



Risk Management and Assessment Rule *Request for Additional Comment*

Executive Summary and Rules Description **February 12, 2009**

ADDITIONAL COMMENTS REQUESTED BY MARCH 7, 2009

NACHA requests additional comments from its voting members on a proposed rule (“Rule”) to establish risk management practices for Participating Depository Financial Institutions. NACHA originally requested comment from all ACH Network participants on January 4, 2008 (the “Original Proposal”). In response to many of the comments that were received, the Rule has been revised. In most cases the revisions have been to simplify the provisions of the Original Proposal, and do not contain any requirements that would exceed those in the Original Proposal. Due to the changes in the overall form of the Rule, however, some NACHA members as well as the Risk Management Advisory Group have asked for an additional opportunity to comment. NACHA is therefore providing an additional comment period for its voting members.

NACHA STAFF CONTACTS

Return comments to:

Maribel Bondoc, Manager, ACH Network Rules
Fax (703) 787-0996
E-mail: mbondoc@nacha.org

Questions:

Michael Herd, Managing Director, ACH Network Rules
Phone (703) 561-3924
E-mail: mherd@nacha.org

Debbie Barr, AAP, CTP, Senior Director, ACH Network Rules
Phone (703) 561-3920
E-mail: dbarr@nacha.org

PART 1: BACKGROUND

In recent years, the banking industry and regulators have devoted additional attention to ACH risk management. The NACHA Risk Management Strategy and the OCC Bulletin 2006-39 are two significant milestones.

Currently, the requirements of the *Rules* related to ODFIs’ risk management is limited to establishing, reviewing, and monitoring exposure limits for an Originator’s ACH activity. This Rule would codify within the *NACHA Operating Rules* additional risk management practices that are common in the industry that would improve risk management in the ACH Network when utilized by all DFIs. Codifying such practices in the *Rules* ties the performance of basic risk

management practices into the *Rules* and sends a strong message to the industry about the importance of risk management.

PART 2: RULES DESCRIPTION

A chart comparing the provisions of this revised Rule to the Original Proposal can be found on Page 8.

A. Risk Assessments

The Rule would require all Participating DFIs to conduct a risk assessment of their ACH activities, and to implement risk management programs based on the results of such assessments, in accordance with the requirements of their regulator(s).

Revisions to Original Proposal

The Original Proposal would have established various levels of risk assessments, and defined specific criteria for such assessments, scaled to the nature and complexity of the DFIs' ACH activities. While responses to the Request for Comment ("RFC") showed a significant amount of support for this framework, there were also significant differences of opinion on the appropriateness of the specific levels and criteria. In addition, a number of commenters identified the potential for DFIs to be confused about the requirements of NACHA's risk assessments relative to those required by their regulators.

In response, the Rule has been revised to take a simpler approach to risk assessments. The various levels of risk assessments are eliminated in favor of a single requirement that cross-references assessments required by regulators.

Examples of recent risk-management requirements and guidance by regulators include:

- OCC Bulletin 2006-39, Automated Clearing House Activities, September 1, 2006 (see <http://www.occ.treas.gov/ftp/bulletin/2006-39.pdf>);
- FFIEC's BSA/AML Examination Manual, 2007 edition (see http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2007.pdf, pages 199 through 205);
- OCC Bulletin 2008-12, Payment Processors, April 24, 2008 (see <http://www.occ.treas.gov/ftp/bulletin/2008-12.html>);
- FDIC Financial Institution Letter 127-2008, Payment Processor Relationships, November 7, 2008 (see <http://www.fdic.gov/news/news/financial/2008/fil08127.html>);
- FFIEC Guidance on Risk Management of Remote Deposit Capture, January 14, 2009 (see http://www.ffiec.gov/pdf/pr011409_rdc_guidance.pdf).

Generally, these regulators stress the importance of 1) assessing the nature of risks associated with ACH activity; 2) performing appropriate know-your-customer due diligence; 3) establishing controls for Originators, third-parties, and direct-access to ACH Operator relationships; and 4) having adequate management, information and reporting systems to monitor and mitigate risk.

Pros and Cons of Revisions

The pros of revising the Rule in this way are: 1) it should be simpler for DFIs to implement than the Original Proposal; and 2) it is by definition consistent with regulatory requirements, which should eliminate the possibility of duplication of effort by DFIs.

The cons of revising the Rule are: 1) the lack of uniformity of regulatory requirements to all DFIs; 2) potential gaps in the level of guidance provided by different regulatory agencies; and 3) less specificity in the Rule, which would have allowed NACHA to state additional requirements where appropriate. If the FFIEC should adopt a uniform approach to ACH risk management (e.g., the OCC approach) in the future, there would then be uniformity for all DFIs in such regulatory requirements.

B. Agreements with Originators and Third-Party Senders

The Rule would provide that each ODFI has:

- The right to terminate or suspend an Originator, or any Originator of a Third-Party Sender, for breach of the *Rules*; and
- The right to audit an Originator's, or Third-Party Sender's and its Originators', compliance with the agreement and the *Rules*.

The Rule would also require an ODFI to expressly address each of the foregoing, as well as any restrictions on ACH origination activity, within a new or renewed agreement with an Originator or Third-Party Sender. The Rule would not prescribe new restrictions on origination activity. Rather, the Rule would require each ODFI to address its internally developed restrictions on origination, if any, within its Originator and Third-Party Sender agreements so as to highlight the importance, and improve the enforcement, of such restrictions.

Revisions to Original Proposal

The Original Proposal would have required ODFIs to identify their Originators' and their Third-Party Senders' Originators' lines of business, and to address requirements specific to those lines of business in their agreements. Responses to the RFC indicated that while a "lines of business" approach is consistent with OCC 2006-39 and can be useful in identifying risk, it is too complicated and burdensome to implement.

In response, the Rule has been revised to take a simpler approach to addressing restrictions on origination activity. The "lines of business" approach is eliminated in favor of a generic requirement that ODFIs address any restrictions on ACH origination activity in their relevant agreements. For example, under this more generic requirement, ODFIs could specify restrictions by Standard Entry Class (SEC) Code, which is often a reasonable determining factor in lines of business, and is also information that is readily available to all ODFIs. ODFIs would also be permitted, however, to use alternative methods for determining restrictions, at their discretion, such as lines of business.

The Original Proposal would also have required ODFIs to address in their agreements their Originators' and Third-Party Senders' recordkeeping requirements. Commenters viewed this requirement as redundant to existing recordkeeping requirements in the *Rules*, and in response the Rule has been revised to eliminate this provision.

The Original Proposal did not address whether existing ODFI agreements with Originators and Third-Party Senders would be "grandfathered" or would need to be modified as of the effective date of the Rule. Commenters stated that revising all such agreements prior to the effective date of the Rule would be an extremely costly and administratively burdensome requirement. Furthermore, several commenters argued that the *Rules* already require Originators and Third-Party Senders to enter into agreements with ODFIs under which they agree to be bound by the *Rules*, and therefore no modifications to such agreements should be required. As an alternative, these commenters suggested that the *Rules* could be modified elsewhere to state that ODFIs have the right to 1) terminate or suspend an Originator or Third-Party Sender for breach of the *Rules*, and 2) audit an Originator's or Third-Party Sender's compliance with the *Rules*. By signing agreements with ODFIs, Originators and Third-Party Senders would presumably be bound by these provisions as well.

In recognition of the administrative burden inherent in modifying existing contracts, the Rule would apply the new content requirements only on a "going-forward" basis to agreements entered into or renewed on or after the implementation date of the Rule. To take advantage of ODFI agreements which generically require *Rules* compliance in the interim, the Rule also incorporates the termination and audit provisions as substantive amendments to Originator and Third-Party Sender obligations.

Pros and Cons of Revisions

Because ODFIs act as the gateway to the ACH Network, the ability of ODFIs to manage risk arising out of their Originator and Third-Party Sender relationships is essential to the overall integrity of the system. The benefit of revising the Rule in the way described is that, on a going-forward basis, certain key requirements, *Rules* provisions and ODFI rights will be made explicit to Originators and Third-Party Senders via ODFI agreements. Pushing these requirements "downstream" to Originators and Third-Party Senders via agreements should result in more effective risk management and better *Rules* compliance for the ACH Network. In addition, because the requirement for new agreement language would apply to agreements only on a going-forward basis, the cost and administrative effort for ODFIs would be reduced. By also incorporating the termination and audit provisions as substantive amendments to Originator and Third-Party Sender obligations, the Rule further provides immediate benefits for ODFIs whose Originator and Third-Party Sender agreements broadly require *Rules* compliance. While ODFIs should notify Originators and Third-Party Senders of such changes, the burden of a simple notice is significantly less than the effort necessary to engage in a mid-term contract negotiation.

The cons of revising the Rule in this way are that ODFIs will still bear the cost and administrative burdens of revising their agreements on a "going-forward" basis, including in contract roll-overs. In the interim, depending on the processes ODFIs use to notify their

Originators and Third-Party Senders of *Rules* changes, the level of attention to and enforcement of these requirements may not be as strong.

C. ODFI Risk Management Practices

The Rule would require ODFIs to perform a more comprehensive set of risk management practices in addition to the current rules on exposure limits. Specifically, an ODFI would be required to:

- Perform due diligence with respect to Originators and Third-Party Senders sufficient to form a belief that the party has the capacity to perform its obligation in conformance with the *Rules*;
- Assess the nature of the Originator's or Third-Party Sender's ACH activity and the risks it presents;
- Establish an exposure limit for the Originator or Third-Party Sender; and
- Establish procedures to (1) monitor the Originator's or Third-Party Sender's origination and return activity, relative to its exposure limit, across multiple settlement dates; (2) enforce the exposure limit; and (3) enforce restrictions on the types of ACH transactions that may be originated.

These requirements reflect ACH industry best practices to ensure that all ODFIs perform appropriate know-your-customer due diligence and establish appropriate procedures, systems and controls to manage the risks of Originators' or Third Party Senders' ACH activities.

Revisions to Original Proposal

The Original Proposal would have required an ODFI to confirm the lines of business of its Originators or Third Party Senders. Similar to the previous section, the Original Proposal has been revised in response to comments received to remove a "lines of business" approach for these ODFI Risk Management Practices. While commenters viewed such as an approach as useful in identifying risk, they generally viewed the approach as too complicated and burdensome to implement.

Pros and Cons of Revisions

The benefit of revising the Original Proposal in the way described is that it should be easier for ODFIs to implement the risk management practices without being required to identify and track Originators' and Third-Party Senders' Originators' lines of business.

The con of this revision is the potential lessening of the effectiveness of the risk management practices. Understanding lines of business, and how it changes over time, is often an effective indicator of risk.

PART 3: IMPLEMENTATION

The Risk Management and Assessment Rule would become effective on December 19, 2009. ODFI agreements with Originators and Third-Party Senders entered into or renewed on or after the effective date would need to comply with the Rule.

PART 4: APPENDICES

A. NACHA's Risk Management Strategy

The Risk Management and Assessment Rule is a component of NACHA's Risk Management Strategy, the goal of which is to ensure high-quality ACH transactions and reduce risk for financial institutions, businesses and consumers. The strategy addresses risk throughout the life-cycle of ACH payments, covering:

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

This Rule addresses network entry requirements and ongoing requirements with respect to risk management and mitigation.

This Rule is consistent with the U.S. Department of the Treasury's Office of the Comptroller of the Currency ("OCC") Bulletin 2006-39 ("Bulletin") of September 1, 2006. The Bulletin provides guidance to national banks on managing the risks of their ACH activities, and states "Each bank should...use this guidance to develop an ACH risk management program that reflects the nature and complexity of the bank's activities."

B. Impact of the Proposal

All Participating DFIs would be impacted by the requirement to perform a risk assessment. This impact would be lessened by the number of DFIs that already conduct such assessments. In response to Original Proposal, over eighty percent of respondents indicated that their institutions already perform a risk assessment similar to that which was proposed for RDFIs; less than half the respondents indicated that their institutions perform an assessment similar to those which were proposed for ODFIs.

ODFIs would also be impacted by the requirement to conduct additional risk management practices prior to originating ACH entries, and by the requirement to cover specific topics in their Originator agreements. The scale of this impact depends on the nature and complexity of each ODFI's ACH activity. ODFIs that do not currently conduct these or similar risk management practices, or that would need to revise their Originator agreements, would be the most significantly impacted. Again, this impact would be lessened by the number of ODFIs that already employ these practices. Many ODFIs already perform the Rule's risk management

practices prior to originating ACH entries. Seventy-three percent of financial institutions responded to the RFC that they would need to modify their Originator agreements.

In response to comments, the Rule attempts to minimize the administrative burden on ODFIs by applying only to Originator agreements on a “going forward” basis; that is, agreements entered into or renewed after the effective date would need to comply with the Rule’s requirements, but agreements in place prior to the effective date would not need to be modified.

C. Technical Summary

The following changes to the technical language within the *Rules* are included in this proposal:

- Article One, subsection 1.2.2 (Risk Assessments) – expands the general rule requirement section for Participating DFIs to incorporate an ACH risk assessment obligation in accordance with the requirements defined by the Participating DFIs’ regulator(s), and the establishment of a risk management program as fundamental requirements with which Participating DFIs must agree to comply.
- Article Two, subsection 2.1.1 (Originator Authorization and Agreement) – expands the current subsection to establish topics that must be addressed in ODFI agreements with Originators and Third-Party Senders.
- Article Two, subsection 2.1.12 (ODFI Risk Management) – expands the current subsection requiring ODFIs to establish exposure limits for Originators and Third-Party Senders to define a broader set of ODFI requirements governing risk management.
- Article Three, section 3.14 (Termination, Suspension and Audit of Originators) – provides that an agreement between an Originator and an ODFI can be terminated or suspended for breach of the *Rules*, and provides that an ODFI can audit an Originator’s compliance with the *Rules*.
- Article Five, section 5.6 (Termination, Suspension and Audit of Third-Party Senders) – provides that an agreement between a Third-Party Sender and an ODFI can be terminated or suspended for breach of the *Rules*, and provides that an ODFI can audit a Third-Party Sender’s compliance with the *Rules*.

D. Comparison of Requirements of Original Proposal and Rule

Requirement	Original Proposal	Rule
Perform Risk Assessment	All DFIs: Level 1 – RDFIs Level 2 – ODFIs, simple Level 3 – ODFIs, complex - Has agreement with TPS - Allows direct access to ACH Operator - Unauthorized exceeds 1% - Exceeds capital ratio - Has money transmitter, online payments processor as Originator - Has been sanctioned for Class 2 or 3 <i>Rules</i> violation	All DFIs per regulator Examples: - OCC 2006-39 - BSA/AML - OCC 2008-12 - FDIC FIL 127-2008 - FFIEC Guidance on RDC
ODFIs Agreements w/ Originators and Third-Party Senders	1. Any restrictions on acceptable lines of business 2. Specific requirements relevant to lines of business 3. Right of ODFI to terminate or suspend for breach of <i>Rules</i> 4. Right of ODFI to audit <i>Rules</i> compliance 5. Originator/TPS reporting and recordkeeping requirements 6. “Grandfathering” not proposed	1. Any restrictions on ACH origination activity 2. Right of ODFI to terminate or suspend for breach of <i>Rules</i> 3. Right of ODFI to audit <i>Rules</i> compliance 4. Effective on “going forward” basis
ODFIs’ Rights to Terminate, Suspend, and Audit Originators and Third-Party Senders	Not proposed	1. Allow ODFIs to terminate or suspend for breach of <i>Rules</i> 2. Allow ODFIs to audit <i>Rules</i> compliance
ODFI Risk Management Practices	1. Perform financial and operational due diligence 2. Confirm lines of business of Originator or TPS 3. Assess nature of ACH activity and its risks 4. Establish exposure limit 5. Monitor and enforce restrictions and limits 6. Periodically update	1. Perform financial and operational due diligence 2. Assess nature of ACH activity and its risks 3. Establish exposure limit 4. Monitor and enforce restrictions and limits

#####