American Bankers Association
Building Success. Together.

Stephen Kenneally
Vice President
Center for Regulatory Compliance
Phone: 202-663-5147
E-mail: skenneal@aba.com

By electronic delivery
Mbondoc@nacha.org

June 22, 2012

Maribel Bondoc
Manager, Network Rules
NACHA,The Electronic Payments Association
13450 Sunrise Valley Drive
Herndon, VA 20171

Re: ACH Security Framework, Request for Comment

Dear Ms. Bondoc,

The American Bankers Association (ABA)[1] respectfully submits its comments to NACHA, The Electronic Payments Association, on the Request for Comment on the proposed ACH Security Framework published on May 8, 2012. The RFC describes a set of proposed rules that would improve the security and integrity of information associated with ACH transactions. Banks already meet the standards prescribed in this RFC under other rules and regulations issued by federal and state banking regulators. It is important for other non-bank participants in the ACH network to make changes to meet these requirements while not burdening banks with unneeded duplicative or overlapping rules. The true value of this proposal is not in requiring that banks comply with yet another set of rules; it is in raising the security requirements for the non-banks in the system to match the requirements already imposed on banks.

This RFC is more limited in scope than outlined in the related Request for Information (RFI) issued in 2011. ABA applauds this more focused approach that eliminates the proposal to verify the identification of ACH receivers and mandates for bank fraud management systems.

It is very important to recognize that banks are already meeting the requirements outlined in this Security Framework proposal. Banks want to improve ACH security across the network but do not want to expend resources solely on a "compliance exercise." Demonstrating bank compliance with the NACHA requirements through compliance with existing federal and state banking regulations should not be onerous. NACHA should clarify in any final rule and any associated guidance that banks are allowed to verify compliance with the ACH rule by demonstrating compliance with any federal or state regulation that has effectively the same requirements. Banks should be allowed to focus effort and resources on protecting consumer data instead of being

[1] The American Bankers Association represents banks of all sizes and charters and is the voice for the nation's $14 trillion banking industry and its 2 million employees. ABA's extensive resources enhance the success of the nation's banks and strengthen America's economy and communities. Learn more at www.aba.com.

subject to a duplicative process of proving compliance with a redundant set of rules and regulations.

Protection of Sensitive Data and Access Controls

The proposed rule would require that all non-Consumer Originators, Participating Depository Financial Institutions (DFIs), Third-Party Service Providers, and Third-Party Senders comply with specific security requirements regarding the handling and storing of Protected Information. These parties will be required to establish, implement, and update security policies as appropriate. Protected information is defined 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." ABA believes these standards are already encompassed within existing regulatory requirements applied to insured depository institutions and the service providers they employ.

The RFC improves upon the RFI in several respects. First, it does not prescribe its own set of specific requirements for the destruction of Protected Information. Second, it does not include its own set of specific requirements for each participant's security policies and procedures. Third, it does not include the unnecessary standard of "commercially reasonable" controls to be established for access controls. Rather than micromanage these information security components, the RFC accommodates the more flexible approach endorsed by the current regulatory expectations.

ABA favors all of these changes to the RFI. Banks participating in the ACH network meet these requirements under a number of different banking regulations. Requiring these requirements in a NACHA Operating Rule would increase the amount of time and money needed to validate compliance without improving customer security. It should be made clear in any final rule issued by NACHA that banks complying with federal or state banking regulations that parallel the NACHA requirements shall be considered in compliance with the NACHA rules. This is intended to avoid unnecessary costs associated with banks complying with overlapping rule sets and demonstrating that compliance using different reporting models.

Self-Assessment

The RFC would require that each participating DFI, Third-Party Service Provider, and Third Party Sender verify, as part of its annual ACH Rules Compliance Audit, that it had established, implemented, and updated its policies and procedures as required by this security requirements rules. This is a marked and welcome change from the RFI's stance that would have established a separate self-assessment process independent of the annual compliance requirements.

ABA favors the changes made to the Self-Assessment requirements. Banks are already meeting these goals, and the revised rules would not unduly burden them to prove compliance. Requiring non-banks to meet the same requirements will benefit all ACH network participants.

Verification of Third-Party Senders and Originators

This proposal would require that Originating Depositary Financial Institutions (ODFIs) verify the identity of all Originators and Third-Party Senders using commercially

reasonable methods. This section of the proposal is unchanged from the original language found in the RFI.

ABA requests that the rule clarify that this verification process would be required when the Third-Party Senders and the Originators begin their relationship with the bank and not each time a payment file is passed on to the bank.

ABA favors this section of the proposal as commonsense and one that banks acting as ODFIs are already pursuing.

ABA favors covering natural persons only with this requirement to keep it consistent with existing rules and regulations protecting consumer information.

Conclusion

As noted previously, ABA looks favorably on this streamlined ACH Security Framework as long as there is no undue additional compliance burden placed on banks that already meet these same expectations under federal and state regulations. When a final rule is published, there must be clear guidance that compliance with federal and state rules that are consistent with NACHA's rules means compliance with NACHA rules. Banks should be focusing on protecting sensitive information and not worrying about "examination creep." Non-banks should be required to meet the same standards of protection.

ABA appreciates the opportunity to comment on the Security Framework RFC. If you have any questions about these comments, please contact the undersigned at 202-662-5147.

Respectfully submitted,

Stephen K. Kenneally
Vice President
Center for Regulatory Compliance