Security Practices for Corporate ACH Originators

The *ACH Rules* requires Originators to establish, implement and (as appropriate) update security procedures relating to the initiation, processing and storage of entries.

Each Originator needs to evaluate its current security policies, procedures and systems to ensure the company identifies safeguards to protect ACH information (non-public information, including financial information of customers). This includes the collection of ACH information from customers, storage of authorizations, destruction of documents that include customers' banking information and access to non-public information about customers.
Security policies, procedure and systems must:

- Protect the confidentially and integrity of the protected information,
- Protect against anticipated threats or hazards to the security or integrity of protected information until its destruction and
- Protect against unauthorized use of protected information that could result in substantial harm to the customer.

If an Originator does not have up-to-date security policies, procedures and systems to ensure the company identifies safeguards for protected ACH information, they must be developed as soon as possible.

The following are security practices that can be implemented to reduce the risk of theft:

- Provide continuous communication and education to employees using online banking systems. Providing enhanced security awareness training will help ensure employees understand the security risks related to their duties.
- Update anti-virus and anti-malware programs frequently.
- Update, on a regular basis, all computers software to protect against new security vulnerabilities (patch management practices).
- Communicate to employees that passwords should be strong and shout NOT be stored on the computer used to access online banking.
- Adhere to dual control procedures.
- Use separate computers to originate and transmit ACH files.
- Transmit ACH files via a dedicated and isolated computer.
- Practice ongoing account monitoring and reconciliation.
- Adopt advanced security measures by working with IT staff or consultants.
- Utilize resources by trade organizations and agencies that specialize in assisting small businesses.