Q2 2026

Payments Newsletter

For Treasury Customers

ACH Fraud Monitoring Is Now Required: What Your Organization Needs to Know

If your organization initiates ACH transactions, Nacha Rules now require you to have fraud monitoring procedures in place. If you originated 6 million or more ACH entries in 2023, this requirement has been in effect since March 20, 2026. For all other non-consumer Originators, the deadline is June 19, 2026.

What the Rule Requires

Your organization must have risk-based processes reasonably designed to identify ACH entries that were initiated due to fraud, particularly fraud involving false pretenses such as Business Email Compromise (BEC), vendor impersonation, payroll redirection, or account takeover.

The rule does not require sophisticated technology or a dedicated fraud team. Your procedures simply need to be appropriate for the size of your organization, the volume of ACH activity you send, and the fraud risks most relevant to your business, and they must be documented and reviewed at least annually.

What We May Ask You to Provide

As your financial institution, we are required under the Nacha Rules to confirm that you have fraud monitoring procedures in place and you have reviewed them at least annually. How we collect that information may vary but the expectation is consistent.

You may be asked to:

- Complete a questionnaire about your current fraud monitoring practices
- Provide a brief written description or summary of your procedures
- Sign an annual attestation or certification confirming your procedures are in place and have been reviewed
- Participate in a conversation or review with your relationship manager

Important: Being unable to describe your fraud monitoring procedures or indicating that none are in place, is not a compliant response. It signals that your organization may not meet Nacha's requirements, which could prompt follow-up from and create risk for your organization. If your current procedures are informal or undocumented, now is a good time to put something in writing. Even a one-page summary of your verification and review steps is a meaningful starting point.

Vendor Payment Controls: Protecting Your Organization Before the Payment Goes Out

Fraud involving vendor payments is one of the most common and costly schemes targeting organizations that use ACH. In many cases, fraud does not involve a system breach. Instead, it exploits gaps in how you verify new vendors, process payment instructions, and handle requests to update banking information. The good news: effective vendor payment controls do not require a large compliance department or sophisticated software. With a few documented procedures and consistent follow-through, you can significantly reduce their exposure.

How Vendor Payment Fraud Happens

The most common scenario is vendor impersonation. A fraudster contacts your team by email, posing as a known vendor, and requests that banking information be updated before an upcoming payment. If that request is processed without independent verification, the next payment goes to the wrong account.

Common warning signs: A request to change payment instructions tied to an upcoming payment. Language describing the change as urgent. An email address that looks similar to but is **not exactly the vendor's real domain**. A callback number provided in the request itself (which may connect to the fraudster, not the vendor).

Controls to Put in Place

Verify banking changes through a separate channel.

Before processing any request to update a vendor's payment, verify it by contacting the vendor directly using a phone number from your own records or the vendor's website, not from the request itself. Document who you spoke with and when.

Require a second set of eyes.

Using dual control within online banking helps protect your organization from payment fraud by ensuring one person cannot both change payment information and initiate or approve a payment. Using the system's built-in dual control features provides stronger protection than relying on manual internal review processes alone.

Set up transaction alerts.

Ask us about setting up alerts for ACH payments.

Write it down.

Put your payment verification steps in writing, even briefly. A simple one-page summary of who can authorize changes and what verification is required is a meaningful starting point and satisfies the documentation expectations under the updated Nacha fraud monitoring rules.

ACH Authorization Obligations

Proper ACH authorization is one of the most fundamental requirements for any organization that initiates ACH payments.

What Authorization Is Required?

The Nacha Operating Rules require that every ACH entry be authorized by the account holder before the transaction is initiated. The format and content requirements vary depending on the type of payment, but the core expectation is consistent: consent must be obtained in advance and documented.

ACH Debits	(Pulling funds from someone else's account) The authorization must be in writing or similarly authenticated, clearly describe the terms of the payment, identify your organization by name, and provide a way for the account holder to revoke consent.
ACH Credits	(Pushing funds, such as payroll direct deposit) A signed authorization form (paper or electronic) is the standard approach. It should identify the recipient, their account information, and the nature of the payment.

Reminder: Any request to change direct deposit or payment account information should be verified directly with the account holder before processing, especially requests received by email. Do not rely on the contact information provided in the change request.

How Long to Keep Authorization Records

Nacha requires that **authorization records be retained for two years from the date the authorization ends or is revoked.** For ongoing relationships, such as a recurring debit or active direct deposit, authorization should be retained throughout the relationship and for two years after the final entry.

Records may be kept in paper or electronic form. What matters most is that they are organized, accessible, and can be produced quickly if your financial institution asks for them.

When a Payment Is Disputed

If an account holder claims a debit was unauthorized, we may receive a return request and ask you to provide a copy of the authorization. If you cannot produce it, or if the transaction did not match the authorization's terms, you will generally be required to accept the return. The simplest way to protect your organization is to obtain authorization before initiating any transaction, keep it on file, and make sure the payment matches what was agreed to.

Contact First American Bank & Trust Commercial Services at cs@fabt.bank or 706-354-5063