

## INSIDE THIS ISSUE

Understanding the 2025 ACH Rules Update for Corporate Originators and Third-Party Senders . . . . .	pg. 1	Significant Third-Party Sender Audit Findings in 2024. . . . .	pg. 3
Significant Third-Party Sender Audit Findings in 2024 . . . . .	pg. 1	Beware of BOI Filing Scams. . . . .	pg. 4

## Understanding the 2025 ACH Rules Update for Corporate Originators and Third-Party Senders

Several significant amendments to the *ACH Rules* are on the horizon. Although new *Rules* do not go into effect until 2026, they will require additional time to prepare and will ultimately impact the way companies process ACH payments. It's essential for corporate Originators and Third-Party Senders to understand these changes to ensure compliance and efficiency in their payment processing operations.

### Standard Company Entry Description

Companies establish the contents of the Company Entry Description field to provide the recipient with a description of the purpose of the payment. A new amendment going into effect in March 2026 will make it so companies initiating (1) Prearranged Payment and Deposit (PPD) credits related to wages/salaries to input a description of "PAYROLL" in the Company Entry Description and (2) e-commerce/online retail purchases (WEB debits) to use "PURCHASE".

### Origination Fraud Monitoring

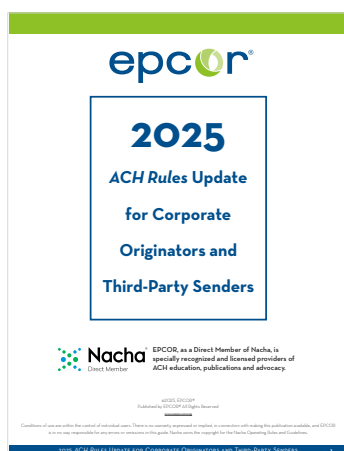
Beginning in March 2026, fraud monitoring will be required regardless of the Standard Entry Class (SEC) code or payment type your company initiates. This is intended to reduce the incidence of successful fraud

attempts. Specifically, your company must establish and implement risk-based processes and procedures to identify payments suspected of being unauthorized or authorized under "false pretenses." Essentially, the expectation is to do your best to detect fraud.

In light of these updates, corporate Originators and Third-Party Senders must

prepare by updating policies, procedures and systems to ensure compliance and effectively mitigate fraud risks.

For more information on these changes, please download this [2025 ACH Rules Update for Corporate Originators and Third-Party Senders](#) document. 📄



## Significant Third-Party Sender Audit Findings in 2024

*By Matthew T. Wade, AAP, APRP, CPA, Senior Manager, Advisory Services, EPCOR*

The ACH Rules require Third-Party Service Providers (TPSPs), which include Third-Party Senders (TPSs), to perform an annual ACH Compliance Audit.

In 2024, EPCOR's expert team performed a record number of these audits for a wide range of TPSPs and TPSs, including payroll processors, bill pay and banking platform providers, healthcare and employee benefit payment companies, government-type payment facilitators and various other payment intermediaries.

Across the spectrum of TPSPs that EPCOR audits, our team frequently sees several audit findings during those engagements.

**Let's discuss the more common and significant audit issues we observed during 2024, along with the suggestions for remediation.**

## Audits

EPCOR performed several first-time ACH Compliance Audits for TPSPs and TPSs in 2024. This is primarily due to the continued influx of new players entering the ACH Network, which is exciting to see as the network continues to grow! There remains a significant number of TPSs that have failed to realize their obligation to conduct an audit. However, as financial institutions continue to make efforts to inform their TPS clients of their audit obligation, requests from these TPSs increase and we hope to see that trend continue. TPSPs and TPSs are reminded by the EPCOR Advisory Team to not only perform the audit annually, but to maintain documentation of those audits for six years as required by the *ACH Rules*. See *ACH Rules, Subsection 1.2.2, Audits of Rules Compliance* for more information.

## Risk Assessments

Another common finding in these audits is the failure of the TPS to conduct an ACH Risk Assessment. While this isn't an annual requirement, TPSs must perform an ACH Risk Assessment per *ACH Rules Subsection 1.2.4, Risk Assessments*, and then establish a risk management program based on that risk assessment. It is worth noting that although the risk assessment requirement only applies to TPSs, it would be wise for other TPSPs to perform risk assessments of their ACH functions as well. To learn more about this, check out our *Did You Know* video, [Risk Management Programs for Third Party Senders](#), where we discuss this topic in more detail.

## Risk Management

ACH risk management is a broad audit topic, and EPCOR offers several key recommendations to TPSs. This requirement derives from two areas of the *ACH Rules, Subsection 1.2.4*, which stipulates that the ACH Risk Assessment be used as the basis for an ACH Risk Management Program and *Subsection 2.2.3, ODFI Risk Management* (which also applies to TPSs). The latter Rule requires the TPS to perform due diligence on each Originator and Nested TPS to assess the nature of the Originator or Nested TPS's ACH activity, implement and enforce exposure limits for each Originator or Nested TPS and monitor ACH return activity.

This can be a tall order, especially for TPS personnel who don't consider themselves bankers, and we often find deficiencies in this area. Missing items include a lack of appropriate ACH-related policies, procedures and controls, failure to establish exposure limits for individual Originators, periodic assessments of individual Originator's ACH activity and insufficient reporting of ACH volumes, returns and losses. There is no defined formula or methodology for an ACH Risk Management Program. TPSs should structure the program based on its business model and ACH use cases, specifically identified ACH risks and their clientele.

However, some key components should include:

1. A thorough know-your-customer (KYC) and onboarding due diligence process,
2. Risk Assessments of individual Originator/Nested TPS ACH activity and
3. Establishment of monitoring and reporting systems.

Office of Foreign Assets Control (OFAC) monitoring continues to be an area of confusion for TPSs. While OFAC is not always seen as a primary ACH compliance issue for TPSPs and TPSs, it remains a key regulation. TPSPs and TPSs share risk with their ODFIs, particularly when third parties are involved. EPCOR auditors have increasingly noted confusion regarding OFAC requirements, with many TPSs unaware of their responsibilities due to a lack of guidance from their ODFIs. TPSs should proactively discuss OFAC requirements with their ODFIs to ensure all parties understand their respective roles and responsibilities.

## Agreements

A very common ACH compliance issue that we run into quite often relates to exceptions or omissions of *ACH Origination Agreement provisions required under Subsection 2.2.2.2, ODFI Must Enter Origination Agreement with TPS*, of the *ACH Rules*. Items (h) and (i) under *Subsection 2.2.2.2* require TPSs to execute ACH Origination Agreements with each Originator or Nested TPS that closely resemble the agreements ODFIs execute with Originators. TPSs tend to have unique contractual agreements with their client Originators, but often the

## Fedwire® ISO 20022 Implementation Rescheduled to July 2025

The ISO 20022 implementation for the Fedwire® Funds Service has been rescheduled for July 14, 2025. This rescheduling also impacts the Financial Institution Reconciliation Data (FIRD) Files, Statement of Account Spreadsheet Files (SASF) and Transaction End-of-Minute (EOM) Detail Reports, all of which will remain on the current format.

For more information on this change, be sure to check out our previous article, [Preparing for Fedwire's ISO 20022 Transformation](#), where we explore how to prepare for this shift.

If you have questions, contact your financial institution or visit the [Fedwire® Funds Service ISO® 20022 Implementation Center](#).

agreements are silent regarding the use of ACH in the services being provided. EPCOR generally recommends TPSs create an “ACH Addendum” to include all the minimum requirements of the *ACH Rules* that can be added to their existing agreements.

### Reinitiated Entries and Micro Entries

Two audit topics that often result in similar findings are Reinitiated Entries and Micro Entries. Compliance issues noted with these types of Entries include improper use, inadequate disclosure on the ACH authorization and improper formatting. The *ACH Rules* related to Reinitiated Entries can be found in *Subsection 2.13.4*, while *Section 2.7* provides the *Rules* related to Micro Entries. The use of these types of Entries is growing, and along with that growth, greater exceptions are bound to follow. Inadequate and unclear disclosures


for Reinitiated Entries and Micro Entries can lead to higher levels of Return Entries, among other issues.

### Final Thoughts

Above are some of the frequent audit issues found by EPCOR during audits of TPSPs and TPSs in 2024. But of course, those don’t represent all issues found. Other audit findings include failure to establish Originator exposure limits, failure to communicate Notifications of Change (NOCs) to Originators in a timely manner, incorrect assignment of Standard Entry Class (SEC) Codes, insufficient authorization language and a lack of monitoring Originator return rates.

If you’re a TPSP or TPS and have any questions or concerns, your financial institution is ready to help! You can also find

a host of resources to help with Third-Party Sender compliance on [EPCOR's Third-Party Sender User page](#), including our *Third-Party Sender ACH Audit & Risk Assessment Workbooks*, which guide you through the process, document your compliance level and provide a report of findings. Additionally, consider becoming an EPCOR member for ongoing support with payments compliance across all payment channels, not just ACH. Membership includes access to exclusive services, webinars, a private Knowledge Community and a toll-free helpline for ongoing questions.

For information about becoming an EPCOR member or to inquire about booking a Third-Party Sender ACH Audit or Risk Assessment, reach out to [advisoryservices@epcor.org](mailto:advisoryservices@epcor.org). 

## Five Key Payments Trends for Businesses to Watch

The payments landscape is evolving rapidly, and businesses must stay informed to remain competitive. Navigating the ever-changing world of payments requires keeping a pulse on emerging trends, regulatory changes and best practices. Here are five critical payment trends that your organization should prioritize in 2025 and beyond.

### 1. RTP® and FedNow® Expansion

The demand for faster, more efficient payment methods is growing. With the introduction of the FedNow® Service, alongside the Real-Time Payments (RTP®) network, businesses can now send and receive funds instantly to improve cash flow management and boost customer satisfaction. Reach out to your financial institution to explore how integrating instant payments can enhance payroll processing, vendor payments and overall liquidity. You can also check out this [repository of use cases](#) from the Faster Payments Council.

### 2. Fraud Prevention and Cybersecurity

As digital payment adoption increases, so do fraud risks. Cybercriminals are leveraging sophisticated techniques such as business email compromise (BEC), synthetic identity fraud and account takeover to target businesses. Businesses must implement artificial intelligence (AI)-driven fraud detection, multi-factor authentication (MFA) and ongoing employee education to safeguard their operations. Stay aware of fraud trends and mitigation techniques by monitoring communications from your financial institution. You can also find a vast library of helpful videos on EPCOR's YouTube Channel, [EPCORPymnts](#). Be sure to subscribe to stay up to date with the latest insights!

### 3. Regulatory Compliance and Payment Standards

Regulations continue to evolve, impacting how businesses handle electronic payments. Updates from Nacha, Payment Card Industry Security Standard Council

(PCI DSS) and the Consumer Financial Protection Bureau (CFPB) are reshaping compliance requirements. Organizations that process ACH transactions or card payments must ensure they meet the latest standards to avoid potential fines or disruptions.

In our previous article, [Your Beneficial Ownership Information Requirements](#), we outlined the critical compliance steps businesses need to follow to ensure they meet ownership disclosure requirements. As regulatory changes unfold, stay informed by reading future editions of *Payments Insider* for the latest news and updates to help your organization remain compliant.

### 4. Embedded Finance and Banking-as-a-Service (BaaS)

More businesses are embedding financial services into their platforms, blurring the lines between traditional banking and Fintech. Businesses can leverage BaaS solutions to offer customers seamless

financing and payments insurance options. Whether you're in retail, manufacturing or professional services, embedded finance can create new revenue streams and enhance customer experience. Reach out to your financial institution to explore options.

### 5. The Role of AI and Machine Learning in Payments

AI is revolutionizing payment processing by improving fraud detection, automating routine transactions and personalizing

customer interactions. Organizations that adopt AI-driven payment solutions can enhance efficiency, reduce errors and provide better service. Contact your financial institution to learn how AI can be effectively integrated into your payment operations.

As these trends continue to evolve, staying ahead of the curve will be critical to your organization's success. For ongoing updates and in-depth strategic insights, *Payments*

*Insider* will continue to be your go-to resource. In addition to this newsletter, consider exploring other valuable resources such as Did You Know videos, available on EPCOR's [website](#) and [YouTube](#) channel. These videos explain essential payments topics in just a few short minutes, and the fun format and easy-to-understand language make them perfect for passing along important information to staff or customers. 🎧

## Beware of BOI Filing Scams

The Financial Crimes Enforcement Network (FinCEN) recently issued an alert regarding fraud schemes that abuse its name, insignia and authorities for financial gain. These scams target companies working to comply with the ongoing implementation of the Corporate Transparency Act (CTA) and file BOI forms with FinCEN. Scammers are taking advantage of this process, attempting to deceive businesses into paying unnecessary fees for fraudulent services and steal proprietary information. The CTA mandates that certain companies file their BOI with FinCEN, detailing information about their beneficial owners (individuals who own or control the company). These filings are essential for reducing financial crimes such as money laundering. Businesses can complete their BOI filings directly with FinCEN for free via their official website, [FinCEN.gov](#).

Three common BOI filing scams that your organization should watch out for include:

- 1. Form 4022:** A form sent by the "United States Business Regulation Department" demands a \$117 fee for a "Mandatory Beneficial Ownership Report". This form is fraudulent, and no such department exists.
- 2. Form 5102:** Mailed by the "Annual Records Service," this form claims to be an updated version of "Form 4022" and requests a \$119 fee. Like "Form

4022," this is not a legitimate filing and only serves to deceive businesses into paying scammers.

- 3. C.P.S. Form:** Sent by "C.P.S.," this form falsely claims to submit paper filings to FinCEN and requests a fee between \$175 and \$195. FinCEN does not accept paper forms, and this request is illegitimate.

Organizations that pay these fraudulent fees and submit the incorrect forms may believe they are fulfilling their legal obligations, but in reality, they are not submitting the information as required by law. As a result, organizations that fail to properly file may be in violation of federal law, potentially facing penalties.

**BOI filings can be completed directly through FinCEN at no cost.** These [fraudulent entities](#), including the "United States Business Regulation Department," "Annual Records Service" and "C.P.S.," are under investigation by the U.S. Department of the Treasury for scamming organizations and collecting money for services that don't exist.

### How to Protect Your Organization:

- 1. File directly with FinCEN:** The BOI filing process is available for free directly through FinCEN's [website](#). Avoid paying third-party entities that

offer to submit filings for a fee.

- 2. Don't trust unsolicited forms:** Legitimate filings from FinCEN will not require substantial fees or come through unknown third parties. Be suspicious of forms or emails requesting fees for BOI filings.
- 3. Verify with FinCEN:** If you receive any suspicious form or request for money, it's crucial to contact FinCEN directly to confirm its legitimacy. You can visit FinCEN's [BOI page](#) to learn more about the filing process.
- 4. Educate your business:** FinCEN provides [updated FAQs](#) and resources to help organizations understand and comply with BOI filing requirements.

Scammers are actively targeting organizations by creating fake forms and charging unnecessary fees for services that don't meet legal requirements. By staying informed, verifying all correspondence with FinCEN and only filing directly with the official government agency, you can avoid falling victim to these harmful scams. If you've received suspicious forms or have questions about legitimate BOI filings, visit FinCEN's official [website](#) for assistance. 🎧

Sources: *FinCEN and Mississippi Secretary of State*