2026 ACH Fraud Monitoring Rules By NACHA

finovifi

Contents

NACHA 2026 ACH Fraud Monitoring Rules

The 2026 NACHA ACH Fraud Monitoring Rules require all ACH participants—including financial institutions and originators—to implement risk-based processes for detecting fraudulent ACH entries. Key updates include:

• **Implementation Phases:** The rules will be rolled out in two phases. **Phase 1**, effective **March 20, 2026**, applies to large originators, Third-Party Service Providers (TPSPs) and Third-Party Senders (TPSs), OFDIs, and Receiving Depository Financial Institutions (RDFIs). **Phase 2**, beginning **June 19, 2026**, extends the requirements to **all remaining ACH originators and TPSPs**, regardless of transaction volume.

• **Fraud Detection Requirements:** Organizations must establish and maintain risk-based monitoring processes to identify ACH entries initiated through fraud, including the detection of **unusual or atypical activity**. These processes and procedures must be **reviewed annually** and updated as needed to address **emerging and evolving risks**.

Risk Management Topics – (Fraud Monitoring Phase 1)

These Rule amendments related to monitoring for fraud become effective on March 20, 2026 and are part of a larger Risk Management package intended to reduce the incidence of successful fraud attempts and improve the recovery of funds after frauds have occurred.

Details

Included in this portion of the Risk Management Rule amendments are the Phase One requirements related to:

- Fraud Monitoring by Originators, Third-Party Service Providers/Third Party Senders and ODFIs; and
- ACH Credit Monitoring by RDFIs.

Technical

Fraud Monitoring by Originators, TPSPs and ODFIs
(*Effective date - Phase 1: March 20, 2026 for all ODFIs and non-Consumer Originators, TPSPs, and TPSs with annual ACH origination volume of 6 million or greater in 2023.)*

This rule amendment will require all ODFI, and each non-Consumer Originator, Third-Party Service Provider, and Third-Party Sender with annual ACH origination volume in 2023 of 6 million or greater, to establish and implement risk-based processes and procedures reasonably intended to identify ACH Entries initiated due to fraud.

- The amendment is intended to reduce the incidence of successful fraud attempts.
- Regular fraud detection monitoring can establish baselines of typical activity, making atypical activity easier to identify.

The Nacha Rules currently require Originators to use a commercially reasonable fraudulent transaction detection system to screen WEB debits and when using Micro-Entries.

- These rules are intended to reduce the incidence of unauthorized debits resulting from transactions initiated online, which can experience increased volume and velocity.

These current requirements do not encompass any other transaction types, and so do not currently apply to other types of debits or to any credits other than Micro-Entries.

- However, the existing Nacha Board policy statement "urges that all participants implement adequate control systems to detect and prevent fraud."

Several changes were made from the original proposal that was issued in a Request for Comment in May 2023.

- Eliminates use of "commercially reasonable" as a standard.
- Replaces "detection system" with "processes and procedures."
- Provides a next level description of requirements – i.e., "reasonably intended to identify…"
- Provides that the requirements apply "to the extent relevant to the role the entity plays."
- Allows an ODFI to expressly consider steps that other participants in origination are taking to monitor for fraud in designing its own processes and procedures.
- Clarifies that monitoring is not required pre-processing.
- Requires a review of processes and procedures "at least annually."

RDFI ACH Credit Monitoring

(Effective date - Phase 1: March 20, 2026 for RDFIs with annual ACH receipt volume of 10 million or greater in 2023.)

The proposal will require RDFIs with annual ACH receipt volume of 10 million or greater in 2023 to establish and implement risk-based processes and procedures designed to identify credit Entries initiated due to fraud.

- RDFIs have a view of incoming transactions as well as account profile information and historic activity on Receivers' accounts.

- A risk-based approach to monitoring can consider factors such as transactional velocity, anomalies (e.g., SEC Code mismatch with account type), and account characteristics (e.g., age of account, average balance, etc.). This aligns with AML monitoring practices in place today.
- Based on its monitoring of incoming credits, an RDFI may decide to return an entry or contact the ODFI to determine the validity of a transaction.

This rule is intended to reduce the incidence of successful fraud and better enable the recovery of funds when fraud has occurred.

- The rule aligns with an institution's regulatory obligation to monitor for suspicious transactions.
- The rule does not require pre-posting monitoring of credit entries.

ACH transaction monitoring may be happening currently within RDFIs. This amendment encourages the necessary communication between compliance monitoring, operations, product management, and relationship staff. Solutions may be developed in-house. Vendor solutions have emerged on the market to assist in monitoring received payment activity.

Similar to Third-Party Senders, any entity that performs a function of an RDFI in delivering transactions to a Receiver should implement monitoring and detection controls based on the functions performed.

Several changes were made from the original proposal that was issued in a Request for Comment in May 2023.

- Eliminates use of "commercially reasonable" as a standard.
- Replaces "detection system" with "processes and procedures."
    - A risk-based approach to fraud monitoring enables RDFIs to apply resources based on risk assessment for various types of transactions.
- Provides a next level description of requirements – i.e., "reasonably intended to identify…"
- Clarifies that monitoring is not required pre-processing.
- Requires a review of processes and procedures "at least annually."

False Pretenses

These new Rules also include references to a newly defined term, False Pretenses:

- 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."

This definition covers common fraud scenarios such as Business Email Compromise (BEC), vendor impersonation, payroll impersonation, and other payee impersonations, and complements language on "unauthorized credits" (account takeover scenario). It does not cover scams involving fake, non-existent or poor-quality goods or services.

Impact

Fraud Monitoring by Originators, TPSPs and ODFIs
Effective dates

- **Phase 1 – March 20, 2026**
    - The rule will apply to all ODFIs
    - The rule will apply to non-Consumer Originators, TPSPs, and TPSs with annual ACH origination volume of 6 million or greater in 2023
- **Phase 2 – June 19, 2026**
    - The rule will apply to all other non-Consumer Originators, TPSP, and TPS

Anticipated benefits

- Expanding fraud detection responsibilities to more parties in the ACH Network provides additional opportunities to detect and prevent fraud, especially for frauds that make use of credit-push payments.
- Reducing the incidence of successful fraud and improving the quality of transactions in the ACH Network.

Potential impacts

- Implementing or updating fraud-detection processes and procedures, particularly by organizations that are not currently performing fraud monitoring.
- Less impact for those who have already implemented a monitoring system for WEB Debits or Micro-Entries.

RDFI ACH Credit Monitoring

Effective dates

- Phase 1 – March 20, 2026
    - The rule will apply to RDFIs with annual ACH receipt volume of 10 million or greater in 2023.
- Phase 2 – June 19, 2026
    - The rule will apply to all other RDFIs.

Anticipated Benefits

- The amendment is intended to reduce the incidence of successful fraud and improve the recovery of funds when fraud has occurred.

- Identifying fraud or potentially fraudulent transactions will better enable an RDFI to exercise heightened scrutiny of accounts that are receiving such transactions.

Potential Impacts

- RDFIs will need to either establish processes and procedures reasonably intended to identify Entries that are suspected of being unauthorized or authorized under False Pretenses or ensure that existing processes and procedures are satisfactory for this requirement, including updating such systems and their alerting processes, if necessary.
- RDFIs may need to enable information sharing internally between teams that monitor transactions for suspicious activity and operations, product, and relationship teams.
- While potentially significant, these impacts are intended to reduce the incidence of fraud that uses ACH payments.

FAQs Section – Phase 1 (March 20, 2026)

***FAQs were** obtained from the NACHA website as of February 7, 2026.*

Which parties involved in the origination of ACH entries will be subject to the new requirements related to the identification of unauthorized entries or entries authorized under false pretenses?

The new requirements on the identification of unauthorized entries or entries authorized under false pretenses will apply to each ODFI, each non-consumer Originator, each Third-Party Sender, and each Third-Party Service Provider that performs any functions of ACH processing on behalf of an Originator, Third-Party Sender, or ODFI.

Will these changes impact all parties to origination at the same time?

No. The new fraud monitoring rules will be implemented under a two-phased approach:

- Phase 1 (effective March 20, 2026) will apply to all ODFIs and to those Originators, Third-Party Senders, and Third-Party Service Providers whose 2023 origination or transmission volume exceeded 6 million entries.
- Phase 2 (effective June 19, 2026) will eliminate the volume threshold and will require all non-consumer Originators, Third-Party Service Providers, and Third-Party Senders (regardless of origination or transmission volume) to comply with the fraud monitoring rules.

What will the new rules expressly require of all ODFIs, non-consumer Originators, Third-Party Senders, and any Third-Party Service Providers that perform any functions of ACH processing on behalf of an Originator, Third-Party Sender, or ODFI?

Each of these parties will be required to:

- 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
- review (at least annually) these processes and procedures and make appropriate updates to address evolving risks.

Do the Rules prescribe specific processes and procedures that ODFIs, non-consumer Originators, Third-Party Senders, and Third-Party Service Providers must use to reasonably identify unauthorized entries or entries authorized under false pretenses?

No. While the Rules require the processes and procedures employed to be relevant to the role each party plays in the handling of ACH entries, the Rules language provides for the application of a risk-based approach to implementing fraud monitoring processes and procedures.

A risk-based approach to fraud monitoring enables financial institutions, Originators, and other parties to apply resources based on a risk assessment for various types of transactions. A party might take extra measures to detect fraud in transactions in which it has determined risks to be elevated; take basic precautions where it has determined that risks are lower, and exempt transactions or activities that it determines involve very low risk.

A risk-based approach should not be used, however, to conclude that no monitoring is necessary at all. At a minimum, an entity applying a risk-based approach should conduct a risk assessment to identify and differentiate higher-risk from lower-risk transactions.

Appropriate processes and procedures reasonably intended to identify unauthorized entries and entries authorized under False Pretenses will vary depending on the role of the participant and the nature of the transaction. For example:

- Originators may be best placed to implement procedures to protect against account takeover or other vectors for initiating unauthorized transactions. Such procedures could include change controls regarding payment information and instructions for vendor and payroll payments.
- Third-Party Senders and Third-Party Service Providers involved in the origination of ACH Entries may have processes and procedures to review the volume, velocity, dollar amounts and SEC Codes of their originated ACH Entries.

The Nacha Operating Rules permit an ODFI's processes and procedures to consider the processes and procedures implemented by other participants in the origination of entries. What does this mean?

This provision of the rules gives originating participants flexibility in how processes and procedures to identify unauthorized entries can be allocated across originating participants. The basis for relying on another originating entity should be reasonable and clear (e.g., allocated by contract and verified by appropriate oversight). Any processes and procedures implemented by RDFIs and other receiving side ACH participants do not affect the obligations of originating participants.

Do the Rules mandate how often ODFIs, non-consumer Originators, Third-Party Senders/Service Providers must review the risk-based procedures they utilize to identify entries that are suspected of being unauthorized or authorized under False Pretenses?

Yes. The rules require these parties to review their processes and procedures at least annually and make appropriate updates to address evolving risks. Parties may determine that more frequent review is appropriate, based on their specific circumstances.

Do the rules require ODFIs, non-consumer Originators, Third-Party Senders, and Third-Party Service Providers to screen every ACH entry individually?

No.

Do the rules require ODFIs, non-consumer Originators, Third-Party Senders, and Third-Party Service Providers to monitor ACH entries prior to the processing of Entries?

No. Monitoring transactions prior to processing provides the greatest opportunity for detecting and preventing potential fraud. Nevertheless, the rules do not require such monitoring to be performed prior to processing Entries.

In situations where an ODFI's monitoring identifies entries as suspect, what actions should the ODFI consider?

For transactions that monitoring identifies as suspect, the ODFI can consider a number of actions. Actions may include, but are not limited to:

- stopping further processing of a flagged transaction;
- consulting with the Originator to determine the validity of the transaction;
- consulting with other internal monitoring teams or systems to determine if the transaction raises other flags; and
- contacting the RDFI to determine if characteristics of the Receiver's account raise additional red flags, or requesting the freeze or the return of funds.

With respect to debits, a robust return and return rate monitoring program in conformance with existing Rules (as well as any required compliance with other specific fraud detection Rules for WEB debits and Micro-Entries) is sufficient as a minimum level of fraud monitoring.

Nacha's Risk Management Advisory Group has developed and published additional guidance for ODFIs:

RMAG Guidance on ODFI Credit-Push Fraud Response Checklists

Do the requirements to identify entries suspected to be unauthorized/authorized under False Pretenses impose obligations on ODFIs, non-Consumer Originators, TPS/TPSP to prevent wrongful activity, or change the allocation of liability between parties?

No. Express disclaimers of modification of Uniform Commercial Code (UCC) Article 4A rights and obligations, and of the creation of any duty other than the commitment to Nacha to comply with the Rules, will allow Nacha to manage compliance with the new standards via existing enforcement mechanisms without upsetting the allocation of liability among Nacha participants under otherwise applicable law.

What risk controls will the Nacha Operating Rules require RDFIs to implement with respect to the receipt of ACH credits?

Each RDFI must establish and implement risk-based processes and procedures relevant to the role it plays in connection with the receipt of credit Entries. The processes and procedures should be reasonably intended to identify credit Entries suspected of being unauthorized or authorized under False Pretenses, and also should include the handling of such credit Entries identified as potentially unauthorized or authorized under False Pretenses.

Will these changes impact all RDFIs at the same time?

No. The new requirement for RDFIs to establish processes and procedures to reasonably identify credit entries that are suspected of being unauthorized or authorized under False Pretenses will be implemented under a two-phased approach:

- Phase 1 (effective March 20, 2026) will apply to all RDFIs whose 2023 ACH receipt volume exceeded 10 million entries.
- Phase 2 (effective June 19, 2026) will eliminate the volume threshold and will require all RDFIs (regardless of ACH receipt volume) to comply with the credit monitoring rules.

Do the Nacha Operating Rules prescribe specific processes and procedures that RDFIs must employ to reasonably identify credit entries suspected of being unauthorized entries or entries authorized under false pretenses?

No. The Rules permit RDFIs to establish a risk-based approach to implementing fraud monitoring processes and procedures. This allows RDFIs to apply resources based on a risk assessment for various types of transactions. An RDFI might take extra measures to detect fraud in transactions in which it has determined risks to be elevated; take basic precautions where it has determined that risks are lower, and exempt transactions or activities that it determines involve very low risk.

A risk-based approach should not be used, however, to conclude that no monitoring is necessary at all. At a minimum, an entity applying a risk-based approach should conduct a risk assessment to identify and differentiate higher-risk from lower-risk transactions.

Do the Nacha Operating Rules mandate how often RDFIs must review the risk-based procedures they utilize to identify credit entries that are suspected of being unauthorized or authorized under False Pretenses?

Yes. The rules require RDFIs to review these processes and procedures at least annually and make appropriate updates to address evolving risks. RDFIs may determine that more frequent review is appropriate, based on their specific circumstances.

Do the rules require RDFIs to screen every ACH entry individually?

No.

Must an RDFI's risk-based processes and procedures be performed prior to processing entries?

No. Although monitoring transactions prior to processing provides the greatest opportunity for detecting and preventing potential fraud, the rules do not require such monitoring to be performed prior to processing Entries.

To the extent that an RDFI's processes and procedures incorporate pre-posting monitoring of credits, an RDFI may delay funds availability for the Entry, as permitted by the rules governing exemptions to the funds availability requirements, to investigate the appropriateness of the Entry.

Do the requirements to identify entries suspected to be unauthorized/authorized under False Pretenses impose obligations on ODFIs, non-Consumer Originators, TPS/TPSP to prevent wrongful activity, or change the allocation of liability between parties?

No. Express disclaimers of modification of Uniform Commercial Code (UCC) Article 4A rights and obligations, and of the creation of any duty other than the commitment to Nacha to comply with the Rules, will allow Nacha to manage compliance with the new standards via existing enforcement mechanisms without upsetting the allocation of liability among Nacha participants under otherwise applicable law.

What should an RDFI consider when establishing policies and procedures reasonably intended to identify credit Entries suspected of being unauthorized or authorized under False Pretenses?

While an RDFI will not likely know the circumstances under which a credit entry was originated, entries that are unauthorized or authorized under False Pretenses potentially may be identified based on characteristics of the entry and the receiving account, such as:

- a Standard Entry Class Code that does not align with the type of receiving account, such as a corporate CCD entry to a consumer account.
- a high-dollar transaction that is atypical for the receiving account.
- a series of similar credit entries received within a short period of time, such as multiple payroll or benefit payments.
- any of the above to a new account, a dormant account, or to an account acting as a mule.

An RDFI flagging such an entry may act by taking advantage of the voluntary exemption from funds availability requirements for credit entries, providing more time to examine the outlier transaction and receiving account. The RDFI can utilize Nacha's Risk Management Portal and ACH Contact Registry for contact information for the ODFI to help in its determination. If the RDFI believes an entry to be unauthorized or authorized under False Pretenses, and it concludes that the best course of action is to return the funds, it may return the entry using Return Reason Code R17 "QUESTIONABLE" or, at the ODFI's request, using Return Reason Code R06.

Nacha's Risk Management Advisory Group has developed and published additional guidance for RDFIs:

- RMAG Offers Guidance for Risk-Based Controls to Address the Potential of Fraudsters Gaining Access to Illicit Funds | Nacha
- RMAG Guidance on RDFI Credit-Push Fraud Response Checklists

Is an RDFI permitted to utilize the services of a Third-Party Service Provider to help carry out the RDFI's new obligations under the Rules?

Yes. This rule does not alter an RDFI's ability to utilize a Third-Party Service Provider to carry out the RDFI's obligations under the Rules.

The obligation to establish processes and procedures reasonably intended to identify unauthorized Entries and Entries authorized under False Pretenses is imposed on all ACH participants involved in the origination of entries and, therefore, expressly permits those parties to consider the procedures and processes of other ACH participants involved in the origination of entries.

Conversely, the corresponding rules on the receipt of entries establish a requirement for such processes and procedures only on RDFIs. Therefore, express language permitting the RDFI to take into consideration other Receiver side processes and procedures is not included. However, the omission of such language is not intended to alter the ability of RDFIs to utilize third parties (e.g., Third-Party Service Providers) to carry out their obligations under the Rules.

The processes and procedures implemented by parties involved in the origination of entries do not affect the obligations of RDFIs pursuant to the RDFI's credit fraud monitoring requirements in Subsection 3.1.10 of the Nacha Operating Rules.

Risk Management Topics – (Fraud Monitoring Phase 2)

These Rule amendments related to monitoring for fraud become effective on June 19, 2026 and are part of a larger Risk Management package intended to reduce the incidence of successful fraud attempts and improve the recovery of funds after frauds have occurred.

NOTE: As June 19 is a federal holiday, the practical effective date for these two rules will be the next banking day – Monday, June 22, 2026. All affected parties are encouraged to become compliant with these rules as soon as possible, but no later than June 22, 2026. This applies to all references to June 19, 2026, which follow.

Details

Included in this portion of the Risk Management Rule amendments are the Phase Two requirements related to:

- Fraud Monitoring by Originators, Third-Party Service Providers/Third Party Senders and ODFIs; and
- ACH Credit Monitoring by RDFIs.

Technical

Fraud Monitoring by Originators, TPSPs and ODFIs
(*Effective date - Phase 2: June 19, 2026 for all non-Consumer Originators, TPSPs, and TPSs that did not fall under the requirement threshold for Phase 1.)*

This rule amendment will require all non-Consumer Originator, Third-Party Service Provider, and Third-Party Sender that did not fall under the requirement threshold for Phase 1, to establish and implement risk-based processes and procedures reasonably intended to identify ACH Entries initiated due to fraud.

- The amendment is intended to reduce the incidence of successful fraud attempts.
- Regular fraud detection monitoring can establish baselines of typical activity, making atypical activity easier to identify.

The Nacha Rules currently require Originators to use a commercially reasonable fraudulent transaction detection system to screen WEB debits and when using Micro-Entries.

- These rules are intended to reduce the incidence of unauthorized debits resulting from transactions initiated online, which can experience increased volume and velocity.

These current requirements do not encompass any other transaction types, and so do not currently apply to other types of debits or to any credits other than Micro-Entries.

- However, the existing Nacha Board policy statement “urges that all participants implement adequate control systems to detect and prevent fraud.”

Several changes were made from the original proposal that was issued in a Request for Comment in May 2023.

- Eliminates use of “commercially reasonable” as a standard.
- Replaces “detection system” with “processes and procedures.”
- Provides a next level description of requirements – i.e., “reasonably intended to identify…”
- Provides that the requirements apply “to the extent relevant to the role the entity plays.”
- Allows an ODFI to expressly consider steps that other participants in origination are taking to monitor for fraud in designing its own processes and procedures.
- Clarifies that monitoring is not required pre-processing.

- Requires a review of processes and procedures “at least annually.”

RDFI ACH Credit Monitoring

(Effective date - Phase 2: June 19, 2026 for all RDFIs that did not meet the threshold requirement for Phase 1.)

The amendment will require all RDFIs that did not meet the requirement threshold for Phase 1 to establish and implement risk-based processes and procedures designed to identify credit Entries initiated due to fraud.

- RDFIs have a view of incoming transactions as well as account profile information and historic activity on Receivers’ accounts.
- A risk-based approach to monitoring can consider factors such as transactional velocity, anomalies (e.g., SEC Code mismatch with account type), and account characteristics (e.g., age of account, average balance, etc.). This aligns with AML monitoring practices in place today.
- Based on its monitoring of incoming credits, an RDFI may decide to return an entry or contact the ODFI to determine the validity of a transaction.

This rule is intended to reduce the incidence of successful fraud and better enable the recovery of funds when fraud has occurred.

- The rule aligns with an institution’s regulatory obligation to monitor for suspicious transactions.
- The rule does not require pre-posting monitoring of credit entries.

ACH transaction monitoring may be happening currently within RDFIs. This amendment encourages the necessary communication between compliance monitoring, operations, product management, and relationship staff. Solutions may be developed in-house. Vendor solutions have emerged on the market to assist in monitoring received payment activity.

Similar to Third-Party Senders, any entity that performs a function of an RDFI in delivering transactions to a Receiver should implement monitoring and detection controls based on the functions performed.

Several changes were made from the original proposal that was issued in a Request for Comment in May 2023.

- Eliminates use of “commercially reasonable” as a standard.
- Replaces “detection system” with “processes and procedures.”
    - A risk-based approach to fraud monitoring enables RDFIs to apply resources based on risk assessment for various types of transactions.
- Provides a next level description of requirements – i.e., “reasonably intended to identify…”
- Clarifies that monitoring is not required pre-processing.
- Requires a review of processes and procedures “at least annually.”

False Pretenses

These new Rules also include references to a newly defined term, False Pretenses:

- 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."

This definition covers common fraud scenarios such as Business Email Compromise (BEC), vendor impersonation, payroll impersonation, and other payee impersonations, and complements language on "unauthorized credits" (account takeover scenario). It does not cover scams involving fake, non-existent or poor-quality goods or services.

Impact

Fraud Monitoring by Originators, TPSPs and ODFIs
Effective dates

- Phase 1 – March 20, 2026
    - The rule will apply to all ODFIs
    - The rule will apply to non-Consumer Originators, TPSPs, and TPSs with annual ACH origination volume of 6 million or greater in 2023
- Phase 2 – June 19, 2026
    - The rule will apply to all other non-Consumer Originators, TPSP, and TPS

Anticipated benefits

- Expanding fraud detection responsibilities to more parties in the ACH Network provides additional opportunities to detect and prevent fraud, especially for frauds that make use of credit-push payments.
- Reducing the incidence of successful fraud and improving the quality of transactions in the ACH Network.

Potential impacts

- Implementing or updating fraud-detection processes and procedures, particularly by organizations that are not currently performing fraud monitoring.
- Less impact for those who have already implemented a monitoring system for WEB Debits or Micro-Entries.

RDFI ACH Credit Monitoring

Effective dates

- Phase 1 – March 20, 2026
    - The rule will apply to RDFIs with annual ACH receipt volume of 10 million or greater in 2023.
- Phase 2 – June 19, 2026
    - The rule will apply to all other RDFIs.

Anticipated Benefits

- The amendment is intended to reduce the incidence of successful fraud and improve the recovery of funds when fraud has occurred.
- Identifying fraud or potentially fraudulent transactions will better enable an RDFI to exercise heightened scrutiny of accounts that are receiving such transactions.

Potential Impacts

- RDFIs will need to either establish processes and procedures reasonably intended to identify Entries that are suspected of being unauthorized or authorized under False Pretenses or ensure that existing processes and procedures are satisfactory for this requirement, including updating such systems and their alerting processes, if necessary.
- RDFIs may need to enable information sharing internally between teams that monitor transactions for suspicious activity and operations, product, and relationship teams.
- While potentially significant, these impacts are intended to reduce the incidence of fraud that uses ACH payments.

FAQs Section – Phase 2 (June 19, 2026)

FAQs were obtained from the NACHA website as of February 7, 2026

Which parties involved in the origination of ACH entries will be subject to the new requirements related to the identification of unauthorized entries or entries authorized under false pretenses?

The new requirements on the identification of unauthorized entries or entries authorized under false pretenses will apply to each ODFI, each non-consumer Originator, each Third-Party Sender, and each Third-Party Service Provider that performs any functions of ACH processing on behalf of an Originator, Third-Party Sender, or ODFI.

Will these changes impact all parties to origination at the same time?

No. The new fraud monitoring rules will be implemented under a two-phased approach:

- Phase 1 (effective March 20, 2026) will apply to all ODFIs and to those Originators, Third-Party Senders, and Third-Party Service Providers whose 2023 origination or transmission volume exceeded 6 million entries.
- Phase 2 (effective June 19, 2026) will eliminate the volume threshold and will require all non-consumer Originators, Third-Party Service Providers, and Third-Party Senders (regardless of origination or transmission volume) to comply with the fraud monitoring rules.

What will the new rules expressly require of all ODFIs, non-consumer Originators, Third-Party Senders, and any Third-Party Service Providers that perform any functions of ACH processing on behalf of an Originator, Third-Party Sender, or ODFI?

Each of these parties will be required to:

- 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
- review (at least annually) these processes and procedures and make appropriate updates to address evolving risks.

Do the Rules prescribe specific processes and procedures that ODFIs, non-consumer Originators, Third-Party Senders, and Third-Party Service Providers must use to reasonably identify unauthorized entries or entries authorized under false pretenses?

No. While the Rules require the processes and procedures employed to be relevant to the role each party plays in the handling of ACH entries, the Rules language provides for the application of a risk-based approach to implementing fraud monitoring processes and procedures.

A risk-based approach to fraud monitoring enables financial institutions, Originators, and other parties to apply resources based on a risk assessment for various types of transactions. A party might take extra measures to detect fraud in transactions in which it has determined risks to be elevated; take basic precautions where it has determined that risks are lower, and exempt transactions or activities that it determines involve very low risk.

A risk-based approach should not be used, however, to conclude that no monitoring is necessary at all. At a minimum, an entity applying a risk-based approach should conduct a risk assessment to identify and differentiate higher-risk from lower-risk transactions.

Appropriate processes and procedures reasonably intended to identify unauthorized entries and entries authorized under False Pretenses will vary depending on the role of the participant and the nature of the transaction. For example:

- Originators may be best placed to implement procedures to protect against account takeover or other vectors for initiating unauthorized transactions. Such procedures could include change controls regarding payment information and instructions for vendor and payroll payments.
- Third-Party Senders and Third-Party Service Providers involved in the origination of ACH Entries may have processes and procedures to review the volume, velocity, dollar amounts and SEC Codes of their originated ACH Entries.

The Nacha Operating Rules permit an ODFI's processes and procedures to consider the processes and procedures implemented by other participants in the origination of entries. What does this mean?

This provision of the rules gives originating participants flexibility in how processes and procedures to identify unauthorized entries can be allocated across originating participants. The basis for relying on another originating entity should be reasonable and clear (e.g., allocated by contract and verified by appropriate oversight). Any processes and procedures implemented by RDFIs and other receiving side ACH participants do not affect the obligations of originating participants.

Do the Rules mandate how often ODFIs, non-consumer Originators, Third-Party Senders/Service Providers must review the risk-based procedures they utilize to identify entries that are suspected of being unauthorized or authorized under False Pretenses?

Yes. The rules require these parties to review their processes and procedures at least annually and make appropriate updates to address evolving risks. Parties may determine that more frequent review is appropriate, based on their specific circumstances.

Do the rules require ODFIs, non-consumer Originators, Third-Party Senders, and Third-Party Service Providers to screen every ACH entry individually?

No.

Do the rules require ODFIs, non-consumer Originators, Third-Party Senders, and Third-Party Service Providers to monitor ACH entries prior to the processing of Entries?

No. Monitoring transactions prior to processing provides the greatest opportunity for detecting and preventing potential fraud. Nevertheless, the rules do not require such monitoring to be performed prior to processing Entries.

In situations where an ODFI's monitoring identifies entries as suspect, what actions should the ODFI consider?

For transactions that monitoring identifies as suspect, the ODFI can consider a number of actions. Actions may include, but are not limited to:

- stopping further processing of a flagged transaction;
- consulting with the Originator to determine the validity of the transaction;
- consulting with other internal monitoring teams or systems to determine if the transaction raises other flags; and
- contacting the RDFI to determine if characteristics of the Receiver's account raise additional red flags, or requesting the freeze or the return of funds.

With respect to debits, a robust return and return rate monitoring program in conformance with existing Rules (as well as any required compliance with other specific fraud detection Rules for WEB debits and Micro-Entries) is sufficient as a minimum level of fraud monitoring.

Nacha's Risk Management Advisory Group has developed and published additional guidance for ODFIs:

RMAG Guidance on ODFI Credit-Push Fraud Response Checklists

Do the requirements to identify entries suspected to be unauthorized/authorized under False Pretenses impose obligations on ODFIs, non-Consumer Originators, TPS/TPSP to prevent wrongful activity, or change the allocation of liability between parties?

No. Express disclaimers of modification of Uniform Commercial Code (UCC) Article 4A rights and obligations, and of the creation of any duty other than the commitment to Nacha to comply with the Rules, will allow Nacha to manage compliance with the new standards via existing enforcement mechanisms without upsetting the allocation of liability among Nacha participants under otherwise applicable law.

What risk controls will the Nacha Operating Rules require RDFIs to implement with respect to the receipt of ACH credits?

Each RDFI must establish and implement risk-based processes and procedures relevant to the role it plays in connection with the receipt of credit Entries. The processes and procedures should be reasonably intended to identify credit Entries suspected of being unauthorized or authorized under False Pretenses, and also should include the handling of such credit Entries identified as potentially unauthorized or authorized under False Pretenses.

Will these changes impact all RDFIs at the same time?

No. The new requirement for RDFIs to establish processes and procedures to reasonably identify credit entries that are suspected of being unauthorized or authorized under False Pretenses will be implemented under a two-phased approach:

- Phase 1 (effective March 20, 2026) will apply to all RDFIs whose 2023 ACH receipt volume exceeded 10 million entries.
- Phase 2 (effective June 19, 2026) will eliminate the volume threshold and will require all RDFIs (regardless of ACH receipt volume) to comply with the credit monitoring rules.

Do the Nacha Operating Rules prescribe specific processes and procedures that RDFIs must employ to reasonably identify credit entries suspected of being unauthorized entries or entries authorized under false pretenses?

No. The Rules permit RDFIs to establish a risk-based approach to implementing fraud monitoring processes and procedures. This allows RDFIs to apply resources based on a risk assessment for various types of transactions. An RDFI might take extra measures to detect fraud in transactions in which it has determined risks to be elevated; take basic precautions where it has determined that risks are lower, and exempt transactions or activities that it determines involve very low risk.

A risk-based approach should not be used, however, to conclude that no monitoring is necessary at all. At a minimum, an entity applying a risk-based approach should conduct a risk assessment to identify and differentiate higher-risk from lower-risk transactions.

Do the Nacha Operating Rules mandate how often RDFIs must review the risk-based procedures they utilize to identify credit entries that are suspected of being unauthorized or authorized under False Pretenses?

Yes. The rules require RDFIs to review these processes and procedures at least annually and make appropriate updates to address evolving risks. RDFIs may determine that more frequent review is appropriate, based on their specific circumstances.

Do the rules require RDFIs to screen every ACH entry individually?

No.

Must an RDFI's risk-based processes and procedures be performed prior to processing entries?

No. Although monitoring transactions prior to processing provides the greatest opportunity for detecting and preventing potential fraud, the rules do not require such monitoring to be performed prior to processing Entries.

To the extent that an RDFI's processes and procedures incorporate pre-posting monitoring of credits, an RDFI may delay funds availability for the Entry, as permitted by the rules governing exemptions to the funds availability requirements, to investigate the appropriateness of the Entry.

Do the requirements to identify entries suspected to be unauthorized/authorized under False Pretenses impose obligations on ODFIs, non-Consumer Originators, TPS/TPSP to prevent wrongful activity, or change the allocation of liability between parties?

No. Express disclaimers of modification of Uniform Commercial Code (UCC) Article 4A rights and obligations, and of the creation of any duty other than the commitment to Nacha to comply with the Rules, will allow Nacha to manage compliance with the new standards via existing enforcement mechanisms without upsetting the allocation of liability among Nacha participants under otherwise applicable law.

What should an RDFI consider when establishing policies and procedures reasonably intended to identify credit Entries suspected of being unauthorized or authorized under False Pretenses?

While an RDFI will not likely know the circumstances under which a credit entry was originated, entries that are unauthorized or authorized under False Pretenses potentially may be identified based on characteristics of the entry and the receiving account, such as:

- a Standard Entry Class Code that does not align with the type of receiving account, such as a corporate CCD entry to a consumer account.
- a high-dollar transaction that is atypical for the receiving account.
- a series of similar credit entries received within a short period of time, such as multiple payroll or benefit payments.
- any of the above to a new account, a dormant account, or to an account acting as a mule.

An RDFI flagging such an entry may act by taking advantage of the voluntary exemption from funds availability requirements for credit entries, providing more time to examine the outlier transaction and receiving account. The RDFI can utilize Nacha's Risk Management Portal and ACH Contact Registry for

contact information for the ODFI to help in its determination. If the RDFI believes an entry to be unauthorized or authorized under False Pretenses, and it concludes that the best course of action is to return the funds, it may return the entry using Return Reason Code R17 “QUESTIONABLE” or, at the ODFI’s request, using Return Reason Code R06.

Nacha's Risk Management Advisory Group has developed and published additional guidance for RDFIs:

- RMAG Offers Guidance for Risk-Based Controls to Address the Potential of Fraudsters Gaining Access to Illicit Funds | Nacha

- RMAG Guidance on RDFI Credit-Push Fraud Response Checklists

Is an RDFI permitted to utilize the services of a Third-Party Service Provider to help carry out the RDFI’s new obligations under the Rules?

Yes. This rule does not alter an RDFI’s ability to utilize a Third-Party Service Provider to carry out the RDFI’s obligations under the Rules.

The obligation to establish processes and procedures reasonably intended to identify unauthorized Entries and Entries authorized under False Pretenses is imposed on all ACH participants involved in the origination of entries and, therefore, expressly permits those parties to consider the procedures and processes of other ACH participants involved in the origination of entries.

Conversely, the corresponding rules on the receipt of entries establish a requirement for such processes and procedures only on RDFIs. Therefore, express language permitting the RDFI to take into consideration other Receiver side processes and procedures is not included. However, the omission of such language is not intended to alter the ability of RDFIs to utilize third parties (e.g., Third-Party Service Providers) to carry out their obligations under the Rules.

The processes and procedures implemented by parties involved in the origination of entries do not affect the obligations of RDFIs pursuant to the RDFI’s credit fraud monitoring requirements in Subsection 3.1.10 of the Nacha Operating Rules.

Disclosure

All information was obtained from the NACHA website as of February 7, 2026.