Understanding New ACH Network Anti-Fraud Rules

By **Aisha Hall** (October 23, 2024)

Aisha Hall

Fraud in the payments space is nothing new. In fact, it is fairly pervasive across the now-numerous available payment systems.

And despite the clear benefits of faster payments, the advent of faster, more easily accessible methods of payment has given rise to new opportunities for bad actors to commit fraud.

From bill payment and payroll, to the behind-the-scenes funds-settlement mechanisms of various payment applications we use daily, one of the primary payment systems used by consumers and businesses alike is the Automated Clearing House network.

The National Automated Clearing House Association, or NACHA, establishes the rules governing the ACH network. In March, NACHA voted on and approved 15 amendments to the rules, including several revisions that are intended to strengthen the ACH network participants' ability to detect potential fraud and efficiently recover funds in the event that fraud does take place.[1]

Several of these so-called risk management topics went into effect on Oct. 1, while others that may require more lead time from a technical perspective have staggered effective dates over the next few years.

Understanding the requirements and the opportunities presented by these new risk management topics is critical for financial institutions and corporations alike. Below is a high-level summary of the new risk management topics.

Expanded Use Cases of the R06 and R17 Return Reason Codes

When a financial institution receives a debit or credit entry from another financial institution through the ACH network, the rules permit the receiving depository financial institution, or RDFI, to return that entry to the originating depository financial institution, or ODFI, in certain circumstances.

The RDFI must follow explicit parameters set forth in the rules surrounding the return of these ACH entries, including that a return reason code, identifying the reason for the return, be attached to the returned entry.

The new revisions to the R06 and R17 return reason codes provide ODFIs and RDFIs with more discretion regarding the return of entries they suspect to be fraudulent.

The R06 return reason code was previously used when an ODFI requested the return of an entry that was either an erroneous entry — which is narrowly defined — or when a credit entry was initiated without the authorization of the party originating the entry.[2]

The new revision to the rules is being implemented in two phases: Phase 1, effective Oct. 1, permits ODFIs to request a return from the RDFI for any reason at all, including suspected fraud.[3] Phase 2, effective April 1, 2025, will require that RDFIs provide a response to the ODFI regarding the requested return within 10 banking days of their receipt of the ODFI's

request.[4]

Importantly: (1) The RDFI still maintains sole discretion in deciding whether to initiate the requested R06 return; (2) the ODFI still indemnifies the RDFI for such requested returns; and (3) there are no specific time constraints pertaining to a requested R06 return.

The R17 return reason code was previously used by RDFIs to return debit or credit entries that (1) it could not process; (2) contained an invalid account number and that the RDFI suspected were initiated under questionable circumstances; or (3) the RDFI or the account holder that received the entry identified as being an improper reversal of an entry.

As revised, RDFIs may now use R17 to return entries they believe to be "initiated under questionable circumstances" without requiring that there also be an error with the account number. This went into effect on Oct. 1,[5] and includes entries transmitted without the originator's authorization and entries that are originated under false pretenses, as defined below.

RDFIs exercising this right must do so within the applicable time frame and must include the descriptor "QUESTIONABLE" in the return addenda of the ACH file.[6]

Financial institutions should ensure their internal procedures reflect the new use cases of R06 and R17, and corporations should get educated about their additional avenues for requesting and initiating returns through their financial institution.

Additional Funds Availability Exceptions

Previously, the rules allowed an RDFI to delay funds availability of ACH credits to a receiver if the RDFI reasonably believed it was an unauthorized credit entry, e.g., in the event of an account takeover of an originator's account.[7]

As revised, and subject to applicable law, the rules will now also allow an RDFI to delay funds availability if it reasonably believes that a credit was unlawful, suspicious or otherwise sent under false pretenses. This is effective as of Oct. 1.[8]

The revised rules define "false pretenses" as "the inducement of a payment by a Person misrepresenting: (a) that Person's identity, (b) that Person's association with or authority to act on behalf of another Person, or (c) the ownership of an account to be credited."[9]

This definition is intended to cover common fraud scenarios like business email compromise, vendor impersonation and other payee impersonations where the originator is induced by a third party to authorize an entry.

Identifying what is, and what is not, an instance of false pretenses is nuanced. For example, while a business email compromise or vendor impersonation that induces someone to make a payment to an improper party would constitute false pretenses, a corporate account takeover or a payment intentionally made to a legitimate receiver who then uses the funds for something other than for the originator's intended purpose would not.

RDFIs need to review their internal policies and procedures with respect to monitoring potential unauthorized credits and credits initiated under false pretenses.

Timing of Written Statements of Unauthorized Debit and Prompt Return of Unauthorized Debits

The previous rules required that an RDFI receive a written statement of unauthorized debit, or WSUD, from consumers on or after the settlement date — as defined in the rules — for a debit in order to return it as unauthorized.

However, technological developments have created an environment where a receiver may become aware of a pending unauthorized debit before its actual settlement date.

Effective Oct. 1, the revised rules allow for more flexibility in the timing of a consumer completing a WSUD,[10] including before the debit actually settles to the receiver's account.

The previous rules were also silent as to exactly how quickly an RDFI was required to take action based on a WSUD it received from a consumer receiver; they merely required that entries returned as unauthorized be transmitted to the ODFI within a certain time frame.

As revised, there is now a requirement that RDFIs return such unauthorized entries no later than the opening of business on the sixth banking day after the RDFI completes its review of the WSUD.[11]

The revisions related to consumer WSUDs and unauthorized debits will allow receivers and RDFIs to respond to potential unauthorized debits sooner than before, thus mitigating the risk of additional fraudulent transactions to the receiver's account and helping to make the affected parties whole more quickly.

Going forward, RDFIs will need to review their internal policies and procedures associated with the handling of WSUDs and returning entries as unauthorized.

Fraud Monitoring by ODFIs, Nonconsumer Originators, and Third-Party Senders and Providers

The rules previously required nonconsumer originators to, among other things, use commercially reasonable fraudulent transaction detection systems when originating WEB debits and also when originating microentries. However, there was no corresponding requirement with respect to other types of entries.

Under the revised rules, all ODFIs, nonconsumer originators, third-party senders and third-party service providers — as each is defined in the rules — must

> (a) establish and implement risk-based processes and procedures relevant to the role it plays in the authorization or transmission of entries that are reasonably intended to identify entries that are suspected of being unauthorized or authorized under False Pretenses; and (b) at least annually review these processes and procedures and make appropriate updates to address evolving risks.[12]

This rule goes into effect in two phases based on the relevant party's 2023 entry origination volume: Phase 1,[13] effective March 20, 2026, applies to parties that had annual origination volumes exceeding 6 million entries in 2023. And Phase 2, effective June 19, 2026,[14] will subsequently apply to all other affected parties.

Importantly, a risk-based analysis cannot be used to conclude that no monitoring at all is needed on a going-forward basis; all ODFIs, nonconsumer originators, third-party senders and third-party service providers should, at a minimum, conduct risk assessments to identify, qualify and quantify their risk exposure to potential fraud.

All affected parties should evaluate their current policies and procedures, and update them accordingly, on an annual basis.

Credit Monitoring by RDFIs

Historically, the onus has been on originators and ODFIs to safeguard against fraudulent credit entries entering the ACH network, with the RDFIs having been largely omitted from that responsibility. However, RDFIs are in the unique position of being able to recognize when a receiver's account is receiving atypical credit entries — for example, based on their typical account balance or the age of the account.

Thus, under the revised rules, RDFIs will now be required to establish and implement processes and procedures to help identify and mitigate against fraudulent credit entries, including those that are unauthorized and those initiated under false pretenses, and to annually review and update such processes and procedures accordingly.

Importantly, these new RDFI credit monitoring obligations do not modify or supersede the ODFI's warranty that the entries it introduces to the network are authorized, nor does it reallocate liability between ODFIs and RDFIs.

This rule is being implemented in two phases based on the RDFI's 2023 receipt volume: Phase 1, effective March 20, 2026,[15] applies to RDFIs that had a receipt volume exceeding 10 million entries in 2023. And Phase 2, effective June 19, 2026,[16] will apply to all other RDFIs.

RDFIs should update their internal policies and procedures to include this new monitoring obligation, and should ensure staff is appropriately trained to perform whatever monitoring the RDFI decides to implement.

Standard Company Entry Descriptions: Payroll and Purchase

The company entry description field of ACH files, as defined in the rules, is a 10-character field that is used to identify batches containing certain types of entries, including for reversals and reinitiated entries.[17]

Effective March 20, 2026, the new updates to the rules will require that ODFIs, nonconsumer originators, third-party senders and third-party service providers, as applicable, also use two new company entry descriptions:

- Prearranged payment and deposit entry credits for the payment of wages or other similar compensation must include the company entry description of "PAYROLL"; and

- E-commerce purchases, which are debits authorized by a consumer online for the online purchase of goods, must include the company entry description of "PURCHASE."[18]

The goal of adding these qualifiers is to help all of the network participants more readily identify and monitor transaction types that are frequently associated with fraudulent transactions.

ODFIs, nonconsumer originators, third-party senders and third-party service providers, as applicable, will need to ensure they are categorizing their payments and using these new company entry descriptions in creating their ACH files.

Conclusion

While the above risk management topics may require substantial changes to the policies and procedures of the affected participants, the overarching result is expected to be a more secure network that is more readily able to stave off, combat and ultimately remedy fraud.

Aisha M. Hall is an associate at Taft Stettinius & Hollister LLP.

[1] NACHA Notice of Amendment to the 2024 NACHA Operating Rules, Supplement #1-2024 (April 12, 2024) ("Supplement #1").

[2] 2024 NACHA Operating Rules, Appendix Four – Return Entries.

[3] Supplement #1.

[4] ACH Operations Bulletin #1-2024: Changes to Upcoming Rules Effective Dates (July 1, 2024) ("Operations Bulletin #1").

[5] Supplement #1.

[6] "An entry returned using R17 must be received by the RDFI's ACH Operator by its deposit deadline for the returned 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." 2024 NACHA Operating Rules, Appendix Four – Return Entries.

[7] 2024 NACHA Operating Rules, Subsection 3.3 – Timing Requirements for RDFI to Make Credit and Debit Entries Available.

[8] Supplement #1.

[9] Supplement #1; NACHA Operating Rules Section 8.42 (as revised).

[10] Supplement #1.

[11] Supplement #1; 2024 NACHA Operating Rules Subsection 3.13.1 (as revised) "An RDFI may Transmit an Extended Return Entry[…] provided that […] (b) the RDFI Transmits the Extended Return Entry to its ACH Operator by its deposit deadline for the Extended Return Entry to be made available to the ODFI no later than the opening of business on the sixth

Banking Day after the Banking Day on which the RDFI completes its review of the Receiver's signed Written Statement of Unauthorized Debit, but in no case later than the opening of business on the Banking Day following the sixtieth calendar day following the Settlement Date of the original Entry."

[12] Supplement #1; NACHA Operating Rules Subsection 2.2.4 (as revised).

[13] Supplement #1.

[14] Operations Bulletin #1. The effective date of Phase 2 is June 19, 2026, which is a federal holiday. Thus, NACHA has stated that the practical effective date for Phase 2 will be June 22, 2026.

[15] Supplement #1.

[16] Operations Bulletin #1. The effective date of Phase 2 is June 19, 2026, which is a federal holiday. Thus, NACHA has stated that the practical effective date for Phase 2 will be June 22, 2026.

[17] 2024 NACHA Operating Rules Subsections 2.13.4.2 and 2.10.2.

[18] Supplement #1.