ACH Security Framework

On September 20, 2013, the ACH Security Framework Rule change was implemented. This rule establishes minimum data security obligations for ACH participants and is aimed at protecting the security and integrity of ACH data throughout its life cycle. A network participant could include a non-consumer Originator, Participating Depository Financial Institution (DFI), Third Party Service Provider &/or Third Party Sender.

The implementation of this rule includes three sets of rules:

- Protection of Sensitive Data and Access Controls
- Self-Assessment; and
- Verification of third-Party Senders and Originators

Protection of Sensitive Data and Access Controls

All participants in the ACH Network are required to establish, implement and regularly update their security policies, procedures and systems in order to:

- Protect the confidentiality and integrity of protected information
- Protect against anticipated threats or hazards to the security or integrity of protected information
- Protect against unauthorized use of protected information that could result in substantial harm to a natural person

Protected information is defined in the rule as the non-public personal information, including financial information, of a natural person used to create, or contained within, an Entry and any related Addenda Record. This not only covers financial information, but also includes sensitive non-financial information (such as health information) that may be incorporated into the Entry or any related Addenda Record.

Security policies and procedures of network participants must include controls on any system used to access and complete the ACH process of initiating, storing and processing these transactions.

Self-Assessment

Each participating DFI, Third-Party Service Provider and Third-Party Sender is required to verify that it has established, implemented and updated the data security policies, procedures and systems required by the Rule as part of their annual ACH Rules Compliance Audit.

Originators are bound to the NACHA Operating Rules through their origination agreement with their Originating Depository Financial Institution (ODFI). Therefore, each originator must attest that they have existing policies, procedures and systems in place to enable compliance with this ACH Security Framework.

Verification of Third Party Senders and Originators

This amendment establishes a requirement that an ODFI use commercially reasonable methods to determine the identity of each non-consumer Originator or Third-Party Sender with which the ODFI enters into an Origination Agreement, at the time the agreement is created.