**ACH Security Framework Policies and Procedures Updates**

**ACH Policies**

It is *suggested* the financial institution consider adding the following language to the existing ACH Policyin regard to the Security Framework Rule which is effective September 20, 2013.

[***Financial Institution****] will implement and maintain security policies, procedures, and systems related to the initiation, processing and storage of Entries and resulting Protected Information.*

**ACH Procedures**

It is suggested the financial institution consider adding the following language to existing ACH Procedures in regard to the Security Framework Rule which is effective September 20, 2013

*[****Financial Institution****] will implement and maintain security policies, procedures, and systems related to the initiation, processing and storage of Entries and resulting Protected Information. The policies, procedures and systems will protect the confidentiality and integrity of Protected Information will protect against anticipated threats or hazards to the security or integrity of Protected Information, will protect against the unauthorized use of Protected Information, and will include controls on system access.*

*[****Describe policies, procedures and systems that have been implemented to protect Entries and Protected information during initiation, processing and storage. If this information is documented within other policies and procedures such as the Information Technology or Information Security Policies and Procedures indicate where they can be found.****]*

***Note: The definition of Protected Information not only covers financial information, but also includes sensitive non-financial information (such as non-financial account information contained in Addenda Records for bill payments) that may be incorporated into the Entry or any related Addenda Record.***

**ODFI/Originator Agreement**

It is suggested the financial institution consider adding the following or similar language to the existing ODFI/Originator Agreement in regard to the Security Framework Rule which is effective September 20, 2013.

[***Originator/Third-Party Sender Name****]**will ensure that the Originator/Third-Party Sender and any Third-Party Service Provider acting on behalf of the Originator/Third-Party Sender will implement and maintain security policies, procedures and systems related to the initiation, processing and storage of Entries and resulting Protected Information.*

*[****Originator/Third-Party Sender Name****] will implement and maintain security policies, procedures, and systems related to the initiation, processing and storage of Entries and resulting Protected Information. The policies, procedures and systems will protect the confidentiality and integrity of Protected Information will protect against anticipated threats or hazards to the security or integrity of Protected Information, will protect against the unauthorized use of Protected Information, and will include controls on system access. [****Originator/Third-Party Sender Name****] will ensure that the Originator and any Third-Party Service Provider acting on behalf of the financial institution or Originator will implement and maintain security policies, procedures and systems related to the initiation, processing and storage of Entries and resulting Protected Information.*

*[****Describe policies, procedures and systems that have been implemented to protect Entries and Protected information during initiation, processing and storage. If this information is documented within other policies and procedures such as the Information Technology or Information Security Policies and Procedures indicate where they can be found.****]*

***Note: The definition of Protected Information not only covers financial information, but also includes sensitive non-financial information (such as non-financial account information contained in Addenda Records for bill payments) that may be incorporated into the Entry or any related Addenda Record.***