



Rules Audit Enhancement Rule

Ballot #1-09

Executive Summary and Rules Description

DRAFT DATE: January 12, 2009

PART 1: A COMPONENT OF THE RISK MANAGEMENT STRATEGY

NACHA, its members, and the ACH Operators are implementing a comprehensive risk management strategy for the ACH Network. The strategy includes components that address risk throughout the life-cycle of ACH payments, covering:

- Network entry requirements;
- Ongoing requirements;
- Enforcement;
- ACH Operator tools; and
- Cross-channel risk management.

The Rules Audit Enhancement Rule (“Rule”) addresses ongoing requirements under the risk management strategy. The Rule will promote more effective annual audits of compliance with the *NACHA Operating Rules* (“Rules”) by Participating Depository Financial Institutions (“DFIs”). Better audits will facilitate compliance with the *Rules* and ultimately lead to lower risk and higher quality in the processing of ACH payments.

PART 2: RULE DESCRIPTION

The Rule would:

- Refine and clarify existing *Rules* compliance audit obligations;
- Include additional provisions to provide a more robust set of audit criteria; and
- Provide additional guidance for ODFIs, RDFIs and their third-party service providers.

In addition, several considerations for industry best practices for ACH operations are referenced in the introduction to provide additional context.

Currently, the *Rules* require all Participating DFIs¹ to audit their compliance with the *Rules*, and requirements for such an audit are defined in Appendix Eight of the *Rules*. The *Rules* themselves, however, are not static but are amended from time to time. This

¹ The Rules compliance audit requirement of the existing *Rules* and the new Rule also applies to Third-Party Service Providers that perform ACH processing functions on behalf of DFIs.

Rule incorporates audit areas related to many recent *Rules* changes and provides additional specific guidance on key audit points. In addition, the audit requirements are reorganized to include a distinct section on provisions that apply generally to all DFIs, which is intended to facilitate use of the material and eliminate redundant information.

The Rule is intended to help lower ACH Network risk and improve quality by ensuring that DFIs perform a broader assessment of their compliance with the *Rules*, helping them to identify key areas of ACH processing where improvement may be necessary.

As all DFIs are currently required to conduct a *Rules* compliance audit on an annual basis, no financial institution or organization would be required by this Rule to conduct a *Rules* compliance audit that does not already do so. The Rule could result, however, in some DFIs expanding the scope of their audits if they identify shortcomings in their current audit practices.

PART 3: RULES FRAMEWORK

The Rule was issued for comment (“RFC”) on January 4, 2008. NACHA received 61 survey responses and comment letters to the Rule as originally proposed (“Original Proposal”). In the descriptions below, the changes made to the Original Proposal due to comments are specifically identified.

A. *Audit Requirements for All Participating DFIs*

The Rule incorporates a new section identifying key audit requirements applicable to all DFIs, regardless of their particular roles as ODFIs or RDFIs. This section includes general audit requirements relating to record retention and reproduction requirements, audit obligations, data security requirements related to the use of unsecured electronic networks, and the payment of Network transaction fees (including those exchanged via direct send relationships).

The addition of this new section will make general audit obligations for all DFIs easier to locate and eliminates the need to include redundant language in separate sections addressing specific ODFI and RDFI responsibilities.

Changes Since RFC

Respondents to the RFC requested that consistent terms be used throughout the language in Appendix Eight. Previous language in the Original Proposal referencing the verification of various policies and/or procedures has been removed, as the *NACHA Operating Rules* do not mandate the establishment of such policies/procedures but instead obligate the DFI to verify its compliance with the substantive processing requirements of the *Rules*. (Note: Similar changes to terminology have also been made to sections described below specific to ODFIs and RDFIs.) Additional language has been made consistent by using “audit” in place of “examination,” and “verify” in place of

“ensure.” An additional audit point is also included within this general DFI section to incorporate the *Rules* related to Network transaction fees.

The Original Proposal also recommended the incorporation of the following “best practices” as components of an ACH audit. While not mandated by the *NACHA Operating Rules*, these issues were viewed as important to successful ACH processing:

- Verification that the financial institution has a current edition of the *Rules*;
- Verification that ACH policies be consistent with the requirements of OCC Bulletin #2006-39 or other regulatory guidance;
- As applicable, verification that the financial institution has written ACH policies and procedures that have been approved by the Board or a Board-approved committee or senior management designate;
- Verification that the financial institution has written policies and procedures in place to address its ACH OFAC compliance obligations; and
- Verification that the financial institution’s business continuity plan includes ACH operations.

Many commenters stated that these practices are not requirements of the *Rules*, and therefore are not appropriate to be included within the scope of a *Rules* compliance audit. NACHA agrees, but also acknowledges the importance of the best practices to ACH processing. The practices have been deleted as a distinct Recommended Audit Practices section. Instead, references to some practices are included in the introduction to Appendix Eight to provide DFIs with additional context for their ACH operations.

B. Audit Requirements for RDFIs

The Rule expands the scope of audit coverage for RDFIs, incorporating additional rules within the RDFIs’ compliance review. In addition to the existing RDFI audit requirements, this Rule incorporates a review of the RDFI’s:

- Handling of XCK entries and entries received to non-transaction accounts;
- Compliance with rules governing the return of unauthorized debits to corporate accounts;
- Proper utilization of return reason codes;
- Timely return of un-posted credit entries and credit entries returned by the Receiver;
- Handling of ODFI requests for return or adjustments of erroneous entries;
- Compliance with notice requirements for credit entries subject to UCC Article 4A.

Changes Since RFC

In response to comments from the RFC, several portions of Section 8.3 in the Original Proposal were removed as they contained explanations of specific rules rather than references to the rules themselves. Other wording was removed to eliminate the inclusion of redundant language.

The Original Proposal recommended the incorporation of the following “best practices” as components of an ACH audit:

- Verification that the RDFI handles Federal Government payments, reclamations, and Death Notification Entries in accordance with the requirements of 31 C.F.R. Part 210 and the Green Book;
- Review the RDFI’s policies related to the DNE process and its responsibility and liability for Federal Government payments under 31 C.F.R. Part 210 and policies related to the RDFI’s responsibilities and liabilities for Federal Government payments, as required by 31 C.F.R. Part 210 and the Green Book; and
- Review whether the RDFI has procedures in place detailing the differences between the return reasons and codes for stop payment, unauthorized, and authorization revoked.

As with the section on all DFIs described above, this section has been eliminated from the Rule as a distinct section, and instead a reference to Federal Government rules for processing Federal Government entries is referenced in the introduction to the Appendix.

C. Audit Requirements for ODFIs

This Rule broadens the current scope of audit coverage for ODFIs, incorporating additional rules within the ODFI’s requirements for a compliance review. In addition to the existing ODFI audit requirements, this Rule incorporates a review of the ODFI’s:

- Compliance with its obligation to accept and inform the Originator of return entries transmitted by the RDFI;
- Compliance with the rules governing dishonored return entries and handling of contested dishonored returns, including proper use of related return reason codes;
- Compliance with the rules governing the refused NOC process;
- Compliance with its requirements to obtain and provide the RDFI with copies of authorizations when requested to do so;
- Compliance with notice requirements for credit entries subject to UCC Article 4A.
- Proper use of the reversal process; and
- Compliance with the requirement to report information on each Originator or Third-Party Sender as requested by the National Association.

Changes Since RFC

The following modifications to the Original Proposal were made in response to comments from the RFC:

- Removal of several portions of Section 8.4 that contained explanations of specific rules rather than references to the rules themselves;
- Inclusion of additional references to the IAT application (which will become effective on September 18, 2009) and to requirements for the reporting of information on each

Originator or Third-Party Sender as requested by the National Association (both of which were approved after this RFC was issued);

- Elimination of a detailed listing of Originator obligations under the requirement for an ODFI to verify its Originators' and Third-Party Senders' compliance with specific rule obligations; and
- Removal of subsection 8.4.1 (Additional Audit Obligations for ODFIs), which contained a point of knowledge only and not a rule requirement or best practice verifiable through the audit process.

D. General Audit Requirements

This Rule clarifies, within the *Rules* compliance audit language, that the failure of a DFI to provide NACHA with proof of completion a *Rules* compliance audit is a violation of the *NACHA Operating Rules* and may be considered a Class 2 rule violation. The criteria defining a Class 2 rule violation within Appendix Eleven (Rules Enforcement) are expanded to specifically identify the failure to provide the results of an audit.

Changes Since RFC

No modifications to the general audit requirements were made since the RFC was issued.

E. Rules Enforcement

This Rule modifies the definition of a Class 2 *Rules* violation within Appendix Eleven (Rules Enforcement) to support the revisions that establish the failure of a DFI to provide NACHA with the results of an audit as a Class 2 *Rules* violation.

Changes Since RFC

Since issuance of the RFC, additional modifications have been made to the scope of the National System of Fines to explicitly permit NACHA to initiate a rules enforcement proceeding in specific circumstances where a DFI fails to comply with a direct obligation to NACHA (e.g., ODFI Reporting Requirements, payment of transaction fees, etc.), as defined by the *Rules*. Current rules enforcement language permits NACHA to file a *Rules* violation report specific to ODFI Reporting Requirements but does not call out other violations of the *Rules* that directly involve obligations to the National Association. The inclusion of this additional language eliminates ambiguity regarding NACHA's right to initiate a *Rules* enforcement proceeding where the *Rules* mandate its involvement, such as the failure of a DFI to provide NACHA with proof of completion of a *Rules* compliance audit.

PART 4: TECHNICAL SUMMARY

The following changes to the technical language within Appendix Eight of the *Rules* are included in this Rule:

- Appendix Eight, Introduction – Modifies the introductory discussion on *Rules* compliance audits to provide additional guidance on the scope of the audit obligation and to incorporate references to additional subsections by which audit requirements are categorized; references a limited number of non-rule-related best practices for ACH operations.
- Appendix Eight, Section 8.1 (General Audit Requirements) – modifies this section to clarify that the failure to provide NACHA with the results of an audit may be considered a Class 2 rule violation and subject to the rules governing such violations under the National System of Fines.
- Appendix Eight, Section 8.2 (Audit Requirements for All Participating DFIs) – removes certain general audit requirements from the RDFI audit section and places them within this section specific to all DFIs; rearranges the location of some existing audit requirements for clarity or ease of use.
- Appendix Eight, Section 8.3 (Audit Requirements for RDFIs) – modifies this section to incorporate new rules sections within the scope of the RDFI's *Rules* compliance audit; rearranges the location of some existing audit requirements for clarity or ease of use.
- Appendix Eight, Section 8.4 (Audit Requirements for ODFIs) – modifies this section to incorporate new rules sections within the scope of the ODFI's *Rules* compliance audit; removes certain general audit requirements from the ODFI audit section and places them within a new section specific to all DFIs; rearranges the location of some existing audit requirements for clarity or ease of use.
- Appendix Eleven, Sections 11.1 (Scope), 11.3.1 (Initiation of a Rules Enforcement Proceeding), and 11.3.3 (Submission Requirements for Rules Enforcement Proceedings Initiated by the National Association) – modifies these sections to clarify the circumstances under which NACHA would be eligible to initiate a *Rules* enforcement proceeding under the National System of Fines.
- Appendix Eleven, Section.11.3.7.4 (Class 2 Rules Violation) – expands the definition of a Class 2 rules violation to include a DFI's failure to provide the National Association with proof of completion of a *Rules* compliance audit.

PART 5: IMPLEMENTATION

The Rule will become effective on December 18, 2009, with *Rules* compliance audits conducted under the revised requirements to be completed no later than December 1, 2010. Although not mandatory until the 2010 audit year, earlier compliance with these expanded audit provisions is encouraged for all DFIs in an effort to mitigate areas of potential risk due to non-compliance with the *Rules*.