



Credit Union National Association

cuna.org

601 Pennsylvania Ave., NW | South Building, Suite 600 | Washington, DC 20004-2601 | PHONE: 202-638-5777 | FAX: 202-638-7734

March 25, 2011

Maribel Bondoc
Manager, Network Rules
NACHA – The Electronic Payments Association
13450 Sunrise Valley Drive, Suite 100
Herndon, VA 20171

Submitted via email: mbondoc@nacha.org

Re: ACH Security Framework

Dear Ms. Bondoc,

This comment letter represents the views of the Credit Union National Association (CUNA) regarding NACHA's Request for Information on a proposed framework to provide additional security for sensitive ACH data. By way of background, CUNA is the largest credit union advocacy organization in this country, representing approximately 90% of our nation's 7,600 state and federal credit unions, which serve 93 million members.

CUNA appreciates NACHA's efforts to improve the security and integrity of the ACH network. However, while we generally agree with NACHA's objective to improve the security and integrity of sensitive ACH data, we have concerns about additional compliance burdens and overlap with other data security regulations, and offer recommendations for NACHA's consideration to improve the proposed framework.

Under the proposed sensitive ACH data framework, originating depository financial institutions (ODFIs), non-consumer Originators, and third-party service providers for ODFIs would generally be required to:

- Protect sensitive ACH data (e.g., social security numbers, account numbers);
- Deploy "commercially reasonable" access controls;
- Assess ACH data security with an annual self-assessment;
- Identify third-party Senders and Originators; and
- Verify the Receiver's identity.

We agree that a sensitive ACH data security framework should provide consistent standards for all participants in the ACH network. The security framework should apply to Originators and third-party service providers for



OFFICES: | WASHINGTON, D.C. | MADISON, WISCONSIN

ODFIs because ACH data must be secure at origination and throughout the transaction.

Further, we support “commercially reasonable” standards which provide flexibility for the evolving data security landscape, accommodate the unique business needs for credit unions and other ACH participants, and minimize compliance costs.

A top concern is the annual self-assessment. We believe that ODFIs should not be required to complete a separate, annual self-assessment for only sensitive ACH data. Instead, we recommend that ODFIs could assess their sensitive ACH data as part of an existing compliance requirement for overall ACH risk management, such as NACHA’s ACH risk assessment.

Also, we urge NACHA to minimize the compliance burdens and costs to all credit unions that will be affected by this proposal. The proposed sensitive ACH data security framework should be consistent with and minimize overlap regarding other relevant requirements, such as due diligence obligations and other responsibilities imposed by the National Credit Union Administration (NCUA), Federal Reserve Board, and the Federal Financial Institutions Examination Council (FFIEC). NACHA should not impose additional ACH security requirements, unless the improvements in fraud and security are greater than the increased compliance costs.

The proposed framework should not impose additional requirements for receiving depository financial institutions (RDFIs) because RDFIs do not generally receive sensitive ACH data. We urge NACHA to assess and minimize any impact to RDFIs, especially for smaller credit unions.

Finally, the proposed sensitive ACH data framework should be flexible enough to accommodate technology changes and regulatory developments, such as the expected FFIEC guidance on internet and mobile authentication.

Thank you for the opportunity to comment on this proposal. If you have any questions about our letter, please feel free to contact me at (202) 508-6733.

Sincerely,

A handwritten signature in blue ink that reads "Dennis Tsang". The signature is fluid and cursive, with the first name "Dennis" and last name "Tsang" clearly legible.

Dennis Tsang
Regulatory Counsel