ACH Security Framework

The ACH Security Framework amendment creates a framework within the NACHA *Operating Rules & Guidelines book* aimed at protecting the security and integrity of certain ACH data throughout its lifecycle. The Security Framework establishes minimum data security obligations for companies and Third Party Providers to protect ACH data within their purview.

The changes to the *NACHA Operating Rules* & Guidelines book related to the ACH Security Framework provisions are noted below.

Article One, Subsection 1.2.2 (Audits of Rules Compliance) – modified to correct language related to Third-Party Senders for consistency throughout the Rules.

SUBSECTION 1.2.2 Audits of Rules Compliance

A Participating DFI must annually conduct, or have conducted, an audit of its compliance with these Rules in accordance with Appendix Eight (Rule Compliance Audit Requirements). A Third- Party Service Provider or a Third-Party Sender that has agreed with a Participating DFI to process Entries must annually conduct, or have conducted, an audit of its compliance with these Rules in accordance with Appendix Eight (Rule Compliance Audit Requirements).

Article One, Subsection 1.6 (Security Requirements) – new subsection incorporates general ACH Security Requirements into the NACHA Operating Rules.

SECTION 1.6 Security Requirements (became a rule in 2014)

Each Non-Consumer Originator, Participating DFI, and Third-Party Service Provider must establish, implement, and update, as appropriate, policies, procedures, and systems with respect to the initiation, processing, and storage of Entries that are designed to:

(a) Protect the confidentiality and integrity of Protected Information until its destruction;

(b) Protect against anticipated threats or hazards to the security or integrity of Protected Information until its destruction; and

(c) Protect against unauthorized use of Protected Information that could result in substantial harm to a natural person.

Such policies, procedures, and systems must include controls that comply with applicable regulatory guidelines on access to all systems used by such Non-Consumer Originator, Participating DFI, or Third-Party Service Provider to initiate, process, and store Entries.

Article Two, Subsection 2.2.1 (ODFI Verification of Originator or Third-Party Sender Identity) – new subsection creates an obligation for the ODFI to use a commercially reasonable method to establish the identity of each Originator or Third-Party Sender.

SECTION 2.2 Prerequisites to Origination

An ODFI must perform, or ensure that an Originator or Third-Party Sender performs, each of the following before permitting the Originator or Third-Party Sender to originate any Entry:

SUBSECTION 2.2.1 ODFI Verification of Originator or Third-Party Sender Identity

The ODFI must utilize a commercially reasonable method to verify the identity of an Originator or Third-Party Sender at the time the ODFI enters into an Origination Agreement with the Originator or Third-Party Sender.

Article Two, Subsection 2.4.1.8 (ODFI has Verified the Identity of Originator or Third- Party Sender That Uses an Unsecured Electronic Network Dishonor of Return by ODFI) – this subsection is removed from the Rules.

Article Eight, Section 8.79 (Protected Information) – adds a definition for the new term "Protected Information."

SECTION 8.79 "Protected Information"

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.

Appendix Eight, Part 8.2 (Audit Requirements for All Participating DFIs) – adds a new item "f" that requires annual ACH Rules Compliance Audits to include a verification that the covered ACH participants (i.e., Participating DFIs, Third-Party Service Providers, and Third-Party Senders) have established, implemented and updated (as appropriate) the security policies, procedures, and systems as required by the Security Requirements provisions.

PART 8.2 Audit Requirements for all Participating DFIs, Third- Party Service Providers, and Third-Party Senders

Each Participating DFI, Third-Party Service Provider, and Third-Party Sender must conduct the following audit of ACH operations. These audit specifications apply generally to all Participating DFIs, regardless of a Participating DFI's status as an ODFI or RDFI. The specifications also apply to Third-Party Service Providers and Third-Party Senders, with the exception of Part 8.2 item (e)

(a) Verify that a Record of each Entry is retained for six years from the date the Entry was transmitted, except as otherwise expressly provided in these Rules. Verify that a printout or reproduction of the information relating to the Entry can be provided, if requested by the Participating DFI's customer or any other Participating DFI or ACH Operator that originated, Transmitted, or received the Entry.

(b) When a Record required by these Rules is created or retained in an Electronic form, verify that the Electronic form
    i. Accurately reflects the information in the Record, and
    ii. Is capable of being accurately reproduced for later reference whether by Transmission, printing, or otherwise.

(c) Verify that the Participating DFI conducted an audit of its compliance with the Rules in accordance with Appendix Eight for the previous year.
(d) Verify that required encryption or a secure session is used for banking information transmitted via an unsecured electronic network.
(e) Verify that for any Entries that are not processed through an ACH Operator but are exchanged with another non-affiliated Participating DFI, the Participating DFI has filed the appropriate N-7 form and paid all Network Administration Fees as required by Section 1.13.
(f) Verify that the Participating DFI has conducted an assessment of the risks of its ACH activities and has implemented a risk management program on the basis of such an assessment.
(g) Verify that the Participating DFI has established, implemented, and updated, as appropriate, security policies, procedures, and systems as required by Article One Section 1.6.

Appendix Eight, Part 8.4 (Audit Requirements for ODFIs) – modifies item "i" for consistency with the new subsection 2.2.1.

PART 8.4 Audit Requirements for all ODFIs, Third- Party Service Providers, and Third-Party Senders

In addition to the audit procedures outlined in Parts 8.1 and 8.2 of this Appendix Eight, ODFIs, and Third-Party Service Providers, and Third-Party Senders when performing an obligation of the ODFI, must conduct an audit of the following relating to the origination of ACH entries. Part 8.4 Items (l) and (m) do not apply to Third-Party Senders.

(a) Verify the ODFI has entered into Origination Agreements with all Originators or Third-Party Senders that bind the Originator or Third-Party Sender to these Rules,
that authorize the ODFI to originate entries on behalf of the Originator or Third- Party Sender; that, within such agreements, the Originator or Third-Party Sender acknowledges that Entries may not be initiated that violate the laws of the United States; that includes any restrictions on types of Entries that may be originated; that includes that the Third Party has entered into an agreement with each Originator, and that such agreements include the right of the ODFI to terminate or suspend the agreement for breach of the Rules, and the right of the ODFI to audit the
Originators, Third-Party Senders and the Third-Party Senders Originators compliance with the Origination Agreement and the Rules. With respect to IAT Entries, verify that agreements contain all necessary provisions.
(b) Verify that, if applicable, the ODFI has entered into agreements with all Sending Points that Transmit Entries on the ODFI's behalf to an ACH Operator.
(c) Verify that the ODFI has assessed the risks of the Originator's or Third-Party Sender's ACH activity, and has established, implemented, and periodically reviewed an exposure limit for each Originator or Third-Party Sender. Verify that the ODFI has established and implemented procedures to monitor the Originators or Third-Party Sender's origination and return activity across multiple Settlement Dates; enforce restrictions on the types of Entries that may be originated; and enforce the exposure limit.
(d) Verify that the ODFI accepts Return Entries and Extended Return Entries that comply with these Rules and that are transmitted by the RDFI within the time limits established by these Rules. Verify that dishonored Return Entries are transmitted within five Banking Days after Settlement Date of the Return Entry and that contested dishonored Return Entries are accepted as required by these Rules. Verify that the ODFI is using Return Reason Codes in an appropriate manner.

(e) Verify that information related to NOCs and Corrected NOCs is provided to each Originator or Third-Party Sender within two Banking Days of Settlement Date of the NOC or Corrected NOC in accordance with Appendix Five. For CIE and credit WEB Entries, verify that information relating to NOCs and Corrected NOCs is provided to any Third-Party Service Provider initiating such entries on behalf of the consumer Originator. Verify that refused NOCs are transmitted within 15 days of receipt of an NOC or corrected NOCs.

(f) With the exception of XCK Entries, verify that the ODFI provides the RDFI, upon receipt of the RDFI's written request, the original, a copy, or other accurate Record of the Receiver's authorization with respect to a Consumer Account within ten Banking Days of receipt of the request without charge. For a CCD, CTX, or Inbound IAT Entry to a non-consumer account verify that the ODFI provides to the RDFI, upon receipt of the RDFI's written request, an accurate record evidencing the Receiver's authorization, or the contact information for the Originator (that at a minimum, includes (a) the Originator's name (b) the Originator's phone number & email address) within ten Banking Days of receipt of the request without charge.

(g) Verify that, when agreed to by the ODFI, late Return Entries are accepted in accordance with these Rules.

(h) Verify that the ODFI has provided the Originator with proper notice to ensure compliance with UCC Article 4A with respect to ACH Transactions.

(i) Verify that the ODFI has utilized a commercially reasonable method to verify the identity of each Originator or Third-Party Sender that enters into an Origination Agreement with the ODFI. When an ODFI has a relationship with a Third-Party Sender rather than with an Originator directly, also verify that the Third-Party Sender has utilized a commercially reasonable method to verify the identity of each Originator that enters into an Origination Agreement with the Third-Party Sender.

(j) Verify that the Reversing Entries and Reversing Files are initiated in accordance with the requirements of these Rules.

(k) For BOC entries, verify that the ODFI has (1) established and implemented commercially reasonable procedures to verify the identity of each Originator or Third-Party Sender of such entries; and (2) established and implemented procedures to document specific information with respect to each Originator as required by these Rules, and that upon request, such information is provided to the RDFI within the required time frame.

(l) Verify that the ODFI has reported Return Rate information on each Originator or Third-Party Sender, as requested by the National Association.

(m) Verify that the ODFI has (1) registered its Direct Access status with the National Association; (2) obtained the approval of its board of directors, committee of the board of directors, or its designee for each Direct Access Debit Participant; (3) provided required statistical reporting for each Direct Access Debit Participant; and
(4) Notified the National Association of any change to the information previously provided with respect to any Direct Access Debit Participant.

(n) Verify that the ODFI has either (1) stated to the National Association that it has no Third-Party Senders; or (2) registered its Third-Party Senders with the National Association, and updated as necessary any such registrations.

(o) Verify that the ODFI has kept Originators and Third-Party Senders informed of their responsibilities under these Rules.