

## Glossary

Term	Definition
<b>Access control</b>	Measures that limit access to information or information processing resources to those authorized persons or applications.
<b>Account harvesting</b>	A method to determine existing user accounts based on trial and error. Giving too much information in an error message can disclose information that makes it easier for an attacker to penetrate or compromise the system.
<b>Account number</b>	The payment card number (credit or debit) that identifies the issuer and the particular cardholder account.
<b>Acquirer</b>	A bankcard association member that initiates and maintains relationships with merchants that accept Visa or MasterCard cards.
<b>Asset</b>	Information or information processing resources of an organization.
<b>Audit Log</b>	A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results. Sometimes specifically referred to as a security audit trail.
<b>Authentication</b>	The process of verifying identity of a subject or process.
<b>Authorization</b>	The granting of access or other rights to a user, program, or process
<b>Backup</b>	A duplicate copy of data made for archiving purposes or for protecting against damage or loss.
<b>Card-validation code</b>	The three-digit value printed on the signature panel of a payment card used to verify card-not-present transactions. On a MasterCard payment card this is called CVC2. On a Visa payment card this is called CVV2.
<b>Cardholder</b>	The customer to whom a card has been issued or the individual authorized to use the card.
<b>Cardholder data</b>	All personally identifiable data about the cardholder and relationship to the Member (i.e., account number, expiration date, data provided by the Member, other electronic data gathered by the merchant/agent, and so on). This term also accounts for other personal insights gathered about the cardholder (i.e., addresses, telephone numbers, and so on).
<b>Compromise</b>	An intrusion into a computer system where unauthorized disclosure, modification, or destruction of cardholder data may have occurred.
<b>Console</b>	A screen and keyboard which allows access and control of the server / mainframe in a networked environment.
<b>Consumer</b>	Individual purchasing goods and /or services.
<b>Cookies</b>	A string of data exchanged between a web server and a web browser to maintain a session. Cookies may contain user preferences and personal information.
<b>Database</b>	A structured format for organizing and maintaining information that can be easily retrieved. A simple example of a database is a table or a spreadsheet.

<b>Term</b>	<b>Definition</b>
<b>DBA</b>	Doing Business As. Compliance validation levels are based on the transaction volume of a DBA or chain of stores (not of a corporate that owns several chains).
<b>Default accounts</b>	A system login account that has been predefined in a manufactured system to permit initial access when the system is first put into service.
<b>Default password</b>	The password on system administration or service accounts when a system is shipped from the manufacturer, usually associated with the default account. Default accounts and passwords are published and well known.
<b>Dual Control</b>	A method of preserving the integrity of a process by requiring that several individuals independently take some action before certain transactions are completed.
<b>DMZ (de-militarized zone)</b>	A network added between a private network and a public network in order to provide an additional layer of security.
<b>Egress</b>	Traffic leaving the network.
<b>Encryption</b>	The process of converting information into a form unintelligible to anyone except 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.
<b>Firewall</b>	Hardware and/or software that protect the resources of one network from users from other networks. Typically, an enterprise with an intranet that allows its workers access to the wider Internet must have a firewall to prevent outsiders from accessing its own private data resources.
<b>Host</b>	The main hardware on which software is resident.
<b>Information Security</b>	Protection of information for confidentiality, integrity and availability.
<b>Ingress</b>	Traffic entering the network.
<b>Intrusion detection Systems</b>	An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.
<b>IP address</b>	An IP address is a numeric code that uniquely identifies a particular computer on the Internet.
<b>IP Spoofing</b>	A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.
<b>ISO 8583</b>	An established standard for communication between financial systems.
<b>Key</b>	In cryptography, a key is a value applied using an algorithm to unencrypted text to produce encrypted text. The length of the key generally determines how difficult it will be to decrypt the text in a given message.
<b>Magnetic Stripe Data (Track Data)</b>	Data encoded in the magnetic stripe used for authorization during a card present transaction. Entities may not retain full magnetic stripe data subsequent to transaction authorization. Specifically, subsequent to authorization, service codes, discretionary data/CVV, and Visa reserved values must be purged; however, account number, expiration date, and name may be extracted and retained.

<b>Monitoring</b>	A view of activity on a network.
<b>Network</b>	A network is two or more computers connected to each other so they can share resources.
<b>Network Address Translation (NAT)</b>	The translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network.
<b>Non consumer users</b>	Any user, excluding consumer customers, that accesses systems, including but not limited to, employees, administrators, and third parties.
<b>Password</b>	A string of characters that serve as an authenticator of the user.
<b>Patch</b>	A quick-repair job for a piece of programming. During a software product's beta test distribution or try-out period and later after the product is formally released, problems will almost invariably be found. A patch is the immediate solution that is provided to users.
<b>Penetration</b>	The successful act of bypassing the security mechanisms of a system.
<b>Penetration Test</b>	The security-oriented probing of a computer system or network to seek out vulnerabilities that an attacker could exploit. The testing involves an attempt to penetrate the system so the tester can report on the vulnerabilities and suggest steps to improve security.
<b>System Perimeter Scan</b>	A non-intrusive test which involves probing external-facing systems and reporting on the services available to the external network (i.e. services available to the Internet).
<b>Policy</b>	Organizational-level rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures.
<b>Procedure</b>	A procedure provides the descriptive narrative on the policy to which it applies. It is the "how to" of the policy. A procedure tells the organization how a policy is to be carried out.
<b>Protocol</b>	An agreed-upon method of communication used within networks. A specification that describes the rules and procedures products should follow to perform activities on a network.
<b>Risk Analysis</b>	Also known as risk assessment, a process that systematically identifies valuable system resources and threats to those resources, quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence, and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure.
<b>Router</b>	A router is a piece of hardware or software that connects two or more networks. A router functions as a sorter and interpreter as it looks at addresses and passes bits of information to their proper destinations. Software routers are sometimes referred to as gateways.
<b>Sanitization</b>	To delete sensitive data from a file, a device, or a system; or modify data so that data is useless for attacks.
<b>Security Officer</b>	The person who takes primary responsibility for the security related affairs of the organization.

<b>Security policy</b>	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
<b>Sensitive cardholder data</b>	Data whose unauthorized disclosure may be used in fraudulent transaction. It includes, the account number, magnetic stripe data, CVC2/CVV2 and expiration date.
<b>Separation of duties</b>	The practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process.
<b>Server</b>	A computer that acts as a provider of some service to other computers, such as processing communications, file storage, or printing facility.
<b>SQL injection</b>	A form of attack on a database-driven Web site in which the attacker executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet. SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization's host computers through the computer that is hosting the database.
<b>SSL</b>	An established industry standard that encrypts the channel between a web browser and Web server to ensure the privacy and reliability of data transmitted over this channel.
<b>Tamper-resistance</b>	A system is said to be tamper-resistant if it is difficult to modify or subvert, even for an assailant who has physical access to the system.
<b>Threat</b>	A condition that may cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the organization.
<b>Token</b>	A device that performs dynamic authentication.
<b>Transaction data</b>	Data related to an electronic payment.
<b>Truncation</b>	The practice of removing a data segment. Commonly, when account numbers are truncated, the first 12 digits are deleted, leaving only the last 4 digits.
<b>Two-factor authentication</b>	Authentication that requires users to produce two credentials - something they have (e.g., smartcards or hardware tokens), and something they know (e.g., a password). In order to access a system, users must produce both factors.
<b>UserID</b>	A character string that is used to uniquely identify each user of a system.
<b>Virus</b>	A program or a string of code that can replicate itself and cause the modification or destruction of software or data.
<b>Vulnerability</b>	A weakness in system security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy.
<b>Vulnerability Scan</b>	An automated tool that checks a merchant or service provider's systems for vulnerabilities. The tool remotely reviews networks and Web applications based on the external-facing Internet protocol (IP) addresses. Scans identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network.