CHAPTER NINE – SECURITY

SECTION 9.1 Compliance

Each Issuer and Acquirer is responsible for ensuring that it and each entity acting on its behalf complies with the requirements in this Chapter.

SECTION 9.2 General Issuer Requirements

Each Issuer shall comply with the following requirements for PIN management and security and shall ensure that each entity acting on its behalf complies with such requirements:

a. ***PIN Issuance.*** Each Issuer may designate the PIN for each Card or may permit Cardholder selection, as permitted under the Issuer Agreement, in either case in a secure and confidential manner. Each Issuer may reissue a Card with the same PIN only if it has reason to believe that the PIN has not been compromised. The Issuer shall not put any data on a Card from which it is possible to deduct the PIN without further knowledge of any cryptographic keys.

b. ***PIN Confidentiality.*** Each Issuer must ensure the confidentiality and security of the PIN during generation, issuance, storage, and verification.

c. ***PIN Verification***. Each CAS must verify the authenticity of each PIN communicated to it.

d. ***PIN Mailing.*** Each Issuer shall not mail a Card and PIN advice in the same envelope, nor shall it mail a Card and PIN so that both would likely be received on the same day.

e. ***Cardholder Education***. Each Issuer must advise Cardholders about the importance of the PIN, PIN security and Card security.

SECTION 9.3 General Acquirer and Merchant Requirements

Each Acquirer shall comply with the following requirements for PIN management and security and shall ensure that each entity acting on its behalf, including any Terminal Operator, complies with such requirements:

a. ***PIN Security.*** Each Acquirer shall ensure that ATMs and POS Terminals it owns, operates, controls or that accepts EBT Transactions by virtue of an agreement with such Acquirers, accept and securely encrypt PINs of 4 to 6 characters in length.

b. ***PIN Disclosure.*** Each Acquirer and Merchant must instruct its employees that they are prohibited from requesting the Cardholder to disclose their PIN.

c. ***PIN Encryption Translation and Key Management***. Each Acquirer must accept and translate encrypted PINs for interchange of Transactions. Each Acquirer must perform key management as described within this Chapter.

d. ***PIN Storage Requirements.*** PIN storage procedures must comply with Section 3.3 of ANSI Standard X9.8-1993. PINs may never be stored, except with respect to Store and Forward Transactions for the time necessary to submit such Transactions for Authorization. If stored, PINs must be encrypted under a unique PIN encryption key not used for any other purpose. Access to stored, encrypted PINs must be strictly controlled. *(Amended September 26, 2014)*

SECTION 9.4 PIN Entry

Each Acquirer must ensure compliance with the following security requirements for PIN entry at Terminals owned, operated or controlled by the Acquirer or for which the Acquirer is otherwise responsible under these Rules:

a. ***PIN Entry Order.*** The first digit entered to the PIN Pad shall be the high-order digit (far left). The last digit to be entered shall be low-order (far right). Each PIN Pad must accept PINs with a variable length of four (4) to six (6) digits.

b. ***Completion Function.*** Each ATM and POS Terminal must have both an enter key function in order to indicate the completion of a variable length PIN and a clear key or other function to allow the Cardholder to clear the PIN entry when an error has been made.

c. ***Non-Display of PIN.*** The value of the entered PIN must not be displayed in plain text or be disclosed by audible feedback. The clear text value of the entered PIN must never be printed, electronically recorded or written to software.

SECTION 9.5 Secure Cryptographic Devices

Each Acquirer must ensure that its systems and equipment, including systems and equipment owned or operated by a third party on behalf of the Acquirer, comply with each of the following security measures regarding secure cryptographic devices. All cryptographic functions must be performed in secure cryptographic devices in which all clear text keys and PINs are physically protected against disclosure and modification. In order for an ATM, POS Terminal, or PIN Pad to qualify as a secure cryptographic device, it must meet the criteria of Section 3.18. For a Host Security Module to qualify as a secure cryptographic device, it must meet the following criteria:

a. ***Encryption.*** The PIN must be encrypted using DES within the device.

b. ***Erasure.*** Penetration of the device must cause immediate erasure of all PINs, cryptographic keys and all useful residue of PINs and keys contained within the device.

SECTION 9.6 PIN Transmission Requirements

Each Issuer and Acquirer shall ensure that it and each entity acting on its behalf complies with the following security requirements for PIN transmission whenever the PIN is electronically transmitted outside of a secure cryptographic device:

a. ***Reversible Encryption.*** The PIN must be reversible encrypted using DEA.

b. ***Security Module.*** A hardware security module must be used to perform all PIN translations.

c. ***Unique Cryptographic Keys.*** All cryptographic keys relating to PIN security must be unique between each pair of communication zones of such keys; in their clear text form, these keys must reside solely within security modules and it must be impossible for any person to determine any such keys.

d. ***PIN in Unenciphered Mode.*** If the PIN is to occur in the unenciphered form in any node, it shall be in a secure cryptographic device. Each secure cryptographic device shall be uniquely identifiable at the interface with connected network zones up to the authorization system of the Issuer.

e. ***Recipherment.*** The Transaction PIN shall never be visible in the clear in the Acquirer central computing facility. In the event recipherment is necessary at this level, this function must be performed in a separate secure cryptographic device.

f. ***Dynamic Key Exchange.*** Dynamic exchange of keys is required between the first level connection and the Switch.

SECTION 9.7 Encrypted PIN Block Format

Each Issuer and Acquirer shall ensure compliance with the following security requirements for encrypted PIN block format.

a. ***Formation of PIN Block.*** The clear text PIN block and the PAN must be X'ORed together to form the standard ANSI PIN block as specified in ANSI Standard X9.8-1995. The ANSI PIN block format specifies the number, position, and function of bits within a 64-bit block used as input to the DEA algorithm operating in electronic code book (ECB) mode (i.e., 64 bits in, 64 bits out). The 64-bit output of the DEA algorithm is transmitted in its entirety.

b. ***Double-Length Key.*** It is recommended that a double-length (112 bits plus parity) key be used for PIN encryption, as follows:

(i) Encrypt the PIN block with the left half of the double-length key;

(ii) Decrypt this result with the right half of the double-length key; and

(iii) Encrypt this result using the left half of the double-length key.

c. ***Rejection of PIN Block.*** Any interchange node having access to the clear text PIN block must reject the encrypted PIN block if, during encryption, reformatting, re-encryption or PIN verification, any of the following conditions are found:

(i) control field is not 0000 (binary);

(ii) PIN length entered field value is less than 4 or greater than 12; or

(iii) a PIN digit has a value greater than 9.

d. ***PIN Block Key Change.*** The PIN block key must be changed between the first level connection and the CAS at least every 24 hours.

SECTION 9.8 Key Management

To ensure the highest level of key security, controls must exist to minimize the risk of cryptographic keys being compromised during creation, transmission, loading, storage, administration and destruction.

a. ***Key Creation Requirements.*** Each key and each key component must be generated by a random or pseudo-random process.

b. ***Zone Encryption.*** Where two organizations share a key to encrypt PINs communicated between them, that key must be unique to those two organizations and must not be given to any other organization. This technique of using keys unique for communication between organizations is referred to as zone encryption and is required under these Rules.

(i) ***Zones.*** A zone must start and terminate at a physically secure device. A zone begins at a device that encrypts the PIN in the zone's DES key(s) and continues through the communications facilities used to transmit the Transaction. A zone ends when the encrypted PIN is decrypted using the same DES key(s). The security of zone encryption, and the ability to change keys used within a zone without affecting other zones, is dependent upon using unique DES keys for each zone.

(ii) ***Unique ZCMK.*** Each pair of communicating organizations must have a unique zone control master key (ZCMK). All keys transmitted between the two organizations must be encrypted under this ZCMK. Such keys include unique PIN encryption keys, which are used to encrypt and decrypt PINs transmitted between the two organizations.

(iii) ***One Cryptographic Function.*** Each encryption key may be used for only one cryptographic function; however, a variant of a PIN encryption key may be used for a different cryptographic function from that of the original key.

(iv) ***Physically Secure Device.*** Each Participant which processes Transactions must use a physically secure device to translate encrypted PIN blocks and other encrypted data from one zone encryption key to another.

c. ***Protection of Keys from Disclosure.*** ny cryptographic key must only exist in the following forms:

(i) ***Encryption.*** Encrypted using a key-encrypting key.

(ii) ***Security of Devices.*** In a physically secure device.

(iii) ***Separation of Components.*** In clear form, in at least two (2) separate components, where each component must be protected under the techniques of split knowledge and dual control. The resulting key shall be a function of all key components. Key components shall be stored in such a way that unauthorized access has a high probability of being detected. Key components must never be in the physical possession of a person when that person is or ever has been similarly entrusted with any other component of the same key.

d. ***Access.*** No one person shall have the capability to access or ascertain any clear text secret key.

e. ***Detection of Secret Keys.*** The system shall prevent and detect:

(i) attempted disclosure of any secret key;

(ii) attempted use of a secret key for anything other than its intended purpose; and

(iii) unauthorized modification, substitution, deletion or insertion of any secret key.

f. ***Protection Against Key Substitution.***

(i) ***Substitution.*** Each Issuer and Acquirer must prevent the unauthorized substitution of one stored key for another, whether encrypted or unencrypted.

(ii) ***Alternative Measures.*** When it is not feasible to physically or cryptographically prevent the substitution of one encrypted stored key for another, (1) it should not be feasible to ascertain clear text and corresponding cipher text encrypted under the key-encryption key, and (2) if the compromise of any key is known or suspected, both the key in question and its key encryption key must be changed.

g. ***Limiting the Effects of a Key Compromise***. The following are required to prevent the compromise of the key or keys in one cryptographic device from compromising any other cryptographic device:

(i) ***Location of Keys.*** Any key-encrypting key, and any key used to encrypt a Transaction PIN in other than a PIN Pad, must be known only at two locations: the location where the key or PIN is encrypted and the location where it is decrypted.

(ii) ***Knowledge of Keys.*** Any key used to encrypt a Transaction PIN in a PIN Pad must be known only in that device and in security modules at the minimum number of facilities consistent with effective system operations. (This is to allow, for example, a POS Terminal to interface with more than one Acquirer.)

(iii) ***Key Value.*** No cryptographic keys other than those cryptographic keys used in conjunction with the operation of a Terminal by a Terminal Operator shall, except by chance, be equal to any other cryptographic key. Except by chance, the variant of a key, the irreversible transformation of a key, or keys encrypted under a key, knowledge of one cryptographic key must provide no information about any other cryptographic key.

(iv) ***Irreversible Transformation.*** The irreversible transformation of a key must be used only at the same level in a key hierarchy as the original key or the level immediately below that of the original key.

(v) ***Key Variant.*** A key shall be used for only one function. The variant of a key may be used only in those devices that possessed the original key. In a unique key per Transaction scheme, a single key may be used for different security functions in the same Transaction, provided it can be shown that no misuse is possible in a given implementation.

h. ***Key Replacement.*** A cryptographic key must be replaced with a new key whenever the compromise of the original key is known or suspected. The replacement key must not be a variant of the original key, nor an irreversible transformation of the original key. A compromised cryptographic key must be replaced with a new key within a reasonable time.

SECTION 9.9 Key Management Between Issuers, Acquirers and Merchants

Issuers, Acquirers and Merchants must use one of the following methods for changing keys and for establishing keys that are not encrypted under any other key:

a. ***Separation of Functions.*** Two or more trusted employees may each enter a key component into the ATM, POS Terminal or PIN Pad. The ATM, POS Terminal or PIN Pad generates the key, e.g., XORing the components. No one person shall have knowledge of more than one component. The key may be similarly entered into the Issuer's, Acquirer's or Merchant's security module or may be generated by the device and printed, as with a secure PIN mailer, for use by trusted employees.

b. ***Key Conveyance***. A physical secure key-transfer device may be used to convey keys from the Acquirer's or Merchant's security module to the receiving security module, ATM, POS Terminal or PIN Pad. The device is first electronically loaded with keys by connection to the generating security module. The device is then connected to the receiving security module, ATM, POS Terminal or PIN Pad and will electronically transfer one or more keys into the security module, ATM, POS Terminal or PIN Pad. No key may be displayed or otherwise disclosed during a transfer process. The key must be erased from the conveyance device immediately after transfer to a security module, ATM, POS Terminal or PIN Pad. Such a device must be loaded and unloaded under dual control to ensure that the device input or output is not tapped to disclose a transferred key.

c. ***Key Transfers.*** The Issuer's Acquirer's or Merchant's security module, or the security module of a Third Party Service Provider, may be used to directly and electronically transfer keys into ATMs, POS Terminals or PIN Pads. The above security requirements for key transfers to and from a key-transfer device apply to this "direct connect" technique as well. When a Third Party Service Provider's security module is used, information concerning the keys thus loaded must be conveyed to the receiving security module in such a way that this information cannot be compromised.

SECTION 9.10 Procedures

Each Participant, as applicable, shall implement appropriate procedures to prevent unauthorized personalization of security equipment, replacement of hardware or software, key generation and initial key loading. Each Issuer and Acquirer is responsible for maintaining up-to-date records regarding any Third Party Service Providers that manufacture or install secure cryptographic devices or load secure cryptographic devices with the initial keys.

SECTION 9.11 Separation

The security of processing Cards shall not be influenced or affected by the simultaneous processing of cards pertaining to other card schemes. In particular it shall be ensured that messages cannot be misrouted to any destination other than the intended one. To this end it is strongly recommended that only one party establishes a cryptographic key relationship with the PIN Pad so that when leaving a PIN Pad, an enciphered PIN is always routed to the same secure cryptographic device under control of the acquiring Network.

SECTION 9.12 Clearing and Reconciliation Data

If a Terminal has a removable storage medium and the data is not protected by encipherment, then only the minimum data necessary for clearing and reconciliation shall be stored. With the exception of the Card sequence number, sensitive data elements residing in the discretionary data field in Track 2, such as the CAV, shall not be recorded in the clearing and reconciliation data.

SECTION 9.13 Data Site Security

Each Issuer and Acquirer shall ensure that all data sites incorporate the following items into security procedures:

a. data sites shall be secured 24 hours, 365 days a year;

b. employee access to the data site shall be controlled by an electronic access system;

c. employee access to departments within the data site shall be controlled by the electronic access system;

d. guests, including vendors, shall be required to sign in and shall be assigned a temporary guest badge for identification;

e. guests, including vendor service personnel, shall be escorted at all times;

f. tapes, disks, and other storage media shall be kept in a secure access controlled environment when not being utilized by computer operations;

g. no storage media shall leave the data site without prior management authorization;

h. programming personnel, including contractors, shall be restricted from sensitive storage media unless prior management approval is obtained; and

i. sensitive output shall be shredded prior to disposal.

SECTION 9.14 System Access Control Software

Each Issuer and Acquirer shall ensure that system access control software is utilized and has the following capabilities:

a. all personnel requiring access to the system must be established within the system;

b. access to files, data bases, Transactions, programs and executable code shall be restricted to personnel with a job description need for access;

c. the system shall identify and verify individual access by the input of both a logon ID and password;

d. the system must support a "blind password" display to ensure password information is not obtained from a Terminal display screen;

e. data site procedures must be in place to ensure passwords are changed, at a minimum, every thirty (30) calendar days;

f. data site procedures must be in place to ensure old passwords are not reissued within three (3) password change cycles;

g. the system shall support a lock-out threshold if excessive invalid access attempts are input;

h. production personnel shall be restricted from accessing both the development systems and the test systems and associated data;

i. development personnel shall be restricted from accessing both the production systems and test systems and associated data; and

j. test personnel shall be restricted from accessing the development systems and the productions systems and associated data.

SECTION 9.15 Security Compliance Review

a. ***Participants Subject to a Security Compliance Review.*** Each Issuer, Acquirer, Processor, Network, or Third Party Service Provider that handles Transactions, PINs, encryption keys, or encryption hardware or software used for encryption must perform, at its own expense, a Security Compliance Review that is verified by a qualified internal or external auditor to ensure that such Participant is in compliance with the security provisions of these Rules. If a Security Compliance Review is being conducted by an internal auditor, the auditor must not have general responsibility for electronic funds transfers for the Participant. Each Issuer is responsible for conducting its own Security Compliance Review and ensuring that any Processor, Third Party Service Provider or Network with which it has an agreement under these Rules conducts a Security Compliance Review. Each Acquirer is responsible for conducting its own Security Compliance Review and for ensuring that any Processor or Third Party Service Provider (including ESSPs and Independent Sales Organizations) that handles Transactions, Cards, PINs, encryption keys, or encryption hardware or software and with which it has an agreement under these Rules conducts a Security Compliance Review. For purposes of the provisions in this Section, a Processor shall include a Merchant that drives its own Terminals.

b. ***Forms.*** For each Participant that completes a Security Compliance Review, an officer of the Participant who does not have operational responsibility related to the subjects covered in the Security Compliance Review shall complete and execute a Security Compliance Review either on the American Banker's Association (ABA) form "PIN Security Compliance Guideline or TG-3 or on a comparable security review form provided to a Network as a requirement for participation in such Network. For purposes of designation of eligible security review forms only, a "Network" includes one that has not entered an agreement to process Transactions. *(Amended January 9, 1998)*

c. ***Timing of Security Compliance Review***. Each new Participant described in paragraph (a) above shall complete a Security Compliance Review at least forty-five (45) calendar days prior to processing Transactions or handling PINs, encryption keys or encryption hardware or software. Thereafter, each such Participant shall complete a Security Compliance Review at least every third calendar year. An Issuer or NACHA may request that an Acquirer, Processor, Network or Third Party Service Provider complete a Security Compliance Review at an earlier date if there is cause to believe that such Participant is not in compliance with the security standards set forth in these Rules. NACHA or another Issuer may request that an Issuer complete a Security Compliance Review at an earlier date if there is cause to believe that such Issuer is not in compliance with the security standards set forth in these Rules. Any Security Compliance Review initiated in response to an identified security concern must be completed as soon as reasonably possible. At any time that a Participant subject to this Section makes a substantive change in its operations that affects security procedures, it must complete a new Security Compliance Review within forty-five (45) days of the change.

d. ***Security Compliance Certification Statements.*** Each Participant described in paragraph (a) above must complete a Security Compliance Review certification statement, as attached hereto in Appendix III or on a comparable form filed with a Network, each calendar year in which it does not complete a Security Compliance Review. A Security Compliance Review certification statement is a certification by an officer of the Participant that there has been no substantive change in the operations that are the subject of the Security Compliance Review since the last Security Compliance Review. *(Amended January 9, 1998)*

e. ***Security Exceptions and Record Retention.*** If the answer to any question on the Security Compliance Review form is other than "yes" (or otherwise indicates the Participant's inability to perform the security procedures pursuant to these Rules), the Participant shall, at its own expense, complete the Security Compliance Review Statement and Exception Form(s), as attached hereto in Appendix III (or comparable forms filed with a Network), which must be certified by its internal auditor or an outside auditor. Each Participant that is obligated to complete a Security Compliance Review Statement and Exception Form (or comparable form filed with a Network) must also indicate the date by which any security exception noted will be remedied, and shall file with the entity that received its original Security Compliance Review Statement and Exception Form (or comparable form filed with a Network) a certification of the removal of such exception promptly upon the completion of any corrective action. The work papers, files and other information compiled during the completion of the Security Compliance Review shall be maintained by each Participant, or its outside auditor, for a period of three (3) years from the submission date of the Security Compliance Review. *(Amended January 9, 1998)*

f. ***Filing of Forms***. Each Security Compliance Review form, Security Compliance Review certification statement and Security Compliance Review Statement and Exception Form (or comparable Network forms) completed by a Participant other than an Issuer or CAS shall be delivered to the Participant's choice of the Issuer for that Participant or a Network acting as Designated Agent for the Issuer. Each Issuer shall deliver to NACHA, or cause any Network acting as Designated Agent to deliver (i) the Security Compliance Review form, Security Compliance Review certification statement and Security Compliance Review Statement and Exception Form (or comparable Network forms) for itself and its CAS, and (ii) a listing of all Participants that have filed the above forms with it or its Designated Agents, including a separate listing of each Participant that has filed a Security Compliance Review Statement and Exception Form (or comparable Network form) and the dates by which the Participant has indicated that any security exceptions will be remedied.

g. ***Confidentiality of Forms***. NACHA and each Issuer and Network receiving Security Compliance Review forms, Security Compliance Review certification statements or Security Compliance Review Statement and Exception Forms (or comparable Network forms) shall treat such materials as strictly confidential and shall disclose such materials only to such persons as are reasonably required to evaluate such materials and address any security issues raised by such materials.

h. ***Network Security Procedures.*** These Rules are intended to accommodate and supplement Network security compliance review procedures, and do not in any way supersede such procedures. NACHA and each Network shall cooperate in utilizing such procedures to address security issues. A Network Security Compliance Review that is comparable to the Security Compliance Review under these Rules may be used to satisfy the requirements of this Section.