

BITS

FINANCIAL SERVICES
R O U N D T A B L E

Submitted electronically

March 25, 2011

Maribel Bondoc
Manager, Network Rules
NACHA
mbondoc@nacha.org

Attention: NACHA Request for Information on proposed ACH Security Framework

BITS¹ appreciates the opportunity to comment on the NACHA proposed ACH Security Framework. We understand the inherent value of the ACH network and NACHA's efforts to promote techniques for security and integrity of data.

Specifically, we appreciate the efforts of NACHA to provide a technique for data protection in the ACH network at a time when fraud using compromised account data is a regular occurrence. If the online environment moves toward a dynamic data architecture for heightened security capabilities, other payment applications may be more vulnerable to security issues. The proposed Framework is an important strategic step by NACHA to prepare the network for the necessary heightened security.

Our members employ a number of controls within their payments processing environments. The exact combination of controls differs based upon institution, transaction type, and risk level. While the way specific controls are used may differ among institutions, at a high level the controls outlined in the Framework by NACHA (e.g., authentication, encryption, system monitoring, etc.) are used throughout the industry to control access to sensitive data.

“Commercially Reasonable” Standards

We appreciate the desire for NACHA to rely on a “commercially reasonable” standard for the protection of sensitive ACH data. This approach allows for at least annual updates without going through a cumbersome rules update process.

¹ BITS is the technology policy division of The Financial Services Roundtable, created to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. BITS focuses on strategic issues where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services by leveraging intellectual capital to address emerging issues at the intersection of financial services, operations and technology. BITS' efforts involve representatives from throughout our member institutions, including CEOs, CIOs, CISOs, and fraud, compliance, and vendor management specialists. For more information, go to <http://www.bits.org/>.

While the use of a “commercially reasonable” standard allows for the flexibility of the NACHA Rules to adapt more quickly to the availability of techniques, it may also significantly reduce NACHA’s enforcement ability. Any illustrations that NACHA cites in the Operating Guidelines or elsewhere are examples only and do not carry the force of a rule.

We recommend NACHA form a Rules work group to provide more specificity on commercially reasonable standards to the NACHA Board or an alternate entity suited to this purpose. This delegated mechanism, supplemented with robust opportunity for member input to annual updates, will provide needed specificity for network participants and will add to the overall security of the network.

Requirements for Business Versus Retail Accounts

Institutions differentiate between business and retail accounts for a variety of reasons, but most importantly in their risk calculations. Given the unique purposes of each account, institutions evaluate them separately, as their risk exposure varies greatly.

We believe that NACHA should recognize the difference in these account types and clearly differentiate the responsibilities to provide “commercially reasonable” standards.

Self Assessment

We agree with the requirement for Originating Depository Financial Institutions (ODFIs) and ODFIs’ Third-Parties to complete an annual self assessment of protected ACH sensitive data.

Currently, some ODFIs report having difficulty receiving the necessary annual security related information from non-consumer originators (e.g., business clients). By requiring self assessments, NACHA will significantly increase the ability of ODFIs to receive the necessary information from these reticent originators and will materially improve ODFIs’ ongoing due diligence ability.

Protection of Sensitive ACH Data

The Framework operates under a premise that the protection of data relating to a financial institution’s own customers is adequately addressed by significant legislative and regulatory requirements. Based on that premise, the Framework does not propose to cover a Receiving Depository Financial Institutions’ (RDFI) protection of its own customers’ ACH data.

We have reservations about this proposed limited scope of protection. The NACHA Operating Rules presently have a number of rules duplicating federal regulations². NACHA should not, therefore, abandon regulating a subject merely because a federal regulation provides a requirement.

We believe that augmenting legislative or regulatory requirements with requirements under the Operating Rules strengthens the regulation and enforcement of important subjects, such as protection of data. By including provisions within the Operating Rules mandating the protection of ACH data by an RDFI, we will bolster the sound policy of generally safeguarding such data.

² Subsection 2.5.10.2 of the Operating Rules, an Originator may secure the authorization of a Receiver for a POP entry by providing a certain notice to the Receiver to authorize the Originator to initiate a POP entry. This mandated notice under the Operating Rules tracks the mandated notice required under Regulation E § 205.3(b)(2)(iii) and Regulation E, Appendix A, A-6-Model Clauses for Authorizing One-Time Electronic Fund Transfers Using Information from a Check (§ 205.3(b)(2)).

NACHA does not need to expand the scope of such legislative or regulatory coverage, instead NACHA should recognize in their Rules the other responsibilities of RDFIs. This acknowledgement will provide additional focus and emphasize the importance of compliance responsibilities for RDFIs.

Overall Network Security

We recognize and appreciate the efforts of NACHA to develop the ACH Security Framework. We believe it is important to remember, however, that this Framework only addresses a part of the ACH payment ecosystem. In addition to this Framework, we strongly suggest NACHA develop additional frameworks to assess and evaluate other critical components of the ecosystem including the ACH network operators. This will help ensure overall security and recognize the need to protect all network users from ACH fraud. In addition, we believe this further effort is necessary.

Only when the users and the network are required to acknowledge and secure the transactions will we be able to more successfully secure data in the ACH network.

Thank you for your consideration of our comments. If you have further questions or comments on this matter, please feel free to contact me at 202-589-2440 or Leigh@fsround.org, or William Henley, BITS Senior Vice President for Regulation at 202-589-2402 or William@fsround.org.

Sincerely,

A handwritten signature in black ink, appearing to read "Leigh Williams". The signature is fluid and cursive, with a long, sweeping tail on the final letter.

Leigh Williams
President