eCommerce Glossary

Analog: For eCommerce purposes, a non- digital line i.e., a phone line as opposed to a network or Ethernet cable.

Attestation: To certify by signature the accuracy and truthfulness of information provided. Attestation is one component of the Payment Card Industry Data Security Standards (PCI DSS) validation process.

Authorization: In the context of a payment card transaction, authorization is the first step in processing a payment card. It occurs when a merchant enters cardholder data for a transaction to their bank (acquirer) for processing and requests approval to proceed with the sale. The merchant's acquiring bank then routes the request to the card-issuing bank where the transaction is authorized or denied and the response is then routed back to the merchant or their processing system.

Cardholder Data (CHD): At minimum, CHD consists of the full Primary Account Number (PAN). CHD 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.

Card Present (CP): A payment card transaction made where the credit card is physically present (e.g., a face to face transaction, or a customer swiping their card directly into a POS terminal).

Card Not Present (CNP): A payment card transaction made where the merchant does not see or touch the card and the cardholder does not, or cannot physically present their card for direct input to the merchant's card/chip reader (e.g., transactions entered over the internet, telephone, mail, or fax).

Credit/Debit Card Processing: Act of storing, processing, or transmitting credit/debit cardholder data.

eCommerce: Any internet-enabled financial transaction.

Employee: Any employee (as defined by the Employee Handbook): faculty, student employee, or contractor employed by a third party and providing services to UNC Charlotte.

Master Services Agreement (MSA): The contract between a merchant and a bank that defines their respective rights, duties, and warranties regarding how each will handle bank card transactions/activity. The MSA for the University is contracted through the state of North Carolina.

Merchant: Any entity that accepts payment cards as payment for goods and/or services.

Merchant Account: A bank account established to allow a business to accept payment card transactions.

Multifactor Authentication: A means of authenticating a user when two or more factors are verified. These factors include something the user has (such as a smart card, dongle, or device), 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.)

PAN: Acronym for "primary account number" and also referred to as "account number." It is a unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

Payment Card Industry Data Security Standards (PCI DSS): A proprietary information security standard for organizations or entities that store, process, or transmit payment card data. The Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council (PCI SSC). The Standard may be referenced at: https://www.pcisecuritystandards.org/.

Payment Card Industry Security Standards Council (PCI SSC): the governing body whose goal is to oversee the ongoing evolution of the Payment Card Industry Data Security Standard. The Council currently consists of the five major payment brands: Visa, MasterCard, American Express, Discover, and JCB, and other registered participants (e.g., banks, processors, and merchants).

Payment Cards: Any payment card/device that is used by a card/device holder and accepted by a merchant for payment of a purchase or other financial obligation. It typically bears the logo of one of the major card brands (e.g., Visa, Inc., MasterCard, American Express, Discover, and JCB International).

Payment Gateway: The application interface between the merchant or customer and the payment processor which authorizes credit card payments for internet based transactions. The gateway is responsible for receiving the payment data from the front-end system, encrypting the card information for security purposes, sending it to the bank for processing, receiving the bank's authorization, and then communicating the authorization back to the front end system.

Personally Identifiable Information (PII): Please see *Confidential University Data*.

PIN: Acronym for "personal identification number." This is a secret numeric password known only to the user and a system which is used 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.

POS - Acronym for "point of sale." Hardware and/or software used to process payment card transactions at merchant locations.

Sensitive Authentication Data (SAD) – Security related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip) PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

Security code: Also known as Card Validation Code or Value. This value appears as a three-digit value printed in the signature panel area on the back of the card for Visa, MasterCard, and Discover; or, a

four-digit number printed above the PAN on the face of an American Express card. The code is uniquely associated with each individual price of plastic and ties the PAN to the plastic.

Self-Assessment Questionnaire (SAQ): A reporting tool used by merchants and service providers to self-report their adherence to the Payment Card Industry Data Security Standards (PCI DSS).

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: A 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 have the ability to impact the security of the cardholder data (e.g., companies that provide managed firewalls or hosting services).

Third Party: An entity outside of the principal organization. For eCommerce, it is a company/software/equipment that provides payment processing functions outside of UNC Charlotte infrastructure.

Truncation: A method of rendering the full PAN unreadable by permanently removing a segment of the PAN data. Truncation relates to protection of PAN when stored on receipts or in files, databases, etc. Only the last 4 digits of the PAN should appear on a payment card transaction receipt.

Virtual Terminal: A 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 on behalf of the customer, or provides the customer with computer/device access to the internet to enter their own card transaction data for processing. Unlike POS terminals, virtual payment terminals do not read data directly from a payment card. In addition, the web interface must be properly configured to secure the CHD; it must route the transaction through the designated approved PCI network and not onto the main network for the University.