ACH Fraud Monitoring Requirements

A risk-based approach to helping prevent ACH fraud

Effective June 19, 2026, Nacha will require all non-consumer ACH Originators to establish and implement risk-based processes and procedures reasonably intended to identify ACH entries initiated due to fraud.

This rule requires non-consumer ACH Originators to establish and maintain risk-based processes and procedures designed to identify ACH entries initiated as a result of fraud. The rule is intended to reduce fraud in ACH transactions, with particular focus on **Unauthorized Entries**—transactions initiated without the account holder's permission, such as account takeover when a fraudster compromises online banking credentials—and **Entries Authorized Under False Pretenses**—payments approved because of deception, such as business email compromise (BEC), vendor impersonation, payroll impersonation, or payment redirection scams.

Key requirements for South Shore Bank ACH Originators

Under the new rule, your business must establish and maintain a proactive, risk-based fraud monitoring program that includes the following:

1. **Establish and Implement Risk-Based Procedures:** You must define and apply processes and procedures relevant to your role as an Originator, that are reasonably intended to identify outgoing ACH Entries that may be unauthorized or initiated under False Pretenses.
2. **Annual Review:** These processes and procedures must be reviewed and, if necessary, updated at least annually to address evolving fraud risks.
3. **Risk-Based Approach:** You must conduct a risk assessment to identify high-risk vs. low-risk transactions and apply appropriate monitoring measures. This allows you to focus your resources where the risk is highest.

Who does this new rule apply to?

This rule applies to all South Shore Bank business clients that originate ACH files. Any business, government entity, or organization that initiates ACH transactions—such as payroll, vendor payments, or collections—is considered a non-consumer Originator.

Is South Shore Bank the only bank affected by the rule?

No. This is a Nacha rule change that applies broadly to financial institutions serving business clients that originate ACH payments.

When do I need to comply with the new rule?

Your business should be prepared to comply with these fraud monitoring requirements by June 19, 2026.

South Shore Bank may review your fraud monitoring processes as part of your established annual ACH review, unless changes to your ACH service require an earlier review.

What is "False Pretenses" fraud and why is it important?

"False Pretenses" refers to fraud scenarios in which a payment is authorized because of deception. It is an important risk to consider when building your fraud monitoring procedures. This addition to the Nacha rules reflects the growing impact of fraud schemes such as the following:

- **Business Email Compromise (BEC):** A fraudster impersonates an executive or vendor by email to direct an ACH payment to a fraudulent account.
- **Impersonation:** A fraudster calls or emails to persuade an employee to change payment information for a legitimate vendor or employee.

Learn more about False Pretenses

What other types of threats should I consider when implementing my fraud monitoring processes?

Effective fraud monitoring should be layered and tailored to your business. The controls you use should reflect the nature of your ACH activity, such as payroll, vendor payments, or client collections. A risk-based approach does not require screening each individual ACH payment, and it does not need to be fully automated. However, businesses are expected to take reasonable steps to detect suspicious activity, document their procedures, and review and update them regularly—at a minimum annually. Having no monitoring is not acceptable.

In addition to the rule's requirements, your fraud monitoring program should also consider the following risks:

- **Unauthorized Withdrawals:** How can you prevent external parties from pulling money without permission?
- **Internal Misconduct:** How can you prevent misuse of payment authority by employees?
- **Compromised Credentials:** How can you protect your internal systems used for managing payment information and activity?

- **Change Request Fraud:** How can you verify the authenticity of payment instruction changes?

Does South Shore Bank require me to use a specific software system?

No. This is a principles-based rule, not a prescriptive one. It requires your business to implement risk-based processes and procedures that are appropriate for your specific operations. Depending on your needs, this may include:

- Manual, documented internal controls
- Utilization of new features in your accounting or payroll software
- Adoption of a third-party fraud monitoring solution

Does this rule change my liability for ACH fraud losses?

No. This rule establishes a compliance standard for Originators, Third-Party Senders, and financial institutions. It does not change the underlying allocation of liability for ACH fraud under existing law, but it does require businesses to strengthen controls designed to mitigate fraud risk.

What are some examples of risk-based processes for my business?

Your ACH fraud monitoring procedures should reflect your business structure, payment volume, and specific risk profile. The examples below are provided for general guidance and are not intended to serve as a complete checklist. Depending on your needs, your program may include a combination of the following procedural and technical controls:

- **Dual Authorization / Segregation of Duties:** Require at least two individuals to authorize high-dollar payments or ACH files. No single person should be able to create, approve, and release a payment.
- **Out-of-Band Verification:** If you receive an email requesting a bank account change for a vendor or employee, confirm the request through a trusted secondary channel, such as calling a known number already on file rather than any number provided in the email.
- **System Controls and Anomaly Detection:** Use your accounting or payment systems to flag unusual activity automatically, such as:
    - Payments to a new vendor that exceed a set dollar threshold
    - Sudden increases in transaction volume or amount outside of normal business patterns
    - Unusual payment destinations (e.g., high-risk geographical locations)

- **Pre-Payment Account Validation:** Use ACH prenotes (zero-dollar verification) or third-party validation services to confirm the existence and ownership of a new vendor's or employee's bank account before initiating the first live payment.
- **Strong Access Controls (MFA):** Limit access to your ACH origination system to authorized employees and require multi-factor authentication (MFA) for all users.
- **Dedicated Payment Workstations:** Restrict computers used to initiate or approve ACH payments from being used for higher-risk activities, such as opening external email attachments or general web browsing.
- **Formal Fraud Incident Response Plan:** Maintain a clear, documented response plan that outlines immediate next steps if fraud is detected, including internal escalation procedures and key South Shore Bank contacts.
- **Ongoing Employee Training:** Provide regular training for employees involved in payments so they can recognize, question, and independently verify suspicious requests.
- **Daily Review and Escalation Procedures:** Review accounts and ACH activity frequently—ideally at least daily—and ensure staff know how to escalate suspected fraud to designated internal personnel, your financial institution, or law enforcement when appropriate.

Additional practical steps to prepare may include verifying account information associated with first-time payments, independently authenticating any change in payment instructions or payment method through a trusted previously known phone number, and reminding staff never to share online banking credentials or account information in response to an incoming call, email, text message, fax, or letter—even if the request appears to come from the financial institution.

We encourage all South Shore Bank business ACH Originators to review their current fraud controls as soon as possible. These examples are not intended to be all-inclusive or one-size-fits-all; your risk-based processes and procedures for detecting fraud should be tailored to your organization and payment activities. Please work with your compliance, legal, and technology teams to ensure your organization is prepared ahead of the required deadline.

If you don't have the newest version of the Nacha Operating Rules and Guidelines, you can purchase it directly from the Nacha website.

For additional guidance or to discuss how these changes may impact your business, please contact our Treasury Management Team at 781.682.3240.