PCI Glossary and Abbreviations

**Acquirer:** Also referred to as “acquiring bank” or “acquiring financial institution.” Entity that initiates and maintains relationships with merchants for the acceptance of payment cards.

**Approved Scanning Vendor (ASV):** A company/individual certified by the PCI Council to conduct vulnerability scans.

**Cardholder Data (CHD):** 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.

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

**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.

**IP Address:** Also referred to as “internet protocol address.” Numeric code that uniquely identifies a particular computer on the Internet.

**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.

**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.

**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.

**Network Segmentation:** Isolates system components that store, process, or transmit cardholder data from systems that do not. Adequate network segmentation may reduce the scope of the cardholder data environment and thus reduce the scope of the PCI DSS assessment.

**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.

**PCI DSS:** Acronym for “Payment Card Industry Data Security Standard.”

**Penetration Test:** Penetration tests attempt to exploit vulnerabilities to determine whether unauthorized access or other malicious activity is possible.

**Qualified Security Assessor (QSA):** A company/individual certified by the PCI Council to conduct PCI DSS assessments.

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

**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 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.

**Virtualization:** Virtualization refers to the logical abstraction of computing resources from physical constraints. One common abstraction is referred to as virtual machines or VMs, which takes the content of a physical machine and allows it to operate on different physical hardware and/or along with other virtual machines on the same physical hardware. In addition to VMs, virtualization can be performed on many other computing resources, including applications, desktops, networks, and storage.

**VLAN:** Abbreviation for “virtual LAN” or “virtual local area network.” Logical local area network that extends beyond a single traditional physical local area network.

**VPN:** Acronym for “virtual private network.” A computer network in which some of connections are virtual circuits within some larger network, such as the Internet, instead of direct connections by physical wires.

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