The Fraud Monitoring Rule
ACH Originators Frequently Asked Questions

What is changing?
Nacha, the National Automated Clearing House Association, has amended the ACH rules requiring all ACH participants to update or implement risk-based fraud monitoring processes to identify and prevent fraudulent outgoing ACH entries.

Why?
- Reduce or even prevent the incidence of successful fraud attempts
- Establish baselines of typical activity, making atypical activity easier to identify
- Protect operations and vendor relationships
- Stay compliant with Nacha requirements

When?
Effective June 19, 2026

Who does this impact?
Businesses that initiate ACH payments, along with all financial institutions.

How do we implement this new rule requirement?
Create adequate risk-based controls, processes, and procedures which should be scaled for the size and operational complexities of your business to reasonably identify ACH entries initiated due to fraud.

- Document processes and procedures.
  - enrollment and on-boarding procedures for new customers.
  - payment requests from customers, company associates, and partners to change payment instructions.
- Monitor ACH activity regularly
- Conduct annual risk assessments
- Implement layered controls
- Train employees to recognize fraud attempts. Criminals often create a sense of urgency to pressure them to make a quick decision.
- Sign up for fraud newsletters

Business originator controls can be developed internally or created by third-party solution providers.

What are some examples of controls that may provide layered security?
- Dual Controls – A fraudster may be able to get past one individual but will have difficulty tricking two
- Account Validation – Account validation tools are used to assess new accounts and changes on existing receiver accounts.
  - Commercial account validation services

    - Verify any changes to account details using trusted contact information.
    - Prenotes do not establish account ownership.
- Multi-factor Authentication - – Multi-factor authentication is considered more robust than password-only authentication. A second factor in addition to the password can be a second credential, operator intervention, or a biometric input. A fraudster can use social engineering to steal a username and password but cannot obtain the second factor required to access the system. A physical token or biometric solution is preferred to a solution using a code via text or email because fraudsters have developed tools to intercept the content of these channels.
- Out-of-Band Authentication – Authenticate payment requests or changes to payment instructions by independently verifying the request/change using a method other than the method used by the original request. *For example, if a vendor calls to request a change to their routing and account information for future payments, use contact information contained within your organization's internal database to contact the vendor via phone or email.*
- Routine and Red Flag Reporting – Review and reconcile accounts daily. Generate regular reports that identify transactions to new relationships, transactions of existing customers to new accounts, or abnormal activity. Verify that these transactions were intentional.
- Review User Rights – Review user rights to online banking systems regularly and promptly remove access for terminated or transferred employees who no longer require access.
- Secure Systems and Applications – Ensure maintenance of firewalls and make sure antivirus software is up to date. Ensure all system components and software have the latest vendor-supplied security patches installed.
- Pinnacle encourages our ACH originating clients to utilize services offered by their organization and to seek other tools to ensure payments are valid.

Where does fraud happen the most?

Fraudsters often target:

- Vendors or receivers
- Payment or account changes
- Payroll files

What are common schemes?

Credit-push fraud schemes rely on social engineering to trick victims into sending the fraudster money. Social engineering fraud isn't complex; controls can be simple, but they must be utilized to be effective.

- Business email compromise
- Vendor payment redirection
- Payroll diversion

How do I demonstrate compliance to my financial institution if requested?

Provide documentation of your process which may include:

- Policies & procedures
- Controls implemented
- Monitoring logs/alerts
- Incident/fraud history and remediation
- Evidence of training

What happens if I don't comply with Nacha rules or have weak ACH risk-controls?

Consequences can include:

- Greater risk of fraud
- Financial losses
- Reputational impacts
- Damaged service relationships; vendors and your bank
- Non-compliance of the Nacha rules resulting in potential fines

Who do I contact if I need assistance with the change?

Your local treasury management client services team, or contact
Treasury Management Client Services
Central Time - 866.839.2781
Eastern Time - 855.282.8655