APPENDIX A - DEFINITION OF TERMS

Acquirer - in an electronic money system, the entity or entities (typically banks) that hold deposit accounts for merchants and to which transaction data are transmitted.

Address Verification Service (AVS) - A fraud protection service created by Visa and MasterCard that checks a shopper's billing address against the card processor's existing address record for the shopper. AVS returns a code that indicates how well the addresses match.

Advanced Encryption Standard (AES) - The Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies.

Application Program Interface (API) – A particular set of rules and specifications that software programs can follow to communicate with each other. API serves as an interface between different software programs and facilitates their interaction.

Auditability - the degree to which transactions can be traced and audited through a system.

Audit Trail - a sequential record of events having occurred in a system.

Authentication - the process of proving the claimed identity of an individual user, machine, software component or any other entity.

Authorization - the process of determining what types of activities are permitted. Usually, authorization is in the context of authentication: once you have authenticated a user, they may be authorized different types of access or activity.

Automated Clearing House (ACH) - is a nationwide electronic funds transfer (EFT) system that provides for the inter-bank clearing of credit and debit transactions and for the exchange of information among participating financial institutions. It is a way of processing payment electronically like an eCheck (Electronic Check). NACHA is the organization responsible for developing the rules and the standards regarding ACH transactions.
Automated Teller Machine (ATM) - an electromechanical device that permits authorized users, typically using machine-readable plastic cards, to withdraw cash from their accounts and/or access other services, such as balance enquiries, transfer of funds or acceptance of deposits. ATMs may be operated either online with real-time access to an authorization database or offline.

Card Verification Value (CVV)/Card Verification Code (CVC): the three-digit security code on the signature strip of most credit and debit cards.

Chargeback - A chargeback is a request by the cardholder or the card-issuer to reverse a disputed purchase. Your acquiring bank may charge hefty fees for each chargeback.

Clearing - the process of transmitting, reconciling and, in some cases, confirming payment orders prior to settlement, possibly including netting of instructions and the establishment of final positions for settlement.

Clearing House - a central location or central processing mechanism through which financial institutions agree to exchange payment instructions. The institutions settle for items exchanged at a designated time based on the rules and procedures of the clearing house.

Clearing System - a set of procedures whereby financial institutions present and exchange data and/or documents relating to funds or securities transfers to other financial institutions.

Compliance – It is the act or state of confirming to the stipulated requirements. These regulations are designed (according to the Card Associations) to prevent fraud.

Cryptography - the principles, means, and methods for rendering information unintelligible and for restoring encrypted information to intelligible form (i.e., scrambling a message).

Digital Certification - a process to authenticate (or certify) a party’s digital signature; carried out by trusted third parties.
**Digital Signatures** - a mathematical encryption technique that associates a specific person with a given computer file and indicates that the file has not been altered since that person signed it.

**Distributed Transaction Processing** - application processing that involves multiple users requiring concurrent access to a single shared resource.

**E**

**Electronic Cash** - the digital equivalent of dollars and cents (also referred to as digital cash).

**Electronic Data Interchange (EDI)** - A computerized system that allows linked computers to conduct business transactions through a computer-to-computer exchange of standard business data according to agreed-upon data formats.

**Electronic Funds Transfer** - the method through which money is transferred between bank accounts, and also credit and debit card payments.

**Electronic Money** - monetary value measured in currency units stored in electronic form on an electronic device in the consumer’s possession. This electronic value can be purchased and held on the device until reduced through purchase or transfer.

**Encryption** - refer Cryptography.

**F**

**File Transfer Protocol (FTP)** - a standard way of transferring files from one computer to another on the Internet.

**Firewall** - a system or combination of hardware and software solutions that enforces a boundary between two or more networks technology and protects network resources from unauthorized access.

**G**

**Gateway** - a computer that performs protocol conversion between different types of networks or applications.
H 

Hacker - a computer operator who breaks into a computer without authorization, either for malicious reasons or just to prove it can be done.

I 

Issuer - in a stored value or similar prepaid electronic money system, the entity which receives payment in exchange for value distributed in the system and which is obligated to pay or redeem transactions or balances presented to it.

K 

Key - A secret value or code used in an encrypting algorithm known by one or both of the communicating parties.

L 

Logging - the storing of information about events that occurred on the firewall or network.

Loyalty Card - Any electronic card which is used only at a single Merchant's business for the purpose of earning discounts, free products and services, or rewards based on frequent buying.

M 

Merchant - Offers goods for sale in exchange for payment. When learning about payment processing, it's easiest to envision a merchant as shipping hard goods, but an online merchant may also provide services, or transmit "soft goods" like downloadable computer software or pay-per-view online content.

Middleware - facilitates the client/server connections over a network and allows client applications to access and update remote databases and mainframe files.

N 

Non-repudiable Transactions - transactions that cannot be denied after the fact.
P

Payment Application Data Security Standards (PA-DSS) – PA-DSS is the global security standard created by the Payment Card Industry Security Standards Council (PCI SSC).

Payment Card Industry Data Security Standards (PCI DSS) – PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

Personal Identification Number (PIN) - a sequence of digits used to verify the identity of a device holder.

Point of Sale (POS) - a system of terminals that debits or charges a customer’s account and credits or pays a merchant’s account to effect payment for purchases at retail establishments.

Processor (Payment Processing Network) - Connects online transaction processing software with the credit card / debit card / ACH networks, which then connect to merchant banks (acquiring banks) and customer banks (issuing banks).

R

Repudiation - the denial by one of the parties to a transaction of participation in all or part of that transaction or of the content of the communication.

Router - a computer system in a network that stores and forwards data packets between local area networks and wide area networks.

S

Secure Electronic Transaction (SET) - a set of standards jointly developed by Visa, MasterCard, and several technologies companies to facilitate secure credit card transactions over the Internet.

Secure Hypertext Transfer Protocol (SHTTP) - provides secure communication mechanisms between an HTTP client-server pair.
Secure Socket Layer (SSL) - a protocol for providing data security during transmission using data encryption, server authentication and message integrity.

Settlement - an act that discharges obligations with respect to funds or securities transfers between two or more parties.

Settlement system - a system used to facilitate the settlement of transfers of funds.

Smart Card - a card with a computer chip embedded, on which financial, health, educational, and security information can be stored and processed.

System Integrity - the quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent manipulation of the system.

Traceability - the degree to which transactions can be traced to the originator or recipient (also referred to as auditability).

Trusted Computer System - a system that employs sufficient assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information.

Trusted Third Party - a reputable entity that authenticates one or more parties to an electronic transaction. The authentication process generally involves the issuance and administration of digital certificates.

Virtual Private Network (VPN) – A mechanism for providing secure, reliable transport over the Internet. The VPN can be used to send any kind of network traffic securely.

Void – A void cancels a transaction that has been recorded for settlement, but has not been settled.

Vulnerability - a weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security.