PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL

Glossary of Payment and Information Security Terms

DATA SECURITY ESSENTIALS FOR SMALL MERCHANTS

A PRODUCT OF THE PAYMENT CARD INDUSTRY SMALL MERCHANT TASK FORCE

VERSION 2.0 | AUGUST 2018

PCi Security Standards Council®

Introduction

This *Glossary of Payment and Information Security Terms* is a supplement to the *Guide to Safe Payments*, part of the Data Security Essentials for Small Merchants. Its intent is to explain relevant Payment Card Industry (PCI) and information security terms in easy-to-understand language.

Definitions for terms marked with an asterisk (*) are based on or derived from definitions in the *Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS): Glossary of Terms, Abbreviations, and Acronyms*. The latest version of this glossary is considered the authoritative source, and must be referred to for the current and complete PCI DSS and PA-DSS definitions.

Please refer to the Data Security Essentials for Small Merchants at the following:

RESOURCE	URL
Guide to Safe Payments	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
Common Payment Systems	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Questions to Ask Your Vendors	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf
Evaluation Tool	https://www.pcisecuritystandards.org/merchants/ This tool is provided for merchant information only. An option for merchants is to use it as a first step to gain insight about security practices relevant to the way they accept payments, to provide their initial responses, and to see their results.

Glossary

TERM	DEFINITION
Acquirer *	See *Merchant Bank* and *Payment Processor.*
Anti-Virus Software *	Software program that detects, removes, and protects against malicious software (also called "malware") including viruses, worms, Trojans or Trojan horses, spyware, adware, and rootkits. Also called "anti-malware software."
Application *	Software program or group of programs that runs on a PC, smartphone, tablet, internal server, or web server.
Approved Scanning Vendor (ASV) *	Company approved by the PCI Security Standards Council to conduct external vulnerability scanning services to identify common weaknesses in system configuration.
Authentication *	Method for verifying the identity of a person, device, or process attempting to access a computer. To confirm the identity/user is valid, one or more of the following is provided: • A password or passphrase (something the user knows) • A token, smart card, or digital certificate unique to the user (something the user has) • A biometric identifier, such as a fingerprint (something the user is or does)
Authorization *	In a payment card transaction, authorization occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.
Bank Identification Number (BIN)	The first six digits (or more) of a payment card number that identifies the financial institution that issued the payment card to the cardholder.
Business Need-to-Know	The principle that access to systems or data is granted by a user's business need—only what is necessary for a user's job function.
Card Data / Customer Card Data *	At a minimum, card data includes the primary account number (PAN), and may also include cardholder name and expiration date. The PAN is visible on the front of the card and encoded into the card's magnetic stripe and/or the embedded chip. Also referred to as cardholder data. See also *Sensitive Authentication Data* for additional data elements which may be part of a payment transaction but which must not be stored after the transaction is authorized.
Chip	Also known as "EMV Chip." The microprocessor (or "chip") on a payment card used when processing transactions in accordance with the international specifications for EMV transactions.
Chip and PIN	A verification process where a consumer enters their PIN in an EMV Chip-enabled payment terminal when they purchase goods or services.

Glossary

TERM	DEFINITION
Chip and Signature	A verification process where a consumer uses their signature with an EMV Chip-enabled payment terminal when they purchase goods or services.
Credential	Information used to identify and authenticate a user for access to a system. For example, credentials are often the username and password. Credentials may include a fingerprint, retina scan, or a one-time number generated by a portable "token-generator." Security is stronger when access requires multiple credentials.
Cryptography	Cryptography is the method of securing data by making it unintelligible to a human or computer. Cryptography is only useful when the intended recipient can reassemble the data into a readable form using a method known only to the sender and receiver. See also *Encryption*.
Cyber-Attack	Any offensive action to break into a computer or system. Cyber-attacks can range from installing spyware on a PC, breaking into a payment system to steal card data, or attempting to break critical infrastructure such as an electric power grid.
Data Breach	A data breach is an incident in which sensitive data may have potentially been viewed, stolen, or used by an unauthorized party. Data breaches may involve card data, personal health information (PHI), personally identifiable information (PII), trade secrets, or intellectual property, etc.
Default Password	A simple password that comes with new software or hardware. Default passwords (like "admin" or "password" or "123456") are easily guessed and usually are available via online search. They are intended as a placeholder and offer no real security—and must be changed to a stronger password after installing new software or hardware.
Data Security Essentials (DSE)	Data Security Essentials for Small Merchants is a set of educational resources and an evaluation tool to help merchants simplify their security and reduce risk. DSE is intended as an alternative approach to the PCI DSS Self-Assessment Questionnaires (SAQs) for those merchants designated as eligible by the payment brands and their acquirers (merchant banks).
Electronic Cash Register (ECR)	A device that registers and calculates transactions and may print out receipts, but does not accept customer card payments. Also called a "till."
Encryption	Process of using cryptography to mathematically convert information into a form unusable except to holders of a specific digital key. Use of encryption protects information by devaluing it to criminals. See also *Cryptography*.
Firewall *	Hardware and/or software that protects network resources from unauthorized access. A firewall permits or denies communication between computers or networks with different security levels based upon a set of rules and other criteria.

Glossary

TERM	DEFINITION
Forensic Investigator	PCI Forensic Investigators (PFIs) are companies approved by the PCI Council to help determine when and how a card data breach occurred. They perform investigations within the financial industry using proven investigative methodologies and tools. They also work with law enforcement to support stakeholders with any resulting criminal investigations.
Hacker	A person or organization that attempts to circumvent security measures of computer systems to gain control and access. Usually this is done in an effort to steal card data.
Hosting Provider *	Offers various services to merchants and other service providers, where their customers' data is "hosted" or resident on the provider's servers. Typical services include shared space for multiple merchants on a server, providing a dedicated server for one merchant, or web apps such as a website with "shopping cart" options.
Integrated Payment Terminal	A payment terminal and electronic cash register in one device that takes payments, registers and calculates transactions, and prints receipts.
Integrator/Reseller	An integrator/reseller is a company that merchants work with to help set up their payment system. This may include installation, configuration, and support. These companies may also sell the payment devices or applications as part of their service. See also *Qualified Integrator Reseller (QIR).*
Log *	A file that is created automatically when certain predefined (often security-related) events occur within a computer system or network. Log data includes date/time stamp, description of the event, and information unique to that event. These files are useful for troubleshooting technical issues or a data breach investigation. Also called an "audit log" or "audit trail."
Malware *	Malicious software designed to infiltrate a computer system with the intent of stealing data, or damaging applications or the operating system. Such software typically enters a network during many business-approved activities such as via email or browsing websites. Malware examples include viruses, worms, Trojans (or Trojan horses), spyware, adware, and rootkits.
Merchant Bank *	A bank or financial institution that processes credit and/or debit card payments on behalf of merchants. Also called an "acquirer," "acquiring bank," "card processor," or "payment processor." See also *Payment Processor.*
Mobile Device	Devices such as smart phones and tablets that are small, portable, and can connect to computer networks wirelessly.
Mobile Payment Acceptance	Using a mobile device to accept and process payment transactions. The mobile device is usually paired with a commercially available card-reader accessory.

Glossary

TERM	DEFINITION
Multi-factor Authentication *	Method of authenticating a user when two or more factors are verified. These factors include something the user has (such as a smart card or dongle), something the user knows (such as a password, passphrase, or PIN) or something the user is or does (such as fingerprints, other forms of biometrics, etc.).
Network *	Two or more computers connected via physical or wireless means.
Operating System *	Software on a computer system that provides overall management and coordination of computer activities. Examples include Microsoft Windows, Apple OSX, iOS, Android, Linux, and UNIX.
P2PE	Acronym for the PCI Security Standards Council's Point-to-Point-Encryption standard. See details at *www.pcisecuritystandards.org*.
PA-DSS *	Acronym for the PCI Security Standards Council's Payment Application Data Security Standard. See details at *www.pcisecuritystandards.org*.
Password *	A word, phrase, or string of characters used to authenticate a user. When combined with the username, the password is intended to prove the identity of the user for access to computer resources.
Patch *	Update to existing software that adds functionality or corrects a defect (or "bug").
Payment Application *	Related to PA-DSS, a software application that stores, processes, or transmits cardholder data as part of authorization or settlement of payment transactions.
Payment Application Vendor	Vendor that sells applications that store, process, and/or transmit card data during payment transactions.
Payment Middleware	A general term for software that connects two or more, perhaps unrelated, payment applications together. For example, it may pass card data between an application on a payment terminal and other merchant systems that send card data to a processor.
Payment Processor *	Entity engaged by merchants to handle payment card transactions on their behalf. While payment processors typically provide acquiring services, payment processors are not considered acquirers (merchant banks) unless defined as such by a payment card brand. Also called a "payment gateway" or "payment service provider" (PSP). See also *Merchant Bank.*
Payment System	Encompasses the entire process for accepting card payments in a merchant retail location (including stores/shops and e-commerce storefronts) and may include a payment terminal, an electronic cash register, other devices or systems connected to the payment terminal (for example, Wi-Fi for connectivity or a PC used for inventory), servers with e-commerce components such as payment pages, and the connections out to a merchant bank.

Glossary

TERM	DEFINITION
Payment System Vendor	A vendor who sells, licenses, or distributes a complete payment solution to a merchant. The solution encompasses the hardware and software needed to handle payments within the store and provides a method to connect to a payment processor.
Payment Terminal	Hardware device used to accept customer card payments via swipe, dip, insert, or tap. Also called “point-of-sale (POS) terminal,” “credit card machine,” or “PDQ terminal.”
PCI *	Acronym for Payment Card Industry.
PCI DSS *	Acronym for the PCI Council's “Payment Card Industry Data Security Standard.” See details at *www.pcisecuritystandards.org.*
PCI DSS Compliant	Meeting all applicable requirements of the current PCI DSS, on a continuous basis via a business-as-usual approach. Compliance is assessed and validated at a single point in time; however, it is up to each merchant to continuously follow the requirements in order to provide strong security. Merchant banks and/or the payment brands may have requirements for formal annual validation of PCI DSS compliance.
PCI DSS Validated	Providing proof that all applicable PCI DSS requirements are met at a single point in time. Depending on specific merchant bank and/or payment brand requirements, validation can be achieved through the applicable PCI DSS Self-Assessment Questionnaire or by a Report on Compliance resulting from an onsite assessment.
PCI Validated Payment Application	Software application that has been validated per the PCI Payment Application Data Security Standard (PA-DSS) and is listed on the PCI Council website.
PCI-Approved Payment Terminal	Payment terminal that has been approved per the PCI PIN Transaction Security (PTS) standard and is listed on the PCI Council website.
PCI-Listed Point-to-Point Encryption Solution	Encryption solution that has been validated per the PCI Point-to-Point-Encryption (P2PE) standard and is listed on the PCI Council website.
PED *	Acronym for "PIN entry device." Keypad into which the customer enters their PIN. Also called a “PIN pad.”
PIN *	Acronym for "personal identification number." A unique number known only to the user and a system to authenticate the user to the system. Typical PINs are used for automated teller machines for cash advance transactions, or for EMV chip cards to replace a cardholder’s signature. PINs help determine whether a cardholder is authorized to use the card and to prevent its unauthorized use if the card is stolen.
Primary account number (PAN) *	Unique number for credit and debit cards that identifies the cardholder account.

Glossary

TERM	DEFINITION
Privilege Abuse	Using computer system access privileges in an abusive manner. Examples include a system administrator accessing card data for malicious purposes, or someone stealing and using an administrator's elevated access privileges for malicious purposes.
PTS *	Acronym for the PCI Council's PIN Transaction Security standard. PTS is a set of modular evaluation requirements for PIN acceptance point-of-interaction (POI) terminals. See details at www.pcisecuritystandards.org.
QIR *	Acronym for "Qualified Integrator or Reseller." QIRs are integrators and resellers specially trained by the PCI Security Standards Council to address critical security controls when installing merchant payment systems. See details at *www.pcisecuritystandards.org*.
Qualified Security Assessor (QSA) *	A company approved by the PCI Security Standards Council to validate an entity's adherence to PCI DSS requirements.
Recurring Payment	A billing method where merchants bill their customers repeatedly over time, such as for monthly memberships or subscriptions. A secure way to do this is for the acquirer/processor to tokenize the card data, which ensures its protection and relieves the merchant from this responsibility.
Remote Access *	Access to a computer network 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. An example of technology for remote access is a virtual private network (VPN). Remote access can be either internal (e.g. IT support) or external (e.g., service providers, third-party agents, integrators/resellers).
Reseller / Integrator *	An entity that sells and/or integrates payment applications but does not develop them.
Router *	Hardware or software that connects two or more internal or external computer networks to "route" or guide data through a network, and to ensure the data flows properly between those networks. The router can also create more security by permitting only approved traffic and denying unapproved traffic.
Secure Card Reader (SCR)	A PTS-approved device that attaches to a mobile phone or tablet for securely accepting payment cards. PCI PTS-approved SCRs protect and encrypt the card data via SRED. See also *SRED*.
Security Code *	A three- or four-digit value printed onto the front or back signature panel of a payment card. This code is uniquely associated with an individual card and is used as an additional check to ensure that the card is in possession of the legitimate cardholder, typically during a card-not-present transaction. Also referred to as card security code.

Glossary

TERM	DEFINITION
Self-Assessment Questionnaire (SAQ) *	A questionnaire covering a set of PCI DSS requirements that is completed by the organization itself to confirm it is meeting those requirements.
Sensitive Authentication Data *	Security-related information used to authenticate cardholders and/or authorize payment card transactions, stored on the card's magnetic stripe or chip.
Service Provider *	A business entity that provides various services to merchants. Typically, these entities store, process, or transmit card data on behalf of another entity (such as a merchant) OR are managed service providers that provide managed firewalls, intrusion detection, hosting, and other IT-related services. Also called a "vendor."
Skimming	Stealing card data directly from the consumer's payment card or from the payment infrastructure at a merchant location such as with an unauthorized hand-held card reader or via modifications made to the merchant's payment terminal. Its purpose is to commit fraud, the threat is serious, and it can hit any merchant's environment.
Skimming Device	A physical device, often attached to a card-reading device, designed to illegally capture and/or store the information from a payment card. Also called a "card skimmer."
Small Merchant	A small merchant is typically an independently owned and operated business with a single location or a few locations, and with limited or no IT budget and often with no IT personnel. Whether a small merchant is required to validate PCI compliance is determined by the payment brand or acquirer (merchant bank).
SRED	An acronym for "Secure Reading and Exchange of Data." A set of PCI PTS requirements designed to protect and encrypt card data in payment terminals. A PCI Council-listed Point-to-Point Encryption (P2PE) solution must use a PTS-approved and listed payment terminal with SRED enabled and actively performing card data encryption.
Stand-Alone Terminal	A payment terminal that does not rely on connection to any other device within the merchant environment and performs no other functions. The only requirement for it to operate is a connection to the processor through either an Internet connection or a telephone line. If the terminal requires connection to a computerized electronic cash register or is multi-function (like a mobile device), it is not a stand-alone terminal.
Strong Authentication	Used to verify the identity of a user or device to ensure the security of the system it protects. The term strong authentication often means with multifactor authentication (MFA).
Till	See *Electronic Cash Register.*

Glossary

TERM	DEFINITION
Tokenization	A process by which the primary account number (PAN) is replaced with an alternative value called a token. Tokens can be used in place of the original PAN to perform functions when the card is absent like voids, refunds, or recurring billing. Tokens also provide more security if stolen because they are unusable and thus have no value to a criminal.
Unencrypted Data	Any data that is readable without the need to decrypt it first. Also called "plaintext" and "clear-text" data.
Vendor	A business entity that supplies a merchant with a product or service needed for the course of business. Where services are offered, the vendor may be considered a service provider and may require access to physical locations or computer systems within the merchant environment that could affect the security of card data. See also *Service Provider.*
Virtual Payment Terminal *	Web-browser-based access to an acquirer, processor or third-party service provider website to authorize payment card transactions. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card. The merchant manually enters payment card data via the securely connected web browser. Because payment card transactions are entered manually, virtual payment terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.
Virtual Private Network (VPN) *	Software that creates a secure, private channel for exchanging data and conducting phone calls over the Internet.
Virus	Malware that replicates copies of itself into other software or data files on an "infected" computer. Upon replication, the virus may execute a malicious payload, such as deleting all data on the computer. A virus may lie dormant and execute its payload later, or it may never trigger a malicious action. A virus that replicates itself by resending itself as an e-mail attachment or as part of a network message is called a "worm."
Vulnerability *	Flaw or weakness which, if abused, may result in an intentional or unintentional compromise of a system.
Vulnerability Scan	A software tool that detects and classifies potential weak points (vulnerabilities) on a computer or network. A quarterly external vulnerability scan per PCI DSS Requirement 11.2.2 must be performed by an Approved Scanning Vendor. Other vulnerability scans (such as internal scans and those performed after network changes) can be conducted by qualified staff in an organization's IT department or by a security service provider (such as an Approved Scanning Vendor). *See also Approved Scanning Vendor (ASV).*
Wi-Fi *	Wireless network that connects computers without a physical connection to wires.
Wireless Payment Terminal	Payment terminal that connects to the Internet using any of various wireless technologies.