

By electronic delivery
Mbondoc@nacha.org

March 25, 2011

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

Re: Request for Information: ACH Security Framework, February 7, 2011

Dear Ms. Bondoc:

The American Bankers Association (ABA)¹ respectfully submits its comments to NACHA, The Electronic Payments Association, on the Request for Information: ACH Security Framework (RFI) published on February 7, 2011. The RFI requests industry feedback on a proposed ACH Security Framework intended to enhance the security and integrity of sensitive ACH data. It would also require the authentication of certain parties to ACH transactions. The industry was asked to provide input on the RFI to assist NACHA develop a formal Request for Comment proposal on a new ACH Security Framework (proposed Framework) later in 2011.

The proposal's intent is to reduce the risk to all ACH Network participants against unauthorized access to ACH data and to secure those data throughout their lifecycle, with special attention paid to authenticating ACH participants that originate transactions.

The ACH system and related bank information technology systems are subject to increasing threats from hacking, fraud, viruses, and most prominently corporate account takeovers. Corporate account takeovers occur when a bank customer, usually a commercial customer, has his or her online banking credentials compromised. This enables criminals who have that information to initiate payments to their own bank

¹ The American Bankers Association represents banks of all sizes and charters and is the voice for the nation's \$13 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.

accounts or to their affiliated “money mules” assigned to receive the initial transfer, then forward the funds for the ultimate benefit of the fraudster. A major hurdle in preventing corporate account takeover is that the data breach does not usually happen at the bank; it happens at the customer site, where the bank has little direct control of security. ABA shares the underlying concern that motivates the proposed Framework to provide enhanced security for sensitive information to combat threats better, such as corporate account takeover. As NACHA’s RFI notes at several points, depository institutions are in compliance with existing standards and make every effort to keep pace with or ahead of developments. In addition, ABA’s bankers acting as Originating Depository Financial Institutions (ODFIs) take seriously their responsibilities as gatekeepers to the ACH system and have every incentive to establish and maintain a system to ensure that its clients, the Non-Consumer Originators and Third-Party Senders, are complying with all applicable rules and regulations. Layering more prescriptive standards on the existing obligations will increase costs without resulting in appreciable benefits.

Accordingly, we believe that the problem is not primarily one of too few rules but inconsistent vigilance by a small segment of ACH participants. Although the proposed Framework may provide a principles-based approach to security risk management, translating those principles to a set of requirements will only add redundancy to existing regulatory mandates and increase the burden on financial institutions, as they would have to document the compliance of their security policies and procedures with their own regulators as well as with new NACHA rules.

Moreover, ABA sees more hazard than help in having the proposed Framework attempt to define the term “commercially reasonable.” Given the litigation surrounding that term in several court cases dealing with corporate account takeover, we are reluctant at this time to interfere with a standard that has developed as a community or market based concept that varies with the context in which it arises.

Fundamentally, ABA believes that NACHA’s proposal as currently structured is premature, and to the extent it focuses on generating rules, miss-directed. While we appreciate the intent of the RFI to explore the need and manner by which the security of the ACH network can be enhanced, we believe that it is appropriate for a banker led group to review the challenges faced by the ACH network, the existing regulatory requirements, and the safeguards that banks have already put into place to determine the best way to improve security without causing undue hardship on financial institutions. By way of example, one less prescriptive option would be for NACHA to consider how it can leverage its expertise by providing tools or education resources to assist non-Consumer Originators and Third-Party Service Providers to recognize and redress vulnerabilities in their controls, conduct more effective risk assessments of their practices, and better tailor monitoring to achieve a dynamic response to evolving security risks.

In summary, we encourage NACHA to stand down on pursuing the application of additional or redundant rules and instead conduct more discussion among financial institutions and other system participants about alternatives to tackling the account

takeover problem. ABA offers to provide both staff and member input to such a more in-depth working group endeavor. If you have any questions about these comments, please contact Stephen Kenneally at 202.663.5147 or via email at skenneally@aba.com.

Respectfully submitted,

A handwritten signature in black ink that reads "Stephen K. Kenneally". The signature is written in a cursive style with a large, stylized 'S' and 'K'.

Stephen K. Kenneally
Vice President
Center for Regulatory Compliance