May 25, 2012

NACHA: ACH Security Framework

Executive Summary

- NACHA – The Electronic Payments Association has issued a proposal regarding the Automated Clearing House (ACH) security framework. The proposal is related to the earlier request for information from February 2011.
- Specifically, the proposal aims to improve the security and integrity of certain ACH data in the following areas: 1) Protection of Sensitive Data and Access Controls; 2) Annual Self-Assessment; and 3) ODFI Verification of All Third-Party Senders and Originators.
- CUNA is interested in the impact of the proposal on your credit union's risk management and ACH compliance procedures. Comments on the proposal are due to the NACHA by June 22; **please submit your comments to CUNA by June 11, 2012.** Please e-mail your comments or questions to CUNA Regulatory Counsel Dennis Tsang at dtsang@cuna.com.
- The proposal covers:
    1. **Protection of Sensitive Data and Access Controls -** The proposal would require a Receiving Depository Financial Institution (RDFI), Originating Depository Financial Institution (ODFI), non-Consumer Originator, Third-Party Provider, or Third-Party Sender to comply with these ACH security requirements on the handling and storage of "protected information" to: 1) protect the confidentiality and integrity of "protected information" until its destruction; 2) protect against anticipated threats or hazards to the security or integrity of "protected information"; and 3) protect against unauthorized use of "protected information" that could result in substantial harm to a natural person. NACHA believes the proposal addresses these requirements in a general way, to allow flexibility for each covered entity to determine how to satisfy these requirements based on its business needs and its regulatory compliance obligations.
        - Access controls must be included in these policies, procedures, and systems that process ACH transactions.
        - The proposed definition of "protected information" is the "non-public personal information, including financial information, of a

natural person used to create, or contained within, an ACH entry and any related Addenda Record."
    - NACHA believes these proposed requirements are consistent with other data security obligations, such as the Gramm-Leach Bliley Act, which applies to financial institutions.
    - These requirements would not apply directly to consumers, but would apply to entities that originate CIE entries for consumers.

2. **Annual Self-Assessment** – The proposal would require that a RDFI, ODFI, Third-Party Service Provider, or Third-Party Sender must verify, as part of its annual ACH Rules Compliance Audit, that it has established, implemented, and updated data security policies, procedures, and systems to comply with the proposed security requirements.

3. **ODFI Verification of All Third-Party Senders and Originators** – The proposal would require an ODFI to use a commercially reasonable method to verify the identity of all Originators/Third-Party Senders, regardless of the manner in which the origination agreement was executed. Currently, this ODFI verification requirement only applies to Originators or Third-Party Senders that enter into an origination agreement via an unsecured electronic network.

- The proposed effective date is September 20, 2013.
- For further details, please refer to the NACHA executive summary of the executive summary of the proposed changes, the proposed modifications to the NACHA Operating Rules, and the NACHA survey on the proposal. If you are contacting NACHA directly, please also send us a copy of your comments to ensure that we incorporate your feedback.

Questions to Consider Regarding the Proposal

1. Does your credit union support the proposed ACH security requirements regarding the protection of sensitive data and access controls? Do you have any concerns, such as with compliance costs, the overlap between existing data security requirements, including the Gramm-Leach Bliley Act, or the scope of the proposed security requirements?

   _____

2. Do you agree with the proposed definition of "protected information"?

   _____

3. Does your credit union support incorporating verification of the proposed ACH security requirements as part of the annual ACH Rules Compliance Audit?

   _____

4. Does your credit union support the proposed ODFI verification of the identity of all Third-Party Senders and Originators?

   _____

5. Does the proposed effective date of September 20, 2013 provide sufficient time to implement the proposed ACH security changes?

   _____

6. Any other comments or suggestions regarding the proposal?

   _____

7. Thank you very much for your time and comments.