



**NOTICE OF AMENDMENT
TO THE
2009 ACH RULES**

April 9, 2009

SUPPLEMENT #1-2009

- 1. NACHA OPERATING RULES: Rules Audit Enhancement Rule**
 - 2. NACHA OPERATING GUIDELINES: OFAC Compliance**
-

NACHA OPERATING RULES: RULES AUDIT ENHANCEMENT RULE

SUMMARY

Since the publication of the 2009 edition of the *ACH Rules*, NACHA's Voting Membership has approved one additional amendment to the *NACHA Operating Rules (Rules)*. This amendment, which will become effective December 18, 2009, will refine and clarify existing *Rules* compliance audit requirements for all Participating DFIs, with specific provisions for ODFIs and RDFIs. These revisions will result in more effective annual audits, which will promote improved *Rules* compliance and higher quality transaction processing. Compliance with the revised audit provisions is not mandatory until the 2010 audit year; however, earlier adoption of these audit provisions is encouraged for all DFIs to mitigate areas of potential risk caused by non-compliance with the *Rules*. Details of the changes are provided below.

KEY COMPONENTS OF RULE AMENDMENT

All Participating DFIs

The Rules Audit Enhancement Rule ("Rule") incorporates a new section identifying key audit requirements applicable to all Participating 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 makes 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.

RDFIs

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

- Appropriate 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; and
- Compliance with notice requirements for credit entries subject to UCC Article 4A.

ODFIs

This Rule broadens the current scope of an ODFI's audit coverage by 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 obligation 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 obligation to report information on each Originator or Third-Party Sender as requested by the National Association.

General Audit Requirements

This Rule also clarifies, within the *Rules* compliance audit language, that the failure of a DFI to provide NACHA with proof of completion of 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.

IMPACT TO PARTICIPANTS

All DFIs must complete an annual compliance audit to ensure they are complying with the *Rules*. Any DFIs that identify gaps or shortcomings in their current audit procedures will need to expand the scope of their *Rules* compliance audits to comply with these revised provisions.

TECHNICAL SUMMARY

Below is a summary of the impact of this rule change on the *NACHA Operating Rules*. Sections of the *Rules* that are affected by this amendment follow later within this document and reflect rule language as it will read upon implementation.

- *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 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 audit section governing RDFIs 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.

Implementation Date: This 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. (Note: Earlier adoption of these expanded audit provisions is encouraged for all DFIs in an effort to minimize potential risk caused by the failure to comply with the *Rules*.)

* * * * *

As approved February 17, 2009, effective December 18, 2009, the current Rules will be modified as follows for the Rules Audit Enhancement changes to the Rules:

Appendix Eight - Rule Compliance Audit Requirements

■ *[As of December 18, 2009, the current Appendix Eight governing audit requirements will be removed from the Rules and replaced with the following Appendix Eight.*

Participating DFIs must comply with all provisions of these rules and conduct an audit of such compliance on an annual basis. A Participating DFI’s audit obligation is not limited to compliance with any specific rule or group of rules, and the descriptions of rules contained within this Appendix Eight are not intended to modify or limit the language of the rules themselves or the obligation of Participating DFIs to comply with, or to audit compliance with, such rules.

This Appendix Eight provides Participating DFIs and any Third-Party Service Providers performing functions of ACH processing on behalf of those DFIs with highlights of the most critical components of an audit of compliance with these rules. The requirements relate solely to compliance with these rules and do not address other audit considerations of a financial institution’s ACH policies, procedures or regulatory compliance. A Participating DFI may wish to audit other aspects of its ACH operations in conjunction with its annual rules compliance audit. These aspects could include OFAC compliance, ACH business continuity plans, ACH risk management policies, and compliance with 31 C.F.R. Part 210 and the Green Book for processing Federal Government ACH transactions.

SECTION 8.1 General Audit Requirements

Each Participating DFI, and any Third-Party Service Provider that provides ACH services to the Participating DFI, shall, in accordance with standard auditing procedures, conduct an internal or external audit of compliance with provisions of the ACH rules in accordance with the requirements of this Appendix Eight. These audit provisions do not prescribe a specific methodology to be used for the completion of an audit but identify key rule provisions that should be examined during the audit process. An annual audit shall be conducted under these Rule Compliance Audit Requirements no later than December 1 of each year. This audit shall be performed under the direction of the audit committee, audit manager, senior level officer, or independent (external) examiner or auditor of the Participating DFI or Third-Party Service Provider. The Participating DFI and its Third-Party Service Provider must retain proof that they have completed an audit of compliance in accordance with these rules. Documentation supporting the completion of an audit must be (1) retained for a period of six years from the date of the audit, and (2) provided to the National Association upon request. Failure of a Participating DFI to provide proof of completion of an audit according to procedures determined by the National Association may be considered a Class 2 rule violation pursuant to Appendix Eleven, subsection 11.3.7 (Fines and Penalties).

SECTION 8.2 Audit Requirements for All Participating DFIs

All Participating DFIs and their Third-Party Service Providers shall 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.

- A. Verify that records of entries, including return and adjustment entries, transmitted from or to an ACH Operator are retained for six years from the date the entry was transmitted. Verify that a printout or reproduction of the information relating to the entry can be provided to the Participating DFI's customer or any other Participating DFI or ACH Operator that originated, transmitted, or received the entry. (Article One, Subsection 1.7.1)
- B. When electronic records are used, verify that such records (1) accurately reflect the information contained within the record, and (2) are capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise. (Article One, Subsection 1.7.2)
- C. Verify that the Participating DFI completed an audit of its compliance with the rules in accordance with this Appendix Eight for the previous year. Verify that the Participating DFI has addressed all issues raised during the previous audit. (Article One, Subsection 1.2.1)
- D. Verify that required encryption is used for banking information transmitted via an Unsecured Electronic Network. (Article One, Section 1.6)
- E. Verify that the Participating DFI has reported and paid to the National Association all annual fees and per-entry fees for each commercial, inter-bank or Federal Government Entry that is transmitted or received by the Participating DFI, including those Entries that are not processed through an ACH Operator but are exchanged with another non-affiliated Participating DFI (i.e., direct send entries). (Article One, Section 1.3)

SECTION 8.3 Audit Requirements for RDFIs

In addition to the audit procedures outlined in Sections 8.1 (General Audit Requirements) and 8.2 (Audit Requirements for All Participating DFIs) of this Appendix Eight, all RDFIs and their Third-Party Service Providers shall conduct an audit of the following relating to the receipt of ACH entries:

- A. Verify that prenotifications received are for valid accounts and that when a prenotification is not processable or is erroneous, the prenotification is rejected on a timely basis through the use of return entry procedures or that changes are requested through the Notification of Change procedure. (Article Four, Subsection 4.1.2)
- B. Verify that, if the RDFI chooses to initiate Notifications of Change, such entries are transmitted within two banking days of the Settlement Date of the entry to which the NOC relates, with the exception of NOCs due to merger, acquisition, or other similar events. (Article Six, Subsection 6.3.1)
- C. Verify that, subject to the RDFI's right of return, all types of ACH entries and prenotifications are accepted. Verify that the RDFI handles XCK entries and entries to non-transaction accounts appropriately. (Article Four, Subsection 4.1.3; Article Six, Subsection 6.1.3)
- D. Verify that funds from ACH credit entries are made available to the Receiver for withdrawal or cash withdrawal on Settlement Date. In the case of PPD credit entries made available to the RDFI by 5:00 p.m. local time on the banking day prior to the Settlement Date, ensure that funds are made available to the Receiver for withdrawal or cash withdrawal no later than the opening of business on the Settlement Date and that debit entries are not posted prior to the Settlement Date. (Article Four, Subsections 4.4.1 and 4.4.2)

- E. *For Consumer Accounts, verify that the RDFI sends or makes available the minimum descriptive information concerning each credit or debit entry consistent with the requirements of Appendix Four (Minimum Description Standards). (Article Four, Section 4.5; Appendix Four, Section 4.1)*

For non-Consumer Accounts, verify that the RDFI sends or makes available to each of its Receivers the contents of the Check Serial Number Field within each ARC, BOC, and POP entry. (Article Four, Section 4.5; Appendix Four, Section 4.2)

- F. *For all entries except RCK:*

Verify that returned entries (including debit entries to a corporate account returned as unauthorized) are received by the RDFI's ACH Operator by its deposit deadline for the return entry to be made available to the ODFI no later than the opening of business on the second banking day following the Settlement Date of the original entry. (Article Six, Subsection 6.1.2)

Verify that permissible return entries (i.e., the late return of unauthorized debit entries to non-Consumer Accounts) are transmitted with the permission of the ODFI and utilize the appropriate Return Reason Code. (Article Eight, Section 8.3; Appendix Five)

Verify that dishonored return entries received by the RDFI are handled appropriately, and that contested dishonored return entries and corrected returns are initiated in a timely manner. (Article Six, Subsections 6.2.2 and 6.2.4; Appendix Five)

Verify that the RDFI utilizes Return Reason Codes and Contested Dishonored Return Reason Codes that accurately describe the reason for the return. (Appendix Five, Section 5.4)

- G. *Verify that the return of an RCK entry is transmitted to the RDFI's ACH Operator by midnight of the second banking day following the banking day of receipt of the presentment notice. (Article Two, Subsection 2.8.4)*

- H. *Verify that a return for any credit entry returned to the RDFI by the Receiver is transmitted to the RDFI's ACH Operator by midnight of the banking day following the banking day of the RDFI's receipt of the entry from the Receiver. Also verify that the RDFI returns all credit entries that are not credited or otherwise made available to its Receivers' accounts by midnight of the banking day following the Settlement Date. (Article Six, Subsections 6.1.4, 6.1.5)*

- I. *Verify that, when the RDFI has agreed to do so, it has returned or adjusted an entry in response to an ODFI's request for the return or adjustment of an erroneous entry initiated by the ODFI (R06). (Article Eight, Section 8.2)*

- J. *Verify that, for consumer entries except ARC, BOC, POP, RCK, TEL, and Single Entry WEB entries, the RDFI has acted on stop payment orders placed with the RDFI at least three banking days prior to the scheduled date of the transfer. For corporate entries, as well as for ARC, BOC, POP, RCK, TEL, and Single Entry WEB entries, verify that the RDFI has acted on stop payment orders that have been received in such time and in such manner that allow the RDFI to act on the stop payment order prior to acting on the debit entry. Verify that the RDFI is aware that Return Reason Code R08 can be used with any Standard Entry Class Code that carries dollar value. (Article Eight, Sections 8.4, 8.5; Appendix Five)*

Verify that the RDFI uses Return Reason Codes R38 (Stop Payment on Source Document) and R52 (Stop Payment on Item) properly. Verify that, for each RCK entry for which a stop payment has been placed on the item to which the RCK entry relates and for each ARC or BOC entry for which a stop payment order has been placed on the source document to which the ARC or BOC entry relates, the adjustment entry is received by the RDFI's ACH Operator by its deposit deadline for

the adjustment entry to be made available to the ODFI no later than the opening of business on the banking day following the sixtieth calendar day following the Settlement Date of the original entry. (NOTE: No written statement under penalty of perjury is required for entries returned for these reasons.) (Article Eight, Subsections 8.7.3 and 8.7.4; Appendix Five)

- K. Verify that written statements under penalty of perjury are obtained from consumers for all returns bearing Return Reason Codes R05, R07, R10, R37, R51, and R53, and that each adjustment entry is received by the RDFI's ACH Operator by its deposit deadline for the adjustment entry to be made available to the ODFI no later than the opening of business on the banking day following the sixtieth calendar day following the Settlement Date of the original entry. Verify that copies of written statements under penalty of perjury are provided to the ODFI within the required time frame, when such copies are requested, in writing, by the ODFI. (Article Eight, Section 8.6; Appendix Five)
- L. Verify that the RDFI has provided the Receiver with proper notice to ensure compliance with UCC Article 4A with respect to ACH transactions. (Article Two, Subsection 2.1.11)
- M. Verify that, when requested to do so by the Receiver, the RDFI provides all payment-related information transmitted with CCD, CIE, CTX, and IAT entries to the Receiver by the opening of business on the second banking day following the Settlement Date of the entry. (Article Four, Subsection 4.4.3)

SECTION 8.4 Audit Requirements for ODFIs

In addition to the audit procedures outlined in sections 8.1 (General Audit Requirements) and 8.2 (Audit Requirements for All Participating DFIs) of this Appendix Eight, ODFIs and their Third-Party Service Providers shall conduct an audit of the following relating to the origination of ACH entries:

- A. Verify that agreements have been made with all Originators (corporate customers) or Third-Party Senders that bind the Originator or Third-Party Sender to these rules, and 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. With respect to IAT entries, verify that agreements contain all necessary provisions. (Article Two, Subsection 2.1.1)
- B. Verify that, if applicable, agreements have been made with all Sending Points originating transactions on behalf of the ODFI. (Article Two, Subsection 2.2.1.11)
- C. Verify that exposure limits are established for each corporate Originator or Third-Party Sender, that these procedures provide for the exposure limits to be reviewed periodically, and for entries initiated by these Originators or Third-Party Senders to be monitored relative to the exposure limits across multiple settlement dates. (Article Two, Subsection 2.1.12)
- D. For IAT entries, verify that the ODFI monitors the payments system risk associated with the initiation of such entries by each Originator or Third-Party Sender. (Article Two, Subsection 2.1.12)
- E. For WEB entries, verify that the ODFI has (1) established procedures to monitor the credit-worthiness of each Originator or Third-Party Sender on an on-going basis, (2) established an exposure limit for that Originator or Third-Party Sender, (3) implemented procedures to review that exposure limit periodically, and (4) implemented procedures to monitor entries initiated by that Originator or Third-Party Sender relative to its exposure limit across multiple settlement dates. (Article Two, Subsection 2.12.2.3)
- F. Verify that the ODFI accepts return entries that comply with Appendix Five of these rules and are transmitted by the RDFI within the time limits established by these rules. Verify that the ODFI informs the Originator of returned entries in a proper manner. Verify that dishonored return entries are transmitted within five banking days after the 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. (Article Six, Subsections 6.1.6, 6.2, and 6.2.2)
- G. Verify that information relating to NOCs and Corrected NOCs is provided to each Originator or Third-Party Sender within two banking days of the Settlement Date of the NOC or Corrected NOC in accordance with Appendix Six (Notification of Change). Verify that refused NOCs are transmitted within fifteen (15) days of receipt of an NOC or corrected NOC. (Article Six, Subsection 6.3.2 and Section 6.4)
- H. With the exception of IAT entries to non-Consumer Accounts, CCD entries, CTX credit entries, and XCK debit entries, verify that the ODFI responds to an RDFI's request for a copy of an authorization within ten (10) banking days at no charge. (Article Four, Subsection 4.1.1)
- I. Verify that, when agreed to by the ODFI, Permissible Return Entries are accepted in accordance with Article Eight, section 8.3 (ODFI Agrees to Accept CCD or CTX Return). (Article Eight, Section 8.3)
- J. Verify that the ODFI has provided the Originator with proper notice to ensure compliance with UCC Article 4A with respect to ACH transactions. (Article Two, Subsection 2.1.10)
- K. Verify that the ODFI has utilized a commercially reasonable method to establish the identity of each Originator or Third-Party Sender that uses an Unsecured Electronic Network to enter into a contractual relationship with an ODFI for the origination of ACH transactions. 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 establish the identity of each Originator that uses an Unsecured Electronic Network to enter into a contractual relationship with the Third-Party Sender for the origination of ACH transactions. (Article Two, Subsection 2.2.1.7)
- L. Verify that Reversing Entries and Reversing Files are originated in accordance with the requirements of these rules. (Article Two, Subsections 2.4 and 2.5)
- M. For BOC entries, verify that the ODFI has (1) employed commercially reasonable procedures to verify the identity of each Originator or Third-Party Sender transmitting such entries, and (2) established 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. (Article Two, Subsections 2.10.3.1, 2.10.3.2 and 2.10.3.3)
- N. Verify that the ODFI has reported information on each Originator or Third-Party Sender, as requested by the National Association. (Article Two, Section 2.18)
- O. Verify that the ODFI has kept Originators and Third-Party Senders informed of their obligations under these rules.]

Appendix Eleven - Rules Enforcement – Section 11.1 (Scope)

SECTION 11.1 Scope

Appendix Eleven governs the rules enforcement procedures to be applied in the event of (1) an ACH rules violation, including a breach of warranty under these rules, filed against a Participating DFI by a party to a transaction, or (2) the identification of a return rate for unauthorized entries by an Originator or Third-Party Sender that exceeds a defined threshold. [Appendix Eleven governs the rules enforcement procedures to be applied in the event of (1) an ACH rules violation, including a breach of warranty under these rules,

- *filed against a Participating DFI by a party to a transaction, (2) the identification of a return rate for unauthorized entries by an Originator or Third-Party Sender that exceeds a defined threshold, or (3) the failure of a Participating DFI to comply with a direct obligation to the National Association, as defined by these rules.]*

This Appendix Eleven (1) defines the criteria under which a rules enforcement proceeding may be initiated for any violation of these rules; and (2) establishes the parameters under which the National Association may undertake specific actions with respect to the monitoring and reporting of activity causing potential harm to Participating DFIs or the ACH Network.

The purpose of these enforcement mechanisms is to maintain the quality of ACH services and the satisfaction of Participating DFIs and their customers by promoting compliance with these rules and reducing the risks to Participating DFIs and their customers by limiting the number of unauthorized entries.

Appendix Eleven - Rules Enforcement – Subsection 11.3.1 (Initiation of a Rules Enforcement Proceeding)

SUBSECTION 11.3.1 Initiation of a Rules Enforcement Proceeding

A rules enforcement proceeding may be initiated for any violation of these rules. A rules enforcement proceeding may be conducted by the National Association in response to an ACH rules violation, including a breach of warranty under these rules, filed against a Participating DFI. The complainant must be a party to the transaction. A rules enforcement proceeding initiated by a party to the transaction must comply with the requirements of subsection 11.3.2 (Submission Requirements for Rules Enforcement Proceedings Initiated by a Party to the Transaction.) The Report of Possible ACH Rules Violation Form and filing instructions are located in Section IV, Chapter VI (Rules Enforcement) of the NACHA Operating Guidelines.

- A rules enforcement proceeding may also be initiated and conducted by the National Association in response to a violation of unauthorized entries pursuant to section 11.2 (ODFI Reporting Requirements) of this Appendix Eleven. *[A rules enforcement proceeding may also be initiated and conducted by the National Association in response to (1) a violation of unauthorized entries pursuant to section 11.2 (ODFI Reporting Requirements) of this Appendix Eleven, or (2) the failure of a Participating DFI to comply with a direct obligation to the National Association, as defined by these rules.]* A rules enforcement proceeding initiated by the National Association must comply with the requirements of subsection 11.3.3 (Submission Requirements for Rules Enforcement Proceedings Initiated by the National Association).

Appendix Eleven - Rules Enforcement - Subsection 11.3.3 (Submission Requirements for Rules Enforcement Proceedings Initiated by the National Association)

SUBSECTION 11.3.3 Submission Requirements for Rules Enforcement Proceedings Initiated by the National Association

Each rules enforcement proceeding initiated by the National Association must contain the following information and conform to the following requirements:

- a copy of the National Association's written request for information pursuant to section 11.2.1 (National Association Request for Information) of this Appendix Eleven; and *[Effective December 18, 2009, this bullet point will be removed from the Rules.]*
- a statement outlining the reason(s) for the initiation of a rules enforcement proceeding:

- (1) the ODFI failed, within the required timeframe, to provide the National Association with complete and accurate information as required by Article Two, Section 2.18 (ODFI Reporting Requirements);
- (2) the information provided by the ODFI substantiates the claim that the Originator or Third-Party Sender exceeded the return rate for unauthorized entries and the ODFI has failed to reduce the Originator's or Third-Party Sender's return rate for entries returned as unauthorized to a rate below the return threshold for unauthorized entries within sixty (60) days after receipt of the National Association's written request, pursuant to Article Two, section 2.18 (ODFI Reporting Requirements);
- (3) the information provided by the ODFI substantiates that the Originator's or Third-Party Sender's return rate for unauthorized entries exceeded the return rate, and the ODFI successfully reduced the return rate to below the return threshold within the 60-day time period, but the ODFI failed to maintain the return rate below the return threshold for 180 additional days; or

■ *[(4) the Participating DFI failed to comply with a direct obligation to the National Association, as defined by these rules;]*

■ *[• for a rules enforcement proceeding initiated in response to a violation of unauthorized entries pursuant to section 11.2 (ODFI Reporting Requirements) of this Appendix Eleven, a copy of the National Association's written request for information pursuant to section 11.2.1 (National Association Request for Information) of this Appendix Eleven.]*

A rules enforcement proceeding initiated by the National Association must be submitted within ninety (90) days of the occurrence of the rule violation(s) asserted.

Appendix Eleven - Rules Enforcement – Subsection 11.3.7.4 (Class 2 Rules Violation)

SUBSECTION 11.3.7.4 Class 2 Rules Violation

A Class 2 Rules Violation is one in which:

- (1) the Participating DFI has not responded to either the Notice of Possible ACH Rules Violation or the Notice of Possible Fine;
- (2) the Participating DFI responds to either notice that it does not intend to correct the rules violation;
- (3) the Participating DFI (i) fails to respond completely and accurately, within the proper time frame, to the National Association's request for information in accordance with the requirements of Article Two, section 2.18 (ODFI Reporting Requirements); (ii) substantiates the claim that the Originator or Third-Party Sender exceeded the return rate for unauthorized entries and the ODFI has failed to reduce the Originator's or Third-Party Sender's return rate for entries returned as unauthorized to a rate below the return threshold for unauthorized entries within sixty (60) days of receipt of the National Association's written request; or (iii) substantiates that the Originator's or Third-Party Sender's return rate for unauthorized entries exceeded the return rate, and the ODFI successfully reduced the return rate to below the return threshold within the 60-day time period, but the ODFI failed to maintain the return rate below the return threshold for 180 additional days. The Panel may consider the Originator's or Third-Party Sender's volume of debit entries as an extenuating circumstance in determining whether a violation under this provision constitutes a Class 2 Rules Violation.

■ (4) *[the Participating DFI fails to provide the National Association with proof of completion of a rules compliance audit, as required by Appendix Eight (Rules Compliance Audit Requirements);]*

- (5) the ACH Rules Enforcement Panel determines the time frame and Resolution Date asserted by a Participating DFI as necessary to resolve the problem causing the rules violation are excessive;
- (6) the National Association believes that the violation causes excessive harm to one or more Participating DFIs or the ACH Network; or
- (7) it is the fourth or subsequent recurrence of the same rules violation.

In situations involving a Class 2 Rules Violation, the ACH Rules Enforcement Panel may levy a fine against the respondent Participating DFI in an amount up to \$100,000 per month until the problem is resolved. Where the violation relates to a specific Originator or Third-Party Service Provider at the DFI, a separate monthly fine may be assessed to the DFI with respect to each such Originator or Third-Party Service Provider.

NACHA OPERATING GUIDELINES

This Supplement #1-2009 updates the *NACHA Operating Guidelines* related OFAC compliance. NACHA developed recommendations and guidance for Gateway Operators and RDFIs for processing inbound IAT debits in accordance with OFAC requirements. This guidance, which was originally issued in December 2008, was in response to a number of requests that NACHA had received from ACH Network participants that are considering how they will handle such debits, and that wish to do so in a manner that is as automated as possible.

Effective March 5, 2009, OFAC revised its requirements and expectations regarding the handing of inbound IAT debits. As a result, NACHA's previous guidance on processing inbound IAT debits, which was designed to meet OFAC's original expectations, is no longer valid. The following guidance replaces that found in Section IV, Chapter IV – "OFAC Compliance" of the 2009 *NACHA Operating Guidelines*.

Effective immediately, the NACHA Operating Guidelines will be modified as follows to provide revised guidance related to OFAC compliance:

SECTION IV—SPECIAL TOPICS

CHAPTER IV OFAC COMPLIANCE

A. INTRODUCTION

The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) administers economic sanctions and embargo programs that require assets and transactions involving interests of target countries, target country nationals, and other specifically identified companies and individuals be frozen. For purposes of OFAC compliance, these entities are referred to as "Specially Designated Nationals and Blocked Persons." OFAC maintains and regularly updates a master list (SDN List) identifying known "blocked parties."

All of the sanctions programs enforced by OFAC involve declarations of national emergency by the President of the United States. As with all payment mechanisms, the ACH Network is subject to the requirement to comply with OFAC-enforced sanctions policies.

Who is subject to OFAC? All U.S. citizens and permanent resident aliens, companies located in the U.S., overseas branches of U.S. companies, and, in some cases, overseas subsidiaries of U.S. companies fall under OFAC jurisdiction. In terms of the ACH Network, this means that all U.S. ACH participants, including Originators, Originating Depository Financial Institutions (ODFIs), Receiving Depository Financial Institutions (RDFIs), Receivers and third-parties need to be aware that they can be held accountable for sanctions violations by the U.S. Government and must understand their compliance obligations.

B. SCOPE OF COVERAGE

OFAC responsibilities for a financial institution vary depending on whether the transaction is considered domestic or international. This Chapter is divided into two sections Domestic ACH OFAC Obligations and International ACH OFAC Obligations.

C. DOMESTIC ACH OFAC OBLIGATIONS

In September 1997, the *NACHA Operating Rules* were amended to require that Originator/ODFI agreements include an acknowledgment by the Originator that ACH transactions it originates comply with the laws of

the United States (“NACHA Rule”). The effect of this rule change is to focus financial institution liability for inadvertent processing of a domestic ACH transaction in violation of OFAC-enforced sanctions policies on the financial institution holding the account of the blocked party.

D. IMPACT TO ACH NETWORK PARTICIPANTS FOR DOMESTIC ACH TRANSACTIONS

1. ORIGINATORS

Domestic Originators should be aware that they are subject to applicable U.S. law, including OFAC-enforced sanctions, when initiating ACH entries. Foreign Originators initiating transactions with a financial institution that is under U.S. jurisdiction similarly must be aware that the institution is subject to OFAC-enforced sanctions. Originators in either category should not be acting on behalf of, or transmitting funds to or from, any blocked party subject to OFAC-enforced sanctions. Agreements between ODFIs and Originators should include a statement that the Originator acknowledges that it may not initiate ACH entries that violate the laws of the United States. Originators should be aware that they will be held to an obligation to originate only lawful ACH transactions under such agreements with their ODFIs. Originators of ACH transactions should also be aware that their ODFI may from time to time need to temporarily suspend processing of a transaction (particularly an international ACH transaction) for greater scrutiny or verification against the SDN List, and that this action may affect settlement and/or availability.

2. ODFIs

ODFIs that choose to originate ACH entries on behalf of their customers should be aware that both they and their Originators are subject to the *NACHA Operating Rules* and applicable U.S. law when transmitting these entries. ODFIs should make this obligation clear in their agreements with Originators. ODFIs processing international ACH transactions may also find it beneficial to include in their agreements a reference to possible delays in processing, settlement and/or availability of these transactions when the ODFI determines that enhanced scrutiny or verification may be necessary.

The NACHA Rule reflects the “Know Your Customer” principle that the ODFI will verify the Originator is not a blocked party and that a good faith effort will be undertaken to determine, through the normal course of business, that the Originator is not engaged in transmitting funds to, from, or on behalf of a party subject to a blocking action. If the ODFI encounters a transaction in the normal course of business initiated by an Originator that would violate OFAC-enforced sanctions, federal law requires the ODFI to comply with OFAC policies. Under U.S. law, the ODFI is responsible for freezing or rejecting the proceeds of illicit ACH transactions involving interests of blocked parties for whom the ODFI holds an account, or on whose behalf the ODFI is acting (which could include the Receiver or other parties to the transaction. As a depository financial institution, the ODFI should have a process in place to determine whether any of their account holders is identified as a blocked party in a current SDN List (see section on “Account Screening” below).

Origination Of Entries

With respect to domestic ACH transactions, by addressing the issues above, the ODFI may rely on the RDFI for compliance with OFAC policies when it is the RDFI that holds the account or is otherwise acting on behalf of a blocked person.

As noted above, the ODFI should address the Originator’s obligation to comply with U.S. laws in its origination agreement. The ODFI should also recognize that when unbundling “on us” transactions (i.e., the ODFI is also the RDFI for a transaction) from files received for processing from an Originator, it will need to review these transactions with greater scrutiny since it is servicing both sending and receiving sides.

Entries Violating OFAC Sanctions

Each ODFI should be aware that if it inadvertently transmits an unlawful ACH credit entry to a Receiver that is subject to OFAC sanctions, the RDFI holding the blocked party's account is obligated to post the credit entry to the Receiver's account, freeze the proceeds, and report the transaction to OFAC.

In the event that the ODFI inadvertently processes an unlawful ACH debit entry to a blocked account, the RDFI holding the blocked account (or an intermediary receiving point such as a correspondent or third-party processor able to identify the transaction), in compliance with OFAC policies, should return the entry in accordance with the NACHA Operating Rules using Return Reason Code R16 (Account Frozen). In this way, the proceeds do not leave the blocked account and the ODFI is informed of the reason.

If the ODFI is instructed to originate an ACH debit entry that it has reason to believe would be a violative transaction, NACHA has been advised that OFAC would prefer that the transaction be transmitted so that, if not returned or rejected by the RDFI, the proceeds from the transaction can be captured by the ODFI, frozen and reported to OFAC. See section on "Handling IAT Debit Processing" for more information.

See the section on "Blocking and Reporting" for more detail on the process required to block proceeds of a violative transaction and report to OFAC.

Identification Of Blocked Parties

As blocked parties and related transactions may be difficult to identify in the normal course of business, ODFIs may wish to become familiar with how to locate and interpret lists of specially-designated nationals and blocked persons subject to U.S. sanctions to facilitate OFAC compliance and avoid liability for monetary penalties. Consultation with counsel, audit/compliance staff, and/or wire transfer operations personnel – in addition to visiting and becoming familiar with the OFAC website at <http://www.treas.gov/ofac> -- is recommended. There are also several vendors of online or database SDN identification services that can assist financial institution reviews at the account level, including the new account set-up phase or reviewing existing accounts when new blocked parties are added to the SDN List.

3. RDFIs

RDFIs should be aware that they are subject to the requirements of the *NACHA Operating Rules* and applicable U.S. law when processing ACH entries. This includes the need to comply with OFAC enforcement policies in the event that the RDFI receives an ACH transaction being made to, from, or on behalf of any party subject to OFAC sanctions. As a depository financial institution, the RDFI should have a process in place to determine whether any of their account holders is identified as a blocked party in a current SDN List (see section on "Account Screening" below).

Receipt Of Entries

With respect to domestic ACH transactions, the RDFI is responsible for rejecting or freezing the proceeds of a transaction involving interests of a blocked party for whom the RDFI holds an account or on whose behalf the RDFI is acting.

Entries Violating OFAC Sanctions

In the event that an ODFI inadvertently transmits an unlawful ACH credit entry to a Receiver that is subject to OFAC sanctions, the RDFI holding the blocked party's account should post the credit entry to the account, ensure the account is frozen, and report the transaction to OFAC. In the event that an ODFI inadvertently transmits an unlawful ACH debit entry, the RDFI holding the account should ensure the account is frozen, report the transaction to OFAC, and return the entry in accordance with the NACHA Operating Rules using Return Reason Code R16 (Account Frozen) with advice that the entry was destined to an account frozen due to OFAC blocking action.

See the section on “Blocking and Reporting” for more detail on the process required to block proceeds of a violative transaction and report to OFAC.

Identification Of Blocked Parties

As blocked parties and related transactions may be difficult to identify in the normal course of business, RDFIs may wish to become familiar with how to locate and interpret lists of specially-designated nationals and blocked persons subject to U.S. sanctions to ensure compliance and avoid liability for sizeable monetary penalties. Consultation with counsel, audit/compliance staff, and/or wire transfer operations personnel is recommended.

4. RECEIVERS

Domestic Receivers (and those otherwise under U.S. jurisdiction) are subject to U.S. law, including OFAC sanctions, and should be aware that their financial institutions are subject to both U.S. law and the *NACHA Operating Rules* when handling ACH transactions on their behalf. This may involve delays in posting, settlement and the availability of proceeds – particularly for ACH transactions initiated by parties outside U.S. jurisdiction – if an RDFI finds it necessary to scrutinize a transaction in more detail. In the rare case where there appears to be a violation of U.S. sanctions policies, proceeds from an ACH credit may be frozen and therefore unavailable to the Receiver pursuant to a blocking action. For violative ACH debits, Receivers may have the proceeds debited from their account and frozen by either the RDFI or the ODFI pursuant to a blocking action.

Receivers wishing to dispute funds frozen in a blocking action should review the section on “BLOCKING & REPORTING” and/or the OFAC website for the procedures and form required to seek a release of funds [Form TD-F 90-22.54; Application for the Release of Blocked Funds].

5. THIRD-PARTIES

Third-parties (including processors and correspondent/respondent banks) should recognize that OFAC sanctions enforcement applies to their role as it would the party they are acting on behalf of. For example, a third-party acting on behalf of a number of downstream corporate Originators should recognize that its ODFI will hold it accountable for ensuring that ACH transactions it introduces into the domestic ACH Network comply with U.S. law. This means that the ODFI has to rely on the third party to police downstream parties for which it is acting.

Similarly, a domestic respondent bank/RDFI receiving ACH transactions through a correspondent bank should not automatically assume that its correspondent will have intercepted and frozen any violative transactions it has processed on the respondent’s behalf. While there may be some attention focused on the correspondent in the event of a violative transaction being passed through, the correspondent serving the RDFI is not in much of a position to verify the identity of the RDFI’s accountholder (or the ODFI’s Originator) on a particular ACH transaction.

E. INTERNATIONAL ACH OFAC OBLIGATIONS

With the addition of the IAT SEC code and rules to the *NACHA Operating Rules*, financial institutions will need to revise their ACH OFAC compliance policies to include the processing and handling of IAT transactions. In a letter from OFAC to NACHA dated November 9, 2004, OFAC outlined their expectations for both the ODFI and RDFI. “U.S. RDFIs and beneficiaries will continue to have an obligation to ensure that all aspects of inbound, cross-border transactions are in compliance with OFAC regulations and to take appropriate steps to investigate, suspend, reject, block and report on transactions as necessary.” “U.S. ODFIs and their Originators will continue to be responsible for ensuring that all parties to the transactions, as well as the underlying purpose of the transactions, are not in violation of OFAC regulations, and they will need to take appropriate steps to investigate, suspend, reject, block, and report on transactions.”

F. DEMONSTRATING OFAC COMPLIANCE

For a financial institution to demonstrate OFAC compliance, it must have a clear and thorough ACH OFAC policy and procedures manual (or section on ACH OFAC policies and procedures in its OFAC policy and procedures manual), educate and train its employees on the new policies, and have a compliance system or procedure that allow for the proper handling of all transactions and customers. Some of the items that should be covered in the ACH OFAC policy are:

- Who is responsible for OFAC compliance;
- How the organization maintains an up-to-date listing of prohibited countries, organizations, and individuals (Detail how the organization obtains the information from OFAC and when);
- How specific transactions are handled (i.e. debits, credits);
- What information is checked against the “SDN” list;
- OFAC reporting procedures;
- Record retention; and
- OFAC compliance audit.

G. IMPACT TO ACH NETWORK PARTICIPANTS FOR INTERNATIONAL TRANSACTIONS

1. GATEWAY OPERATORS

The Gateway Operator is defined as either a financial institution or an ACH Operator that acts as the entry point to or exit point from the United States for IAT transactions. The capabilities and responsibilities vary between financial institution and ACH Operator.

ACH Operator Acting as a Gateway Operator

An ACH Operator acting as a Gateway Operator may process Outbound IAT debit and credit entries but may only process Inbound IAT credit entries and reversing debits. No Inbound IAT debit entries may be processed by an ACH Operator acting as a Gateway Operator.

An ACH Operator acting as a Gateway Operator must review all IAT transactions for OFAC compliance and populate the Gateway Operator OFAC Screening Indicator (Field 10 of the IAT Entry Detail Record) with the results of the review before passing the entry to the RDFI. The ACH Operator is not required to investigate any suspect transaction.

Financial Institution as a Gateway Operator

A financial institution acting as a Gateway Operator may process Inbound and Outbound IAT credit and debit transactions. The FI acting as a Gateway Operator must review the IAT transactions for OFAC compliance. Although populating the Gateway Operator OFAC Screening Indicator with the results of the scan is considered optional, it is considered a good business practice. OFAC has stated that the responsibility for investigating suspect IAT transactions may be passed to the RDFI, but within the *NACHA Operating Rules* the Gateway Operator has taken on the warranties and responsibilities of the ODFI. As such, the Gateway Operator warrants that all transactions originated are in compliance with U.S. law. To that end a financial institution acting as a Gateway Operator should investigate and clear any suspect IAT transactions before they are originated into the ACH Network. If an IAT debit transaction is found to be in violation of an OFAC sanctions policy, OFAC has stated that all processing should cease; that the Gateway Operator/ODFI is to notify OFAC within 10 days; and that the Gateway Operator should notify the Foreign Gateway Operator that the item has been rejected because it was in violation of U.S. law and should send a copy of the rejected transaction to the RDFI.

2. ORIGINATORS

Corporate Originators should be aware that they are subject to applicable U.S. law, including OFAC-enforced sanctions, when initiating ACH entries. Originators should not be acting on behalf of, or transmitting funds to or from, any blocked party subject to OFAC-enforced sanctions. Agreements between ODFIs and Originators should include a statement that the Originator acknowledges that they may not initiate ACH entries that violate the laws of the United States. Originators should be aware that they will be held to an obligation to originate only lawful ACH transactions under such agreements with their ODFIs. Originators of ACH transactions should also be aware that their ODFI may, from time to time, need to temporarily suspend processing of a transaction for greater scrutiny or verification against the SDN List, and that this action may affect settlement and/or availability.

3. ODFIs

ODFIs that choose to originate ACH entries on behalf of their customers should be aware that both they and their Originators are subject to the *NACHA Operating Rules* and applicable U.S. law when transmitting these entries. ODFIs should make this obligation clear in their agreements with Originators.

The ODFI is responsible for reviewing all IAT transactions for OFAC compliance prior to the items being released to the ACH Operator. All parties to the transactions should be reviewed including the name and physical address of the Originator and Receiver, the receiving bank name, identification and branch country code, and any remittance information in the Payment Related Information contained in the optional Remittance Information addenda record. If suspect transactions are identified during the review, the items should be investigated and cleared before the transactions are released to the ACH Operator. If the ODFI encounters a transaction initiated by an Originator that would violate OFAC-enforced sanctions, Federal law requires the ODFI to comply with OFAC policies. Under U.S. law, the ODFI is responsible for freezing or rejecting (depending on the specifics of the particular sanctions program) the proceeds of illicit ACH transactions involving interests of blocked parties.

See the section on “Blocking & Reporting” for more detail on the process required to block proceeds of a violative transaction and report to OFAC.

4. RDFIs

RDFIs should be aware that they are subject to the requirements of the *NACHA Operating Rules* and applicable U.S. law when processing ACH entries. This includes the need to comply with OFAC enforcement policies in the event that the RDFI receives an ACH transaction being made to, from, or on behalf of any party subject to OFAC sanctions. The RDFI is responsible for rejecting or freezing the proceeds of a transaction involving interests of a blocked parties.

Handling Violative Transactions

Credit Entries:

- If the RDFI receives an inbound unlawful IAT credit entry to a Receiver that is subject to OFAC sanctions, the RDFI holding the blocked party’s account should post the credit entry to the account, ensure the account is frozen, and report the transaction to OFAC.
- If the Originator of the IAT transaction is subject to OFAC sanctions the transaction should not be posted to the Receiver’s account, the funds should be suspended and the transaction reported to OFAC.

Debit Entries:

- If the RDFI receives a violative IAT debit transaction, the RDFI should investigate the transaction and, if it is found to be in violation of an OFAC sanction, should contact OFAC for guidance. OFAC will handle these transactions on a case by case basis.

There is no time limit for the resolution of the suspect transaction. The RDFI needs to ensure that it communicates with the ODFI on the resolution of the suspect transaction. See the section on “Blocking & Reporting” for more detail on the process required to block proceeds of a violative transaction and report to OFAC.

5. RECEIVERS

Receivers are subject to U.S. law, including OFAC sanctions, and should be aware that their financial institutions are subject to both U.S. law and the *NACHA Operating Rules* when handling ACH transactions on their behalf. This may involve delays in posting, settlement and the availability of proceeds – particularly for ACH transactions initiated by parties outside U.S. jurisdiction – if an RDFI finds it necessary to scrutinize a transaction in more detail. In the rare case where there appears to be a violation of U.S. sanctions policies, proceeds from an ACH credit may be frozen and therefore unavailable to the Receiver pursuant to a blocking action. For violative ACH debits, Receivers may have the proceeds debited from their accounts and frozen by the RDFI pursuant to a blocking action.

Receivers wishing to dispute funds frozen in a blocking action should review the section on “Blocking & Reporting” and/or the OFAC website for the procedures and form required to seek a release of funds [Form TD-F 90-22.54; Application for the Release of Blocked Funds].

6. THIRD-PARTIES

Third-parties (including processors and correspondent/respondent banks) should recognize that OFAC sanctions enforcement applies to their role as it would the party they are acting on behalf of. For example, a third-party acting on behalf of a number of downstream corporate Originators should recognize that its ODFI will hold it accountable for ensuring that ACH transactions it introduces into the domestic ACH Network comply with U.S. law. This means that the ODFI has to rely on the third-party to police downstream parties for which it is acting.

Similarly, a domestic respondent bank/RDFI receiving ACH transactions through a correspondent bank should not automatically assume that its correspondent will have intercepted and frozen any violative transactions it has processed on the respondent’s behalf. While there may be some attention focused on the correspondent in the event of a violative transaction being passed through, the correspondent serving the RDFI is not in much of a position to verify the identity of the RDFI’s account-holder (or the ODFI’s Originator) on a particular ACH transaction.

H. RECOMMENDED PROCEDURES FOR HANDLING OF INBOUND IAT DEBIT TRANSACTIONS

NACHA developed the following recommendations and guidance for Gateway Operators and RDFIs for processing inbound IAT debits in accordance with OFAC requirements, as revised on March 5, 2009.

Inbound IAT debit transactions are debits that are being originated into the U.S. ACH Network by U.S. financial institutions acting as Gateway Operators. Inbound IAT debit transactions will not be processed through the FedACH International Service. While a Gateway Operator is also, by definition, the ODFI for an inbound IAT debit, the recommendations here are intended to address the financial institution’s role as a Gateway Operator. Nothing here should be construed to apply to ODFIs for any transactions other than inbound IAT debits.

NACHA strongly encourages financial institutions that are considering serving as Gateway Operators to thoroughly understand OFAC requirements, transaction risks, and operational issues for various processing scenarios. Financial institutions should have well-thought-out business plans and should thoroughly understand the implications and responsibilities of implementing IAT debit transactions.

The recommendations and guidance contained within this section reflect the expectations of OFAC – they are not requirements of the *NACHA Operating Rules*. Financial institutions can always contact OFAC for guidance whenever appropriate.

1. REVISED OFAC REQUIREMENTS RELATED TO INBOUND IAT DEBITS

Under OFAC’s revised requirements, a Gateway Operator that identifies the presence of a blocked party in an inbound IAT debit should cease processing the entry, and should take several additional steps to report the hit to OFAC, the Foreign Gateway Operator, and the RDFI.

OFAC further expects that Gateway Operators’ notifications to RDFIs about OFAC hits will eventually take place through the ACH Network. NACHA will issue additional guidance when methods and procedures for these notifications are established.

2. GATEWAY OPERATOR (ODFI) RESPONSIBILITIES FOR INBOUND IAT DEBIT TRANSACTIONS

A financial institution acting as a Gateway Operator (ODFI) for Inbound IAT debits should:

- Review all Inbound IAT debits for OFAC compliance, including all parties to the transaction and all remittance data;
- Segregate any suspect transactions into an OFAC review module or queue;
- Populate the Gateway Operator OFAC Screening Indicator (Field 10, IAT Entry Detail Record) for clean transactions with “0.” (NOTE: This field is Optional under the *NACHA Operating Rules*, but its use is strongly encouraged);
- Rebalance original batch and file, if necessary, and send to ACH Operator (see section below on Gateway Operator Procedures for Rebalancing a Batch and File);
- Investigate suspect transactions:
 - a. For a suspect transaction **cleared** by the investigation:
 - i. Populate the Gateway Operator OFAC Screening Indicator (Field 10, IAT Entry Detail Record) for clean transactions with “0.” (NOTE: This field is Optional under the *NACHA Operating Rules*, but its use is strongly encouraged);
 - ii. Batch cleared transactions and send to the ACH Operator for normal processing and settlement.
 - b. For transactions **confirmed** as an OFAC hit:
 - i. Cease processing of the entry;
 - ii. Notify the Foreign Gateway Operator that the debit entry has been rejected and is in violation of U.S. law;
 - iii. Notify OFAC within 10 days;
 - iv. Notify the RDFI that the transaction destined for one of its customers has been rejected, and provide a copy of the transaction.

Under these processing guidelines, there should be no instances in which a Gateway Operator sends an inbound IAT debit in which there is a “1” in the OFAC Screening Indicator. All suspect transactions would either be cleared or processing would cease.

3. GATEWAY OPERATOR PROCEDURES FOR REBALANCING A BATCH AND FILE

ACH Operations software would rebalance the batch and file to include revisions to the following fields: Total Debit Entry Dollar Amount in Batch/File, Total Credit Entry Dollar Amount in Batch/File, Entry/Addenda Count and Entry Hash at both the Batch Control and File Control level and possibly the Batch Count and/or Block Count in the File Control Record.

4. RDFI RESPONSIBILITIES FOR INBOUND IAT DEBIT TRANSACTIONS

An RDFI should recognize that it may receive IAT debits and be prepared in advance to handle the IAT debits. The RDFI for Inbound IAT debits should:

- Review all incoming IAT debits for OFAC compliance;
(NOTE: Use of the Gateway Operator Screening Indicator field by the Gateway Operator is optional. An RDFI should not assume a transaction is clean because of the presence of a “0” in the Gateway Operator OFAC Screening Indicator (Field 10, IAT Entry Detail Record), or because of the absence of any indicator in this field. The RDFI should rely on the results of its own investigation.);
- Post clean transactions normally;
- Investigate any suspect IAT debits:
 - a. For a suspect transaction **cleared** by an investigation, post normally;
 - b. For a suspect transaction **confirmed** as an OFAC hit – contact OFAC directly. The Gateway Operator may have missed this transaction or the OFAC list may have been revised. OFAC will handle these situations on a case-by-case basis.

Under these processing guidelines, there should be no instances in which an RDFI receives an inbound IAT debit in which there is a “1” in the OFAC Screening Indicator. This does not relieve the RDFI of its obligation to screen the IAT debits that it receives and report SDN hits to OFAC.

If an RDFI receives notification from a Gateway Operator that an inbound IAT debit destined for one of its accounts has been rejected due to the presence of a blocked party (as described in Gateway Operator Responsibilities, section 5(b)(iv)), the RDFI should take appropriate due diligence measures.

I. DEBIT BLOCKS AND FILTERS

A number of financial institutions currently offer a debit block service to their corporate customers. For an IAT debit that is not in violation of an OFAC sanctions program, an IAT debit processed against an account with a debit block may be returned as unauthorized as with any other debit transaction. For an IAT debit that is in violation of an OFAC sanctions program, contact OFAC directly before the debit is returned. OFAC has indicated that it wants to address this issue on a case-by-case basis.

Remember: Any entry that is identified as a potential hit against the SDN list must be handled as an exception item, requiring investigation and closer examination by the RDFI. Such transactions may not be automatically returned by the RDFI.

J. IAT OFAC SCREENING INDICATOR

A financial institution should only use the OFAC Screening Indicators as a reference and not the final determining factor in an OFAC review. As in the wire transfer procedures, each financial institution that is party to the transaction is responsible for doing an OFAC review of the transaction. While the actual OFAC review of the transaction may be handled by a third-party, OFAC has been very clear that a financial institution may not contract away its legal liability for OFAC compliance.

Within the IAT Entry Detail Record, two fields have been identified as OFAC Screening Indicators. Field Ten is identified as the Gateway Operator OFAC Screening Indicator and Field Eleven is the Secondary OFAC Screening Indicator. These fields are optional and may or may not be populated. The Gateway Operator OFAC Screening Indicator indicates the results of a Gateway Operator screen for OFAC compliance. A value of “0” indicates that the Gateway Operator has not found a potential blocked party, as identified by OFAC on the list of SDN list. A value of “1” indicates the potential presence of a blocked party. [Field formatting - This field must be space filled if no screening has been conducted.]

IAT Transactions Coming into the U.S.

If the IAT transactions enter the U.S. ACH through the Federal Reserve FedACH International Service, Field Ten will be populated by the Federal Reserve as the Gateway Operator. If the IAT transaction enters the U.S. ACH through any other Gateway Operator, the decision to populate these fields is optional. If Field Ten has been populated, that information should not be changed, even if a suspect transaction has been reviewed and cleared. If a secondary party to the transaction does another OFAC review of the file, the results of the additional review should be placed in Field Eleven.

The Secondary OFAC Screening Indicator indicates the results of a Third-Party Service Provider screen for OFAC compliance. A value of “0” indicates that the Third Party Service Provider has not found a potential blocked party, as identified by OFAC on the SDN list. A value of “1” indicates the potential presence of a blocked party. [Field formatting: This field must be space filled if no screening has been conducted].

K. ACCOUNT SCREENING

The issue of screening accounts for the purpose of identifying any account-holding parties subject to blocking action is a critical one. Depository financial institutions and other enterprises with customers that make or receive financial or other trade transactions are accountable if their customers are blocked parties on the SDN List. OFAC makes the current SDN List available to the public through several accessible forms and channels (See section “For More Information”).

Some financial institutions have the capability to download this list directly into their account systems as changes are made to the list and/or on a periodic basis to ensure that the current version is being applied to review their account base and to verify new customers. There are also several vendors that have OFAC account-level screening solutions from which a wide range of services are available. Regardless of whether an internal or a third-party option is used, the objectives are the same:

- Running existing or new accountholder information against the SDN List to identify those accounts or applicants that involve the interests of a blocked party (resulting in a “hit”); and
- Reviewing information about a “hit” to establish whether the identification is valid, if necessary contacting OFAC for verification (caution: more “false” hits than “true” hits are likely, given close approximations in the names or aliases of individuals or companies on the SDN List with the names of legitimate individuals or companies); and, freezing and reporting to OFAC those accounts that are “true” hits.

L. BLOCKING AND REPORTING ACH TRANSACTIONS

Blocked accounts and proceeds associated with violative transactions should be held by the financial institution in an interest-bearing status. Transactions involving blocked parties should be reported via fax within ten days to OFAC’s Compliance Programs Division. The blocking report should include the name and telephone number of a contact at the reporting financial institution and, in the case of a frozen ACH credit, a copy of the payment instruction (e.g., the Company/Batch Header Record & Entry Detail Record).

Official OFAC reporting, recordkeeping and licensing procedures

Section VII of “Foreign Assets Control Regulations for the Financial Community” states¹ :

¹ U.S. Department of the Treasury, Office of Foreign Assets Control, “Foreign Assets Control Regulations for the Financial Community,” July 3, 2002, pp. 29-30. Current versions of this Guidance are available from OFAC at: <http://www.treas.gov/offices/eotffc/ofac/regulations/t11facbk.pdf>

VII. Reporting and Procedures

Reporting and Procedures Regulations (31 C.F.R. Part 501) OFAC now has a uniform requirement across all of its sanctions programs that records be maintained for five years.

Reports have also been standardized:

Reports on Blockings and Reject Items – Blocking reports must be filed within ten days of blocking. They preferably should be tele-transmitted to OFAC’s Compliance Programs Division at 202/622-2426 and must identify: the owner or account party, the property, the property’s location, any existing or new account number or similar reference necessary to identify the property, actual or estimated value, the date it was blocked, a photocopy of the payment or transfer instructions (if blocking involves a payment or transfer of funds), a confirmation that the payment has been deposited into a new or existing blocked account which is clearly identifying the interest of, the individual or entity subject to blocking, the name and address of the holder, and the name and telephone number of a contact person from whom compliance information can be obtained. Reports on reject items must be filed within 10 days and include: the name and address of the transferee financial institution, the date and amount of transfer, a photocopy of the payment or transfer instructions received, the basis for rejection, and the name and telephone number of a contact person at the transferee financial institution from whom compliance information can be obtained.

Annual reports on Blocked Property – OFAC requires the filing of a comprehensive annual report on blocked property held as of June 30 by September 30 each year. The report is being filed using Form TDF 90-22.50 which is available from OFAC’s fax-on-demand service or electronically by clicking on the GPO ACCESS button on OFAC’s Home page or going directly to The Federal Bulletin Board and accessing OFAC’s extended electronic information reading room, the FAC_MISC file library. Requests to submit the information in an alternative format or for an extension of the reporting deadline are invited and will be considered on a case-by-case basis by OFAC.

Reports on litigation, arbitration and dispute resolution proceedings – U.S. persons involved in litigation, arbitration, or other binding alternative dispute resolution proceedings regarding blocked property must: provide notice of such proceedings to OFAC Chief Counsel, submit copies of all documents associated with such proceedings within 10 days of their filing to OFAC Chief Counsel at U.S. Treasury Department, 1500 Pennsylvania Ave., NW – 3123 Annex, Washington, DC 20220, and fax information about the scheduling of any hearing or status conference to OFAC Chief Counsel at 202/622-1911.

Licensing requests – License applications are not accepted by fax or electronically, unless specifically authorized. Most applications may be submitted in letter format, with the exception of license applications for the unblocking of fund transfers. Applications for the unblocking of fund transfers must be submitted using TD-F 90-22.54, “Application for the Release of Blocked Funds,” accompanied by two complete copies of the entire submission. The form, which requires information regarding the date of the blocking, the financial institutions involved in the transfer, and the beneficiary and the amount of the transfer, may be obtained from the OFAC Internet Home Page: <http://www/treas.gov/ofac> and the OFAC fax-on-demand service: 202/622-0077. Any person having an interest in a transaction or proposed transaction may file an application for a license authorizing the transaction. For individuals, if U.S., inclusion of a social security number is recommended but not required. For corporations or other entities, the application should include a principal place of business, the state of incorporation or organization, and, if U.S., a taxpayer identification number. Applications should be sent to the Licensing Division, Office of Foreign Assets Control, 1500 Pennsylvania Avenue, N.W., Annex 2, Washington, D.C. 20220.

For More Information

The OFAC compliance manual specific to the financial community is available on the OFAC website at: <http://www.treas.gov/offices/eotffc/ofac/regulations/t11facbk.pdf>

OFAC reporting forms -- including the appropriate forms for reporting blocked or rejected transactions, annual report of blocked property, and a request for release of blocked funds -- are available online at: <http://www.treas.gov/offices/eotffc/ofac/forms/index.html>

ACH Network participants are encouraged to check with OFAC regularly to determine whether blocked parties have been added to the SDN List, or whether other modifications to the sanctions programs have taken place. OFAC's Compliance Hotline may be reached at (800) 540-OFAC. OFAC also maintains a comprehensive website of compliance information, a current SDN List, and links to other information referenced above on its homepage at: <http://www.treas.gov/offices/eotffc/ofac/>

Finally, OFAC now has an e-mail alert service advising recipients of changes as they are approved. To subscribe (no charge), go to: <http://www.treas.gov/offices/eotffc/ofac/subscribe.html> and enter your e-mail address to be added to the "OFAC Financial Operations Bulletin E-mail List."