epcor
Electronic Payments Core of Knowledge

PAYMENTS INSIDER

The inside scoop on payments for businesses of all sizes

Don't Let New Rules Changes Creep Up on Your Organization

by Trevor Witchey, AAP, APRP, NCP,
Senior Director, Payments Education

By March 20 or June 19, 2026 (*Phase 1*, starting March 20, 2026, applies to non-consumer originators and third-parties with 2023 ACH origination volume of 6 million or more. *Phase 2*, starting June 19, 2026, applies to all remaining non-consumer originators and third parties), ACH Originators must establish and implement risk-based processes and procedures reasonably intended to identify ACH Entries initiated due to fraud. This is part of Nacha's new Origination Fraud Monitoring Rule, designed to keep fraudsters from initiating ACH payments due to unauthorized access or inducing an Originator to send something under false pretenses. If you're unsure how the requirements apply to your organization, check with your financial institution for guidance.

These procedures should be tailored to your role in authorizing and transmitting entries and must be reviewed and updated at least annually to keep pace with evolving fraud risks.

Where to Focus Your Efforts

Most ACH payments are sent to the same Receivers, such as payroll, vendors, utilities, etc., so concentrate your controls on atypical situations that could hide fraud, such as:

- **Brand-New Receivers:** Before initiating a credit, verify the legitimacy of the Receiver. This includes checking identification, performing background checks and confirming signers are authorized representatives. Obtain their authorization legitimately, while ensuring sensitive account information is transmitted securely and/or through an encrypted fashion.
- **Existing Receivers with Account Changes:** If a long-time Receiver sends new account details unexpectedly (especially via email, text or fax), treat it as a red flag. Always verify using known contact information on file (not from an email), not the message that initiated the change. Apply Know-Your-Customer (KYC) practices to confirm the request is valid.

These are the moments when your fraud detection procedures should kick in.

Two Key Compliance Points

- **Point of Transmission:** Under *ACH Rules Section 1.7*, sensitive data like account and routing numbers must be encrypted during transmission. Originators transmitting such data over unencrypted email are at risk and in violation. You're also more vulnerable to business email compromise. Implement encryption and consider tokenization to keep data safe from lurking fraudsters.
- **Point of Authorization:** Per *ACH Rules Subsection 2.3.1*, Originators must obtain valid, legally compliant authorization from the Receiver. This means the method must clearly link the Receiver to the consent. Email alone isn't enough, as anybody could initiate an email and it does not fit legal requirements for an authorization. Instead, use traceable methods like HR systems, written authorizations or voided checks to protect both parties.

Why It Matters

According to the FBI's IC3 2024 report, business email compromise was the second most common fraud type (behind investment fraud, which has escalated recently). Meanwhile, a Center for Payments survey identified "Authorized User was Manipulated" as the top emerging threat. Regardless of size, Originators must document and follow clear procedures to meet the Rule's requirements and reduce fraud exposure.

Reach out to your financial institution to discover the tools they offer to strengthen your fraud defenses. Having more than one set of eyes makes it much harder for fraudsters to succeed—don't let invisible threats haunt your payments.

Catch the ghouls before they strike! Watch EPCOR's Monitoring for Fraud *Did You Know* video for bone-chilling tips on spotting unauthorized activity and be sure to subscribe to EPCOR's YouTube channel, EPCORPymnts, to stay in the know and keep your payments safe from hidden threats.

Stay Informed.

Check out this year's ***2025 ACH Rules Update for Corporate Originators and Third-Party Senders*** to understand the latest requirements and best practices.

Electronic Payments Core of Knowledge

EPCOR is a not-for-profit payments association which provides payments expertise through education, advice and member representation. EPCOR assists banks, credit unions, thrifts and affiliated organizations in maintaining compliance, reducing risk and enhancing the overall operational efficiency of the payment systems. Through our affiliation with industry partners and other associations, EPCOR fosters and promotes improvement of the payments systems which are in the best interest of our members.
For more information on EPCOR, visit www.epcor.org.

Nacha® Direct Member

The Nacha Direct Member mark signifies that through their individual direct memberships in Nacha, Payments Associations are specially recognized and licensed providers of ACH education, publications and advocacy.

www.epcor.org
800.500.0100 | 816.474.5630