E-Commerce Policy Definitions

AOC- Attestation of compliance: a form for merchants and service providers to attest to the results of a PCI DSS assessment.

Acquirer- Also referred to as "merchant bank," or "acquiring bank," or "acquiring financial institution."

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.

CERT- "Computer Emergency Response Team" The CERT Program develops and promotes the use of appropriate technology and systems management practices to resist attacks on networked systems, to limit damage, and to ensure continuity of critical services.

Change Control- Processes and procedures to review, test, and approve changes to systems and software for impact before implementation.

Critical systems / critical technologies- A system or technology that is deemed by the entity to be of particular importance. For example, a critical system may be essential for the performance of a business operation or for a security function to be maintained. Examples of critical systems often include security systems, public-facing devices and systems, databases, and systems that store, process, or transmit cardholder data. Considerations for determining which specific systems and technologies are critical will depend on an organization's environment and risk-assessment strategy.

CVV- Also known as Card Validation Code or Value, or Card Security Code. Refers to either: (1) magnetic-stripe data, or (2) printed security features.

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

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.

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.

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 particular cardholder account.

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, 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."

PED- Acronym for "PIN entry device."

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

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

E-Commerce Policy Definitions

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.

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.

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.

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).

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.

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.

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.