



January 18, 2008

NACHA's RISK MANAGEMENT AND ASSESSMENT PROPOSAL RULES COMPLIANCE AUDIT PROPOSAL

EXECUTIVE SUMMARY

- NACHA issued two proposals simultaneously; Risk Management and Assessment and Rules Compliance Audit.
- The proposals are part of NACHA's comprehensive risk management strategy.
- The Risk Management and Assessment Proposal would require all depository financial institutions (DFIs) to annually assess the risks of their ACH activities.
- Originating depository financial institutions (ODFIs) would be required to conduct additional risk management practices before originating ACH entries and include certain topics in their Originator and Third-Party Sender agreements.
- The Rules Compliance Audit would provide additional compliance guidance for ODFIs, RDFIs and Third-Party Service Providers.
- The NACHA Rules would clarify existing compliance audit obligations and reference several industry best practices related to ACH transaction quality.
- **Please submit your comments to CUNA by February 5, 2008. Comments are due to the NACHA by February 19, 2008.**

Please feel free to fax your responses to CUNA at 202-638-7052; Assistant General Counsel Lilly Thomas at lthomas@cuna.com; or mail them to Lilly c/o CUNA's Regulatory Advocacy Department, 601 Pennsylvania Avenue, NW, South Building, Suite 600, Washington, D.C. 20004. [Click here](#) for a copy of this Request for Comment.

BACKGROUND

NACHA is implementing a comprehensive risk management strategy to ensure high-quality ACH transactions and reduce risk for financial institutions, businesses and consumers. The Risk Management Strategy's framework has the following categories:

1. Network Entry Requirements
2. Ongoing Requirements
3. Enforcement
4. ACH Operator Tools; and
5. Cross-Channel Risk Management

The Risk Management and Assessment Proposal is part of NACHA's entire risk management strategy and would require all DFIs in the ACH Network to annually assess the risks of their ACH activities. Additionally, ODFIs would be required to conduct additional risk management practices before originating ACH entries.

The Rules Compliance Audit Proposal would modify NACHA's Operating Rules to clarify and expand the rules compliance audit obligations and reference certain best practices as a key component of the rules compliance audit.

DISCUSSION OF PROPOSALS

Risk Management and Assessment Proposal

NACHA is proposing to broaden the scope of its Operating Rules related to risk management to incorporate specific requirements for participating depository financial institutions (DFIs). DFIs would be required to conduct an overall assessment of their risk regarding their ACH origination and receipt activity, as well as adopt specific risk management practices specific to each Originator or Third-Party Sender. Additionally, a participating DFI's agreement would be expanded so that each participating DFI would agree to comply with any rules involving the assessment of the risk of its ACH activity and to implement a risk management program based on the results.

Specific requirements would be incorporated into the current rules creating greater comprehensive risk management obligations for ODFIs. The ODFI would be required to:

- Perform financial and operational due diligence of Originators and Third-Party Senders;
- Identify the line(s) of business of the Originator or Originators of the Third-Party Sender;
- Assess the nature of the Originator's or Third-Party Sender's ACH activity and the risk it presents;
- Establish an exposure limit for the Originator or Third-Party Sender that is related to the nature of its ACH activity and related risks;
- Establish procedures and controls to monitor and enforce limits on the Originator's or Third-Party Sender's origination activity, return activity, and exposure across multiple settlement dates;
- Implement procedures to periodically review the practices outlined above; and

- Address within its agreement with the Originator or Third-Party Sender:
 - any restrictions on acceptable lines of business;
 - specific Originator or Third-Party Sender requirements relevant to the lines of business;
 - the right of an ODFI to terminate or suspend the agreement for breach of the Rules;
 - the right of an ODFI to terminate or suspend an Originator or a Third-Party Sender for breach of the Rules;
 - the right of an ODFI to audit the Originator's compliance with the agreement and the Rules; and
 - the Originator's or Third-Party Sender's reporting and record-keeping requirements.

A new Appendix Nine would be added to NACHA's Operating Rules that would define criteria for an evaluation of ACH payment system risk by the Participating DFI's role and would base specific requirements on the nature and complexity of that activity. Participating DFIs would have to review their systems and/or procedures to monitor and control the risks associated with their ACH activity. The risk assessments must be completed by December 1 of each year and DFIs would be required to provide NACHA with the results upon request.

Appendix Nine would provide the requirements for an assessment of the risks of a Participating DFI's ACH activities. There would be three levels of risk assessments scaled to the nature and complexity of ACH activity:

- Level 1 Risk Assessment for RDFIs;
- Level 2 Risk Assessment for ODFIs; and
- Level 3 Risk Assessment for ODFIs.

Level 1 Risk Assessment requires an RDFI to conduct an annual assessment by those persons not responsible for the RDFI's daily ACH operations to ensure that it:

- Clearly identifies the risks of its receiving activities;
- Sets sound objectives for the management of risks; and
- Identifies and implements policies and practices to achieve the objectives.

Level 2 Risk Assessment would be required for an ODFI that is not required to conduct a Level 3 Risk Assessment. An ODFI in this category would be obligated to conduct an annual assessment by those individuals not responsible for the ODFI's daily ACH operations to ensure that it:

- Clearly identifies the risks of its origination activity;
- Sets sound objectives for the management of risks;
- Identifies and implements policies and practices to achieve the objectives;
- Has systems in place to monitor and control the risks of its ACH activity; and
- Complies with the risk management practices defined for ODFIs under Article Two (Origination of Entries).

A Level 3 Risk Assessment must be performed by independent auditors or dedicated audit personnel not responsible for the ODFI's daily ACH operations activity. ODFIs under a Level 3 Risk Assessment would be required to:

- Clearly identify the risks of its origination activity;
- Set sound objectives for the management of risks;
- Identify and implement policies and procedures to achieve the objectives;
- Adequately report to, and have adequate oversight by, its Board of Directors or Board-approved committee(s) on its ACH origination risk profile and risk management objectives;
- Evaluate on an ongoing basis whether the ACH activities are conducted within the risk parameters established by the Board of Directors;
- Have systems in place to monitor and control the risks of the ACH activity;
- Comply with the risk management practices defined for ODFIs under Article Two (Origination of Entries); and
- Have adequate oversight of Third-Party Senders.

Level 3 Risk Assessment is required for ACH origination activity with one or more of the following criteria within the twelve-month period preceding the assessment or since the most recent risk assessment was conducted, whichever is greater:

- The ODFI has an agreement with a Third-Party Sender;
- The ODFI permits an Originator or Third-Party Sender to transmit ACH files directly to an ACH Operator using its routing number(s);
- The ODFI originates ACH debit transactions for an Originator whose return transactions for unauthorized entries exceeds one percent of its forward debit transactions;
- The value of debit entries originated by the ODFI on any business day exceeds a percentage or multiple (e.g. 10 percent, 25 percent, 100 percent, 2 times) of its risk-based capital, as published from time to time by NACHA;
- The ODFI originates ACH debit transactions for an Originator whose business lines include, but are not limited to, money services, money transmission, or online payments processing;
- The ODFI originates ACH debit transactions for an Originator whose business lines include those published from time to time by the National Association as having high rates of return;
- The ODFI has been subject to a Class 2 or Class 3 rules enforcement action by NACHA, pursuant to the requirements of Appendix Twelve (Rules Enforcement).

In determining whether an ODFI must conduct a Level 3 Risk Assessment, one of the conditions requires that the value of debit entries originated by the ODFI on any business day exceeds a percentage or multiple of its risk-based capital, as published from time to time by NACHA. This is a new concept in the NACHA Rules environment of ODFIs comparing the dollar amount of their ACH debit

origination from one business day in relation to their available risk-based capital. NACHA estimates that the total dollar amount of ACH debits originated by ODFIs on an average business day is 3.5% of their risk-based capital.

Rules Compliance Audit Proposal

This proposal would clarify and expand the rules compliance audit obligations for ODFIs, RDFIs and their third-party service providers. Additionally, certain best practices would be introduced as a key component of the rules compliance audit where these practices play a critical role in helping to ensure the participating DFI's ability to comply with the ACH rules

Key audit requirements applicable to all participating DFIs and their third-party service providers would be incorporated into a new section of the Rules. It would include general audit requirements relating to record retention and reproduction requirements, audit obligations and data security requirements related to the use of unsecured electronic networks.

Even though not specifically required by the Rules, the following best practices would be included as a component of the rules compliance audit:

- Verification that the financial institution has a current edition of the *Rules*;
- As applicable, verification that the financial institution has Board-approved, written ACH policies and procedures in place that are consistent with OCC Bulletin #2006-39 or other regulatory guidance;
- Verification that the financial institution has reasonable procedures in place to monitor for OFAC compliance; and
- Verification that the financial institution has a contingency plan in place that has been tested successfully within the past year and that references ACH Operations.

The audit coverage for RDFIs would be expanded, incorporating additional rules within the RDFI's compliance review. This proposal would add a review of the following to the existing RDFI audit requirements:

- Procedures to handle destroyed check entries (XCK entries) and entries to non-transaction accounts;
- Policies with respect to responsibility and liability for Federal Government and non-government benefit payments;
- Compliance with rules governing the return of unauthorized debits to corporate accounts;
- Policies with regard to the proper use of return reason codes, and the specific procedures to handle each code;
- Policies with respect to the RDFI's obligations and timing requirements for the return of unposted credit entries and credit entries returned by the Receiver;

- Policies related to an ODFI's request for return or adjustments of an erroneous entry;
- Policies related to requests to an ODFI for a copy of the Receiver's authorization; and
- Compliance with notice requirements for credit entries subject to UCC Article 4A.

In some cases, these audit criteria are not directly related to a specific NACHA rule, but address best practices to ensure proper processing of ACH transactions. These include:

- A review of the RDFI's (1) policies related to the DNE process and its responsibility and liability for Federal Government payments under 31 C.F.R. Part 210; (2) 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 (3) procedures to handle Federal Government reclamation entries; and
- A review of whether the RDFI has procedures in place detailing the differences between the return reasons and codes for stop payment, unauthorized, and authorization revoked.

Audit coverage for ODFIs would be broadened to include additional rules. This proposal includes the audit criteria to verify that the ODFI has documented policies with respect to entries originated under its routing number on behalf of another financial institution. This audit criterion is not directly related to a specific NACHA rule, but addresses best practices to ensure proper processing of ACH transactions.

In addition to the existing ODFI audit requirements, this proposal would incorporate 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;
- policies for compliance with the rules governing the refused NOC process;
- compliance with its requirements to obtain and provide the RDFI with copies of authorizations;
- compliance with notice requirements for credit entries subject to UCC Article 4A.
- policies and procedures with respect to the proper use of the reversal process;
- Originators' compliance with the rules governing:
 - Retention and copy requirements for authorization;
 - Proper use of Standard Entry Class Codes;

- Requests for copies of written statements under penalty of perjury;
- Notice to the Receiver concerning changes to dates and amounts of debit entries;
- Recent changes to rules related to electronic check applications (ARC, BOC, POP); and
- Data security requirements for WEB entries.

QUESTIONS REGARDING THE RULES COMPLIANCE PROPOSAL

1. Do you agree with the requirement for all Participating DFIs to annually conduct an assessment of the risks of their ACH activities?

Yes _____ No _____

Please explain

2. Do you agree with the proposed method of scaling risk assessments to the nature and complexity of a Participating DFI's ACH activity?

Yes _____ No _____

Please explain

3. Do you agree that Risk Assessment Requirements should be a separate appendix in NACHA's Operating Rules?

Yes _____ No _____

Please explain

4. Do you agree with expanding the ODFI exposure limit requirements to incorporate more detailed risk management practices prior to origination?

Yes _____ No _____

Please explain

5. Do you agree that additional risk-related topics should be addressed in ODFIs' agreements with Originators and Third-Party Senders?

Yes _____ No _____

Please explain

6. Would you need to modify your agreements with Originators and Third-Party Senders if this proposal is implemented?

Yes _____ No _____

Please explain

7. Do you support the Level 1 Risk Assessment requirements for RDFIs?

Yes _____ No _____

Please explain

8. Do you support the proposed distinctions between Level 2 and Level 3 Risk Assessments?

Yes _____ No _____

Please explain

9. Which of the following, if any, of the seven conditions that would require a Level 3 Risk Assessment do you agree with (check all that you support)?

_____ the ODFI has an agreement with a Third-Party Sender;

- _____ the ODFI permits an Originator or Third-Party Sender to transmit ACH files directly to an ACH Operator using its routing number(s);
- _____ the ODFI originates ACH debit transactions for an Originator whose return transactions for unauthorized entries exceeds one percent of its forward debit transactions;
- _____ the value of debit entries originated by the ODFI on any business day exceeds a percentage or multiple (i.e., 10 percent, 25 percent, 100 percent, 2 times, etc.) of its risk-based capital, as determined by NACHA;
- _____ the ODFI originates ACH transactions for an Originator whose business lines include, but are not limited to, money services, money transmission, or online payments processing;
Are there other lines of business that should be included?
- _____ the ODFI originates ACH transactions for an Originator whose business lines include those published from time to time by the National Association as having high rates of return;
- _____ the ODFI has been subject to a Class 2 or Class 3 rules enforcement action by NACHA?

Please explain

10. A. If you support comparing ACH originated debit dollars to risk-based capital, what factors should NACHA consider in setting the percentage or multiple (e.g. 10%, 25%, 2 times) of risk-based capital (check all that apply)?

- _____ the number of ACH debits originated by an ODFI;
- _____ the type of ACH debits originated by an ODFI;
- _____ a specific time period based on the number of days a debit can be returned;
- _____ the percentage of debits originated to corporate accounts vs. consumer accounts;
- _____ the ODFI's return rates;
- _____ the ODFI's relationship(s) to an industry average(s);
- _____ Other _____
- _____ We do not support comparing ACH originated debit dollars to risk-based capital;

Please explain

B. What should the percentage or multiple be?

- _____ 3.5% of risk-based capital (NACHA's estimate of the industry average)
- _____ 10%
- _____ 25%
- _____ 100%
- _____ 2 times
- _____ Other _____
- _____ Do not know

11. What would be the operational and/or financial impact to you associated with this proposal?

12. Do you believe changes to your ACH software would be required with this proposal?

Yes _____ No _____

If yes, please explain: _____

13. Do you agree with the proposed implementation date for this proposal of December 19, 2008, with the first new assessment to be completed by December 1, 2009?

Yes _____ No _____

Please explain

Amendments to the NACHA Operating Rules may be implemented up to four times each year in March, June, September, and December. Amendments with software changes may be implemented in March and September. If you believe another implementation date would be more appropriate, please select the date below.

- _____ June 2008 (first assessment to be completed by 12/1/08)
- _____ September 2008 (first assessment to be completed by 12/1/08)
- _____ September 2008 (first assessment to be completed by 12/1/09)
- _____ March 2009 (first assessment to be completed by 12/1/09)
- _____ Other (please specify) _____

QUESTIONS REGARDING THE RULES COMPLIANCE PROPOSAL

14. Do you agree with the proposed restructuring of the descriptions of the ACH Rules Compliance Audit which creates a section for all Participating Depository Financial Institutions (DFIs), as well as separate sections for Receiving Depository Financial Institutions (RDFIs) and Originating Depository Financial Institutions (ODFIs)?

Yes _____ No _____

Please explain

15. Do you agree with including audit obligations that do not relate directly to specific rules requirements?

Yes _____ No _____

Please explain

16. Do you believe NACHA should randomly request proof of completion of the ACH Rules Compliance Audits?

Yes _____ No _____

Please explain

17. Do you agree with requiring verification that a DFI completed its audit from the previous year and addressed any outstanding issues?

Yes _____ No _____

Please explain

18. Do you agree with the proposed audit requirements for RDFIs?

Yes _____ No _____

Please explain

19. Do you support the proposed audit requirements for ODFIs?

Yes _____ No _____

Please explain

20. Do you support the proposed audit requirements for ODFIs related to Originators and Third-Party Senders?

Yes _____ No _____

Please explain

21. What would be the operational and/or financial impact to you associated with this proposal?

22. Do you believe changes to your ACH software would be required with this proposal?

Yes _____ No _____

If yes, please explain

23. Do you agree with the proposed implementation date for this proposal of December 19, 2008, with the first audit under these requirements to be completed by December 1, 2009?

Yes _____ No _____

If not, please explain _____

Amendments to the NACHA Operating Rules may be implemented up to four times each year in March, June, September, and December. Amendments with software changes may be implemented in March and September. If you believe another implementation date would be more appropriate, please select the date below.

- _____ June 2008 (first audit to be completed by 12/1/08)
- _____ September 2008 (first audit to be completed by 12/1/08)
- _____ September 2008 (first audit to be completed by 12/1/09)
- _____ March 2009 (first audit to be completed by 12/1/09)
- _____ Other (please specify) _____

24. Please provide any additional comments.

Eric Richard • General Counsel • (202) 638-5777 • erichard@cuna.com Mary Mitchell Dunn • Deputy General Counsel • (202) 638-5777 • mdunn@cuna.com Jeffrey Bloch • Senior Assistant General Counsel • (202) 638-5777 • jbloch@cuna.com Lilly Thomas • Assistant General Counsel • (202) 638-5777 • lthomas@cuna.com
