Glossary Terms for Credit Card Business

AAA - Acronym for "authentication, authorization, and accounting." Protocol for authenticating a user based on their verifiable identity, authorizing a user based on their user rights, and accounting for a user's consumption of network resources.

Access control - Mechanisms that limit availability of information or information-processing resources only to authorized persons or applications.

Account Data - Account data consists of cardholder data plus sensitive authentication data. See Cardholder Data and Sensitive Authentication Data

Account number - See Primary Account Number (PAN).

ACH (Automated Clearing House) - Electronic funds transfer system governed by the NACHA OPERATING RULES which provide for the interbank clearing of electronic payments for participating depository financial institutions. The Federal Reserve and Electronic Payments Network act as ACH Operators, central clearing facilities through which financial institutions transmit or receive ACH entries.

Acquirer - Also referred to as "acquiring bank" or "acquiring financial institution." An entity that initiates and maintains relationships with merchants for the acceptance of payment cards.

Adware - Type of malicious software that, when installed, forces a computer to automatically display or download advertisements.

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.

Application - Includes all purchased and custom software programs or groups of programs, including both internal and external (for example, web) applications.

Audit Trail - See Audit Log.

ASV - Acronym for "Approved Scanning Vendor." Company approved by the PCI SSC to conduct external vulnerability scanning services.

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:

- Something you know, such as a password or passphrase
- Something you have, such as a token device or smart card
- Something you are, such as a biometric

Authentication Credentials - Combination of the user ID or account ID plus the authentication factor(s) used to authenticate an individual, device, or process.

Authorization - Granting of access or other rights to a user, program, or process. For a network, authorization defines what an individual or program can do after successful authentication. For the purposes of a payment card transaction authorization occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.

Breach – The unintentional release of secure information. This includes incidents such as theft, loss, or exposure of credit card or other personally identifiable information records in paper or electronic form.

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.

Cardholder Data Environment - The people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components.

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.

1. Data element on a card's magnetic stripe that uses secure cryptographic process 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:
    - **CAV** - Card Authentication Value (JCB payment cards)
    - **CVC** - Card Authentication Value (JCB payment cards)
    - **CVV** - Card Validation Code (MasterCard payment cards)
    - **CSC** - Card Security Code (American Express)
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 unembossed 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:
    - **CID** - Card Identification Number (American Express and Discover payment cards)
    - **CAV2** - Card Authentication Value 2 (JCB payment cards)
    - **CVC2** - Card Validation Code 2 (MasterCard payment cards)
    - **CVV2** - Card Verification Value 2 (Visa payment cards)

Cash – "Cash" receipts include currency, coin, checks, money orders, credit/debit cards, and electronic funds transfers.

Chargeback – The required reversal of a credit card transaction to return funds to a card holder due to a complaint filed by the customer. A customer may initiate a chargeback by contacting their issuing bank

and filing a substantiated complaint. The complaint may be refuted by the University. The dispute is then settled by the applicable Credit Card Company.

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: (1) Meet the intent and rigor of the original PCI DSS requirement; (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 (4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement. 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.

Consumer - Individual purchasing goods, services, or both.

Convenience Fee - A fee that is added to on-line or credit card payments.

Credit Card Number – A unique number used in a financial transaction that identifies a particular credit card account (customer).

Database - Structured format for organizing and maintaining easily retrievable information. Simple database examples are tables and spreadsheets.

Data Base Administrator - Also referred to as "DBA." Individual responsible for managing and administering databases.

Default Accounts - Login account predefined in a system, application, or device to permit initial access when system is first put into service. Additional default accounts may also be generated by the system as part of the installation process.

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.

Deposit Transmittal – Form which accompanies the physical transfer of all university funds to the Cashier's Office for processing of the bank deposit and posting to the general ledger.

Discount rate – This is a per transaction charge for each credit card transaction. The rate is variable depending on several factors, some of which include the interchange rate at the time, the type of credit card being used, the method in which the card is processed, etc.

Disk Encryption - Technique or technology (either software or hardware) for encrypting all stored data on a device (for example, a hard disk or flash drive). Alternatively, File-Level Encryption or Column-Level Database Encryption is used to encrypt contents of specific files or columns.

DNS - Acronym for "Domain Name System" or "domain name server." System that stores information associated with domain names in a distributed database on networks such as the Internet.

DSS - Acronym for "Data Security Standard" and also referred to as "PCI DSS".

E-Commerce – The buying and selling of products or services over electronic systems such as the Internet and other computer networks

EFT (Electronic Funds Transfer) - Electronic Funds Transfer. Any transfer of funds that is initiated by electronic means, such as an electronic terminal, telephone, computer, ATM or magnetic tape.

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.

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.

Funds - Any form of tender (cash, checks, credit cards, ACH, debit cards, web checks, etc).

Hashing - Process of rendering cardholder data unreadable by converting data into a fixed-length message digest via Strong Cryptography. Hashing is a (mathematical) function in which a non-secret algorithm takes any arbitrary length message as input and produces a fixed length output (usually called a "hash code" or "message digest"). A hash function should have the following properties: (1) It is computationally infeasible to determine the original input given only the hash code, (2) It is computationally infeasible to find two inputs that give the same hash code. In the context of PCI DSS, hashing must be applied to the entire PAN for the hash code to be considered rendered unreadable. It is recommended that hashed cardholder data includes a salt value as input to the hashing function (see Salt).

Host - Main computer hardware on which computer software is resident.

Hosted Payment Gateway - With a hosted payment gateway, no cardholder data is stored, processed or transmitted on UNCW premises or through a UNCW network, or stored on a UNCW server. The 3rd party hosting the payment gateway must be confirmed annually to be PCI DSS compliant.

Hosting Provider - Offers various services to merchants and other service providers. Services range from simple to complex; from shared space on a server to a whole range of "shopping cart" options; from payment applications to connections to payment gateways and processors; and for hosting dedicated to just one customer per server. A hosting provider may be a shared hosting provider, who hosts multiple entities on a single server.

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.

Information Security -Protection of information to insure confidentiality, integrity, and availability.

Information System - Discrete set of structured data resources organized for collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

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.”

Issuing Services -Examples of issuing services may include but are not limited to authorization and card personalization.

Magnetic-Stripe Data - Also referred to as “track 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.

Mainframe - Computers that are designed to handle very large volumes of data input and output and emphasize throughput computing. Mainframes are capable of running multiple operating systems, making it appear like it is operating as multiple computers. Many legacy systems have a mainframe design.

Malicious Software / Malware - Software designed to infiltrate or damage a computer system without the owner‹s knowledge or consent. 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.

Merchant Account - A special account number that numerically identifies each merchant, outlet, or line of business to the Processor for accounting and billing purposes.

Merchant Identification Number - Unique merchant identification number that is used in conjunction with all transactions by the approved merchant.

MSA – Acronym for "Master Services Agreement".

NACHA (National Automated Clearing House Association) - The Electronic Payments Association is a not-for-profit association that oversees the Automated Clearing House (ACH) Network, one of the largest electronic payment networks in the world.

Network - Two or more computers connected together via physical or wireless means.

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.

Network Components - Include, but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.

Network Security Scan - 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.

Operating System / OS - Software of a computer system that is responsible for the management and coordination of all activities and the sharing of computer resources. Examples of operating systems include Microsoft Windows, Mac OS, Linux and Unix.

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 particular cardholder account.

Password - A string of characters that serve as an authenticator of the user.

Patch - Update to existing software to add functionality or to correct a defect.

Payment Application - Any application that stores, processes, or transmits cardholder data as part of authorization or settlement.

Payment Card - 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 Card Industry (PCI) Data Security Standards (PCIDDS) - The compliance requirements that have been established by the leading card associations with the objective of improving the safekeeping of cardholder information and the prevention of system breaches.

Payment Gateway - An e-commerce application that transmits, authorizes, and settles web payments. Payment gateways protect credit card details by encrypting sensitive information, such as full credit card numbers, to ensure that information is passed securely between the customer and the merchant and also between the merchant and the payment processor.

Penetration Test - Penetration tests attempt to exploit vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application testing as well as controls and processes around the networks and applications, and occurs from both outside the network trying to come in (external testing) and from inside the network.

Personnel - Full-time and part-time employees, temporary employees, contractors, and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.

Personally Identifiable Information - An individual's personal data that may be subject to misuse. Examples include full credit card number, credit card expiration date, credit card security code, social security number, medical records, student records, bank account numbers, 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.

Policy - Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures.

POS (Point of Sale) terminal or machine - A device placed in a merchant location which is connected to the Processor's system via analog telephone lines and is designed to authorize, record and settle data by electronic means for all sales transactions with Processor.

Point of Sale System - A point of sale system refers to the computer hardware, software and checkout terminals used by departmental staff to process in-person customer transactions, create and print receipts, and maintain and update the associated data bases and reports. POS systems process and transmit card holder data but do not store card holder data on University equipment or systems.

Private Network - Network established by an organization that uses private IP address space. Private networks are commonly designed as local area networks. Private network access from public networks should be properly protected with the use of firewalls and routers.

Procedure - Descriptive narrative for a policy. Procedure is the "how to" for a policy and describes how the policy is to be implemented.

Protocol - Agreed-upon method of communication used within networks. Specification describing rules and procedures that computer products should follow to perform activities on a network.

Public Network - Network established and operated by a 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 in scope of the PCI DSS include, but are not limited to, the Internet, wireless, and mobile technologies.

PVV - Acronym for "PIN verification value." Discretionary value encoded in magnetic stripe of payment card.

QSA - Acronym for "Qualified Security Assessor," company approved by the PCI SSC to conduct PCI DSS on-site assessments.

Remote Access - Access to computer networks from a remote location, typically originating from outside the network. An example of technology for remote access is VPN.

Removable Electronic Media - Media that store digitized data and which can be easily removed and/or transported from one computer system to another. Examples of removable electronic media include CD-ROM, DVD-ROM, USB flash drives and removable hard drives.

Revenue Safeguarding Procedures - Procedures established to ensure funds received by a department are properly protected and recorded on University financial records.

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 so as to minimize total exposure.

Rootkit - Type of malicious software that when installed without authorization, is able to conceal its presence and gain administrative control of a computer system.

Router - Hardware or software that connects two or more networks. Functions as sorter and interpreter by looking at addresses and passing bits of information to proper destinations. Software routers are sometimes referred to as gateways.

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.

Secure Website - A web site that provides the capability of securely and privately exchanging data and financial transactions. This involves the encryption of data in transit.

Security Code - A three- or four-digit value printed on the card or signature strip on the back of the card, used to verify that the customer has the card in their possession or has a least physically seen the card.

Security Officer - Primary responsible person for an entity's security-related affairs.

Security Policy - Set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Protocols - Network communications protocols designed to secure the transmission of data. Examples of security protocols include, but are not limited to SSL/TLS, IPSEC, SSH, etc.

SAQ - Acronym for “Self-Assessment Questionnaire.” Tool used by any entity to validate its own compliance with the PCI DSS.

Separation of Duties - Practice of dividing steps in a function among different individuals, so as 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 Code - Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.

Service Provider - Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. 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. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.

Smart Card - Also referred to as “chip card” or “IC card (integrated circuit card).” A type of payment card that has integrated circuits embedded within. The circuits, also referred to as the “chip,” contain payment card data including but not limited to data equivalent to the magnetic-stripe data.

Spyware - Type of malicious software that when installed, intercepts or takes partial control of the user’s computer without the user’s consent.

Threat - Condition or activity that has the potential to 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.

Transaction Data - Data related to electronic payment card transaction.

Transaction Fee – Service costs charged to a merchant on a per transaction basis.

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.

Trusted Network - Network of an organization that is within the organization’s ability to control or manage.

Virtual Terminal - A virtual terminal is web-browser-based access to an acquirer, processor or third party service provider website to authorize payment card transactions, where the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.

VPN - Acronym for "virtual private network." A computer network in which some 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.

Vulnerability - Flaw or weakness which, if exploited, may result in an intentional or unintentional compromise of a system.

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.

Web Server - Computer that contains a program that accepts HTTP requests from web clients and serves the HTTP responses (usually web pages).

Wireless Access Point - Also referred to as "AP." Device that allows wireless communication devices to connect to a wireless network. Usually connected to a wired network, it can relay data between wireless devices and wired devices on the network.

Wireless Networks - Network that connects computers without a physical connection to wires.