steps in a function among different individuals, to keep a single individual from being able to subvert the process. |
| **Server** | Computer that provides a service to other computers, such as processing communications, file storage, or accessing a printing facility. Servers include, but are not limited to web, database, application, authentication, DNS, mail, proxy, and NTP. |
| **Service Provider** | Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. If an entity provides a service that involves *only* the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services). |
| **Spyware** | Type of malicious software that when installed, intercepts or takes partial control of the user’s computer without the user’s consent. |
| **SysAdmin** | Abbreviation for “system administrator.” Individual with elevated privileges who is responsible for managing a computer system or network. |
| **Token** | In the context of authentication and access control, a token is a value provided by hardware or software that works with an authentication server or VPN to perform dynamic or two-factor authentication. See *RADIUS, TACACS,* and *VPN.* See also *Session Token* . |
| **Track Data** | Also referred to as “full track data” or “magnetic-stripe data.” Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. Can be the magnetic-stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe. |
| **Transaction Data** | Data related to electronic payment card transaction. |
| **Trojan** | Also referred to as “Trojan horse.” A type of malicious software that when installed, allows a user to perform a normal function while the Trojan performs malicious functions to the computer system without the user’s knowledge. |
| **Truncation** | Method of rendering the full PAN unreadable by permanently removing a segment of PAN data. Truncation relates to protection of PAN when *stored* in files, databases, etc. See *Masking* for protection of PAN when *displayed* on screens, paper receipts, etc. |

| Name | Description |
|---|---|
| **Two-Factor Authentication (2FA) or Multi-factor Authentication** | Sometimes referred to as two-step verification, multi-factor or dual factor authentication. It is a security process in which the user provides two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access. Two-factor authentication methods rely on users providing a password as well as a second factor, usually either a security token or a biometric factor like a fingerprint or facial scan. |
| **Third Party Service Provider** | An entity that is involved in some way in an interaction that is primarily between two other entities |
| **VPN** | Acronym for "virtual private network." A computer network in which some of connections are virtual circuits within some larger network, such as the Internet, instead of direct connections by physical wires. The end points of the virtual network are said to be tunneled through the larger network when this is the case. While a common application consists of secure communications through the public Internet, a VPN may or may not have strong security features such as authentication or content encryption. |
| | A VPN may be used with a token, smart card, etc., to provide two-factor authentication. |
| **Web Application** | An application that is generally accessed via a web browser or through web services. Web applications may be available via the Internet or a private, internal network. |
| **Wireless Networks** | Network that connects computers without a physical connection to wires. |
| **WLAN** | Acronym for "wireless local area network." Local area network that links two or more computers or devices without wires. |
| **WPA/WPA2** | Acronym for "WiFi Protected Access." Security protocol created to secure wireless networks. WPA is the successor to WEP. WPA2 was also released as the next generation of WPA. |