ALERUS

ACH FRAUD MONITORING PROCESSES AND PROCEDURES

SUGGESTED GUIDELINES FOR BUSINESSES

Beginning June 19, 2026, Nacha will require all non-consumer ACH originators to implement fraud-monitoring processes and procedures that are reasonably intended to identify potential fraud. As ACH-related fraud attempts continue to increase, the updated rule is aimed at strengthening fraud protection at the point of transaction initiation.

All businesses that originate payments via ACH are expected to have fraud-monitoring processes and procedures in place by June 19. The amended rule does not require every ACH entry to be individually screened, nor does it require screening to occur prior to processing. Rather, the rule is intended to encourage consistent, risk-based screening, which can help effectively detect potential fraud.

General Guidelines

As you develop your fraud-monitoring practices, we recommend including:

- Documented, risk-based procedures to identify suspicious activity
- Regular reviews — at least annually — to ensure effectiveness and implement updates as needed
- Management review and approval of procedures
- Employee training to ensure procedures are consistently followed

Additional Considerations

It is suggested that all business ACH originators also consider including the following fraud-monitoring measures in their processes and procedures.

- Implement dual control for payment processing. Dual control requires two levels of approval to release payments.
- Establish and follow documented procedures for processing any requested changes to payment information, such as updates to account or routing numbers. Require verification of all payment change requests using a trusted contact method, such as a phone number on file.
- Use an anomaly detection tool to assist in identifying suspicious activities, such as unusual payment frequency, unusual amounts, and account information changes.
- Validate every new account by sending an ACH prenotification, a micro-entry verification, or a validation service before issuing an initial payment.
- Conduct regular origination and return rate monitoring for everyone you process payments for. Regular monitoring can help establish a baseline for normal activity, making it easier to detect fraudulent activity.
- Act promptly to assist if a receiving bank flags an ACH entry as suspicious, and ensure correct internal teams are informed. This could include facilitating direct inquiries from the financial institution or investigating entries returned using the QUESTIONABLE code to determine whether fraud may be involved.

Resources

- Nacha Operating Rules – New Rules (nacha.org)
- Fraud Monitoring Rule Changes - Phase 2 (nacha.org)
- Company Entry Description Rule Changes (nacha.org)
- Nacha Operating Rule Changes: Risk Management Resources (umacha.org)

The information contained herein is general in nature, is provided for educational purposes only, and should not be construed as legal or tax advice.

Member FDIC

03.05.2026 | D-TM