Payment Card Industry Glossary:

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

**Approved Scanning Vendor (ASV)** – An organization that has been approved by the Payment Card Industry Security Standards Council (PCI SSC) to conduct external vulnerability scanning services for PCI compliance.

**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. The acquirer obtains the transactions. UWM’s acquiring bank is US Bank.

**Card Brand** – Credit card companies including Discover Card, American Express, Visa, MasterCard, JCB and others. These are the companies that are driving PCI.

**Cardholder Data** – At a minimum, cardholder data consists of the full Primary Account Number (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.

**Consumer** – an individual who buys goods, services, or both.

**Credit Card Acceptance Team** – The governance committee at UWM responsible for aligning strategies, policies and procedures for accepting credit cards with customer needs, risk, and compliance. The work of the Team is chartered and sponsored by the Provost, the Vice Chancellor for Student Affairs, and the Vice Chancellor for Finance and Administrative Affairs. To contact the Team, send a message to: ccat@uwm.edu

**ePayment** – a digital payment for a transaction made on the Internet. Generally a more convenient approach compared to sending checks, swiping credit cards or handling paper money.

**ePayment Application** – the term used within UWM when discussing the approved online solution with US Bank.

**Hypercom** – A credit card terminal brand used by departments/units on campus.

**Issuer** – Entity that issues payment cards or performs, facilitates, or supports issuing services including but not limited to issuing banks and issuing processors. Basically, the issuer is whoever the consumer gets the card from. Also referred to as “issuing bank” or “issuing financial institution”.

**Merchant** - For the purpose of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members (American Express, Discover, JCB, MasterCard or Visa) of the Payment Card Industry Security Standards Council (PCI SSC) 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
Internet Service Provider (ISP) is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers. In the case of UWM, this means accepting credit cards and **not** Purchasing cards. The merchants at UWM would be the unit with the unique ID number.

**Merchant Card Administration (BFS Accounting Procedure)** – document that lays out the detailed responsibilities of the involved departments/units with respect to merchant cards such as the merchant, the Controller’s office, UWM Information Security and Internal Audit.

**Merchant Identification Number (MID)** - The distinctive number assigned by the merchant account provider (i.e., US Bank) to a merchant. It is used to identify the merchant during authorization. Departments are prohibited from obtaining MID’s directly from credit card companies; they must be established through Controller’s office. Sometimes referred to as the Merchant Card.

**Network Segment** – network segmentation isolates system components that store, process, or transmit cardholder data from system 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.

**Open/Closed Merchant** – Status of merchant accounts, closed merchant ID’s should no longer be doing business.

**Payment Application Qualified Security Assessor (PA-QSA)** – Company approved by the Payment Card Industry Security Standards Council (PCI SSC) to conduct assessments on payment applications against the PA-DSS. These assessors are used only for purchased applications to check compliance. Their contracted relationship is with the actual application vendor and not UWM.

**Payment Card Industry Security Standards Council (PCI SSC)** – An open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. The PCI Security Standards Council’s mission is to enhance payment account data security by driving education and awareness of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

**Payment Gateways** - A means by which users of one computer service or network can access certain information on a different service or network. Examples of vendors that provide this service for UWM include TouchNet and Elavon.

**Phishing** – attempting to deceive a user to surrender confidential information by pretending to be a legitimate entity through electronic communication.

**PIN Entry Device (PED)** – A device for secure PIN entry and processing. It typically consists of a keypad with a display for user interface. It also has a distinct physical and logical boundary and a tamper resistant shell. A Hypercom device can be an example of a PED.
**Point of Sale (POS)** - Hardware and/or software used to process payment card transactions at merchant locations. POS sales are conducted most often through swipe terminals but are also completed with credit card imprimers or phone approvals.

**Qualified Security Assessor (QSA)** – An individual or company who is certified by the Payment Card Industry Security Standards Council (PCI SSC) to perform PCI DSS on-site assessments; they are often considered the most thorough and dependable way to prove compliance. UWM is contracted with Trustwave for purposes of consulting and limited scans, among other things.

**Self Assessment Questionnaire (SAQ)** – A tool used by an entity/merchant to validate its own compliance with PCI DSS. Depending on merchant level, the merchant may be required to complete this Attestation of Compliance. There are five different questionnaires--A, B, C-VT, C and D.

**Service Level Agreement (SLA)** – a document between the merchant and the UWM Controller’s Office that lays out the minimum criteria a merchant promises to meet in terms of the nature, quality and scope of the service.

**Service Provider** – Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of other merchant’s (Alumni Association, Foundation) cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data. For example, when UWM collects, transports and/or processes credit card transactions for the Foundation, UWM is a service provider to the Foundation.