American Bankers Association
Building Success. Together.

Stephen Kenneally
Vice President
Center for Payments and Cybersecurity Policy
Phone: 202-663-5147
E-mail: skenneal@aba.com

August 4, 2017

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

Re: Request for Information on Account Information Security

Dear Ms. Bondoc:

The American Bankers Association[1] (ABA) respectfully submits its comments to NACHA, the Electronic Payments Association (NACHA) on the Account Information Security Request for Information (RFI) published on June 26, 2017. The opportunity to review and comment on NACHA's initial discussion of the topic is most welcome.

The RFI outlines three areas where new rules may help to increase the security of ACH data being stored by Originators or Third Parties. We appreciate the effort behind NACHA's research into data security and tokenization that has led to this RFI. Banks must continually review their data security practices to minimize any risk of customer information being compromised.

Protecting customer data is paramount for banks. However, it is imperative that it be accomplished in an efficient and effective manner where the benefits outweigh the associated expenses. At this point, we believe that the concepts provided for discussion need to be refined and clarified to enable a thorough examination to determine if they make the most economic sense.

The RFI cites research conducted by NACHA that total fraud losses related to breached ACH data are approximately $20 million per year across the industry, representing only about 1% of all Demand Deposit Account (DDA) fraud losses. While there is no "acceptable" amount of fraud, this is very low. The same research also indicates that tokenizing all customer ACH data would cost $80 to $240 million annually. Clearly, mass tokenization is not the answer.

The low loss rates associated with ACH can be attributed to the security procedures currently in place to protect data and the difficulty of using fraudulently obtained account

[1] The ABA 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.

numbers after a breach. Debiting funds from a compromised account requires that a perpetrator establish an account at a financial institution. Further due diligence is conducted by financial institutions of any customer seeking to become an Originator because the Originating Depository Financial Institutions (ODFI) that initiates the transaction warrantees that it is valid and authorized. Finally, ACH debits are monitored to determine if there is an unusual number of returns for reasons like bad account numbers or unauthorized transactions. These are tip offs that an Originator should be subject to more scrutiny and a key part of the layered security apparatus that keeps ACH fraud so low.

The first concept asks for comment on a potential change to the ACH Security Framework to require that large ACH Originators and Third Parties protect ACH information through encryption, masking or removal or replacement of data held at rest.

We would like to note that ODFIs and many Originators that hold ACH data at rest already take extensive protective measures regarding ACH data, including encryption. This fact is verified by the very low total of breach related losses identified by NACHA. Any potential enhancements to this data security must be justifiable on a cost basis.

The RFI asks for input regarding any potential new rule applying towards large Originators and Third Parties and ABA agrees that would be the most effective approach since relatively few of these entities are responsible for a large proportion of ACH transactions. As the largest ACH Originator, it would be essential for the U.S. Treasury Department to be supportive any future rules. However, as we will repeat often in this response, the ACH fraud loss rate is low and any recommendations to further protect the data must reflect common sense when it comes to the cost of any marginal improvement that is gained.

If there is an increasing threat of ACH fraud, approaching the largest Originators and Third Parties makes sense as part of the initial plan, but this is complicated by the fact that many of these entities already have instituted data security restrictions. Any new requirement must recognize the need for flexibility terms of how data is protected. There should also be a recognition that if there is an increasing threat of ACH fraud, then eventually it will find its way to smaller entities and that data will also need to be protected. NACHA should ensure that any data security enhancements be adopted with the understanding that smaller parties will be hit with disproportionate costs due to the smaller volume of transactions that they process.

The second area under discussion asks for an indication of interest in creating a new Standard Entry Class Code "Compromise Notification Entry" that would allow ODFIs to notify Receiving Depository Financial Institutions (RDFIs) that their customer account information has been breached.

ABA does not believe that there will be any significant benefit to be gained from creating this new entry code. As noted in the RFI, the total cost associated with ACH data breaches is $20 million per year. The costs associated with creating and maintaining the new entry code and managing these notifications outweighs any potential benefit that could be

gained. NACHA's research indicates that even if ACH data is breached, it is difficult for it to be accessed because the fraudster must have a relationship with an ODFI that has approved it as an Originator. ODFIs are responsible for the entries that they introduce to the network and they are careful about who they do this for because they are responsible for any losses to RDFIs for unauthorized transactions. This system works well as it exists.

The third area under consideration seeks input on how to identify and remove barriers preventing RDFIs from using the Notification of Change (NOC) process to send substitute account numbers or tokens to ODFIs. Currently, NOCs are used by RDFIs to provide ODFIs with corrected or updated account information. ODFIs are required to update their records with the new account information.

ABA believes that this concept could be adopted without any additional rule changes. If an RDFI sends a NOC with updated account information then RDFIs are obligated to use that new data. Whether it is a new account number or a token associated with an account number should make no difference.

There could be related customer service difficulties if the new tokenized account number is different than the one the customer authorized. Educating customers of any new protocol such as this should fall on the RDFI that is altering the ACH data.

ABA would like to thank NACHA for the opportunity of responding to the RFI on Account Information Security. If you have any questions about these comments, please contact the undersigned at (202) 663-5147.

Sincerely,

Stephen K. Kenneally
Vice President
Center for Payment and Cybersecurity Policy