epcor
Electronic Payments Core of Knowledge

PAYMENTS INSIDER

The inside scoop on payments for businesses of all sizes

INSIDE THIS ISSUE

The ACH Fraud Monitoring Rules Are Now Effective

by Shelly Sipple, AAP, AFPP, APRP, NCP, Director, Certifications & Continuing Education

The new ACH Fraud Monitoring Rules are no longer a future requirement. They're now effective for everyone, so if your organization originates ACH payments, the changes now apply to you.

Need a refresher on all *ACH Rules* changes taking effect in 2026 and beyond? Review EPCOR's *2026 ACH Rules Update for Corporate Originators and Third-Party Senders*.

What's Changed?

Under the new Rule, your company as an ACH Originator must establish and implement risk-based processes and procedures designed to identify payments that are unauthorized or originated under false pretenses. These fraud-monitoring processes must be:

- Tailored to your organization's operations and risk profile.
- Reviewed and updated at least annually and
- Focused on areas where fraud is most likely to occur.

The Rule also applies to Third-Party Senders (TPSs) and Third-Party Service Providers (TPSPs), reinforcing fraud prevention responsibilities throughout the ACH payment chain.

Why the Change Matters

Businesses acting as Originators are often best positioned to identify suspicious activity before fraudulent transactions enter the ACH Network. This Rule is designed to strengthen fraud prevention by requiring companies to take a proactive, risk-based approach to monitoring ACH activity.

Building Your Risk-Based Fraud Monitoring Process

While the Rule does not prescribe specific procedures, two areas deserve particular attention:

New Payment Receivers. When establishing new Receiver relationships—such as with employees, customers, members or vendors—consider the following steps:

- Requesting supporting documentation,
- Verifying identities and authorized personnel,
- Conducting background checks when appropriate,
- Using secure methods to transmit account information and
- Confirming authorization forms meet *ACH Rules* requirements.

Tip: Maintain a verified contact on file for future validation and protect stored account information through appropriate security controls.

Account Change Requests. When an existing payment Receiver requests updated account information, proceed carefully:

- Accept only valid signed or authenticated authorization requests,
- Verify changes using existing contact information already on file,
- Apply Know Your Customer (KYC) procedures where appropriate and
- Follow dual-control and multi-factor authentication practices.

Tip: If dual-control procedures are not already in place, now is a good time to evaluate them as an additional safeguard against fraud.

Ongoing Review Is Essential

Fraud threats continue to evolve, and your controls should evolve with them. The Rule requires your company to review and update their fraud-monitoring processes at least annually to ensure they remain effective.

With this Rule now in effect for all, it is time to confirm that your procedures are documented, risk-based and compliant with the Rule's requirements. Acting today can help reduce the risk of fraud while supporting the continued integrity of the ACH Network.

Understanding ACH Agreements: What Businesses Need to Know

by Amy Donaghue, AAP, APRP, NCP, Director, Third Party, Risk and Compliance, EPCOR

ACH payments have become a central component of how organizations move money today. Businesses rely on ACH for payroll, vendor payments, recurring customer billing and countless other transactions.

If your organization originates ACH payments, either directly through a financial institution or on behalf of clients as a Third-Party Sender (TPS), an ACH Origination Agreement plays an important role in establishing expectations, managing risk and supporting compliance with the *ACH Rules*.

While many organizations sign these agreements during account setup and rarely revisit them, understanding their purpose can help reduce operational disruptions, strengthen fraud prevention efforts and support reliable payment processing as your organization grows.

Why ACH Origination Agreements Matter

An ACH Agreement establishes the expectations and responsibilities of everyone involved in the payment process. It helps define how ACH transactions should be authorized, transmitted and managed, while outlining the obligations of both the business and the financial institution or payment provider.

A comprehensive agreement helps establish compliance with *ACH Rules* requirements, define responsibilities for authorizations, returns and dispute handling, support fraud prevention and security practices and clarify procedures for addressing issues when they arise.

By having clear documentation of these expectations, businesses can help reduce risk, avoid payment disruptions and support more efficient ACH operations.

Protecting Your Business

ACH Origination Agreements often include provisions designed to help protect both the business and the financial institution from losses resulting from fraud, unauthorized transactions, processing errors or other payment-related risks.

These provisions may address topics such as:

- Security and authentication requirements
- Authorization and record retention expectations
- Transaction limits and risk controls
- Reporting procedures for suspicious or unusual activity

Understanding these requirements can help businesses strengthen internal controls, protect sensitive information and maintain reliable payment operations.

And, while many businesses originate ACH payments solely for their own organization, some originate ACH transactions on behalf of other companies and have additional responsibilities under the *ACH Rules*.

Additional Considerations for Third-Party Senders

Some organizations originate ACH transactions on behalf of other companies. These organizations are known as Third-Party Senders (TPSs).

Because TPSs act as intermediaries between Originators and the ACH Network, they have additional responsibilities under the *ACH Rules*. TPSs are required to maintain agreements with their clients that clearly define responsibilities related to ACH origination, authorizations, security, risk management and compliance.

For TPSs, comprehensive agreements are more than a business best practice—they are an important component of maintaining a sound compliance and risk management program. Clear agreements help establish expectations, allocate responsibilities and support effective oversight of ACH activity conducted on behalf of clients.

The Takeaway

Whether your organization originates ACH payments for its own business purposes or on behalf of clients, ACH Origination Agreements play an important role in supporting safe, compliant and efficient payment operations.

These agreements help:

- Define responsibilities and expectations
- Support compliance with the *ACH Rules*
- Strengthen fraud prevention and security controls
- Clarify procedures for resolving issues
- Provide a framework for managing risk

By understanding the purpose of your ACH Origination Agreement and revisiting it when your payment activity, services or business model changes, you can help support reliable ACH operations and reduce potential risks associated with payment processing.

Instant Payments Are Becoming a Business Tool, Not Just a Faster Way to Move Money

by Sharon Hallmark, AAP, AFPP, APRP, Director, Payments Education, EPCOR

Instant payments in the U.S. are entering a new phase of maturity. According to the *2025 U.S. Instant Payments Adoption Quantitative Study* from the U.S. Faster Payments Council (FPC), adoption is increasingly being driven by practical business use cases rather than the novelty of moving money in seconds. The conversation is shifting from speed to business value, focusing on how organizations can improve cash flow, create better client experiences and gain greater control over payment timing.

The study suggests that success in this next phase will be driven less by payment speed alone and more by relevance, trust and thoughtful implementation. Businesses are beginning to recognize that instant payments are most valuable when they solve specific operational challenges and support critical moments in the client journey.

Business Use Cases Are Driving Adoption

While early instant payment adoption was fueled by client-focused use cases such as earned wage access, wallet funding and peer-to-peer (P2P) payments, business use cases are becoming increasingly important. The FPC's research found growing interest in applications such as loan disbursements, business-to-business (B2B) payments and invoice-related payment flows.

Several business scenarios highlight where instant payments can create meaningful value:

- **Insurance claims payouts:** Following a vehicle accident, natural disaster or other insured event, businesses can deliver approved claim payments immediately rather than requiring clients to wait days or weeks for a paper check. Faster access to funds can significantly improve customer satisfaction during high-stress situations.
- **Transportation and logistics:** Small trucking companies and independent carriers often face significant cash flow challenges while waiting for payment. Instant payments allow factoring platforms and shippers to release funds immediately after delivery, helping businesses cover fuel, maintenance and operating expenses without delay.
- **Just-in-time B2B payments:** Businesses can pay suppliers precisely when funds are due, improving liquidity management while providing suppliers with immediate access to funds. Recent research found growing business interest in both supplier payments and just-in-time B2B payment scenarios.
- **Urgent client payments:** Organizations can issue refunds, rebates, reimbursements and other time-sensitive disbursements instantly, improving client experience while reducing administrative overhead.

As transaction limits on both the RTP® Network and the FedNow® Service have increased to $10 million, instant payments are also becoming more practical for larger-value commercial transactions that previously may have relied on traditional payment methods.

Control and Visibility Matter More Than Speed

For businesses, the value of instant payments extends beyond faster settlement. Instant payments provide certainty, finality and visibility into when funds are received or delivered.

Unlike traditional payment methods that may require businesses to estimate settlement timing, instant payments allow organizations to manage liquidity with greater precision. Businesses can hold funds longer when needed, pay suppliers at exactly the right time and gain immediate confirmation that payments have been completed.

This level of control is becoming increasingly important as treasury teams seek ways to optimize working capital and improve forecasting accuracy. Businesses are finding that the ability to pay precisely when necessary often delivers greater value than simply paying earlier.

Trust and User Experience Remain Critical

As adoption expands, trust continues to play a central role. The FPC's study identified fraud mitigation tools as one of the highest priorities for future growth in instant payments, alongside improvements to business user interfaces and payment exception handling.

Businesses evaluating instant payments are looking for:

- Strong fraud detection and risk management tools,
- Clear payment confirmations and visibility into transaction status,
- Seamless integration with treasury, accounting and enterprise resource planning (ERP) systems and
- Straightforward exception and dispute management processes.

Organizations that combine strong controls with intuitive payment experiences will be best positioned to maximize the benefits of instant payments.

Request for Payment: A Growing Opportunity for Businesses

Request for Payment (RfP) is emerging as one of the most promising opportunities for expanding instant payments within business workflows. RfP enables a business to send a digital request for payment directly to a client or counterparty, who can then authorize the payment in real time.

Potential applications include:

- Invoice payments,
- Supplier payments,
- Supply chain finance,
- Subscription and recurring billing scenarios and
- Loan repayment requests.

While adoption is still developing, industry participants view RfP as a key component in bringing instant payments deeper into accounts receivable and B2B payment processes. Success will likely depend on focusing on specific, high-value use cases rather than broad deployment across every payment scenario.

From Faster Payments to Better Business Outcomes

The future of instant payments is not simply about moving money faster. Businesses are increasingly viewing instant payments as a tool to improve cash flow, strengthen client relationships and create more efficient financial operations.

Whether providing immediate insurance payouts, enabling faster freight payments, improving supplier payment timing or streamlining invoicing processes, the most successful implementations will focus on business outcomes rather than payment speed alone.

As instant payment capabilities continue to expand, organizations that align technology, risk management and practical business use cases will be best positioned to realize the full value of real-time payments.

Sources: The U.S. Faster Payments Council and The Clearing House

Understanding Double-Sided Spoofing: A Growing Fraud Threat

by Madison Howard, Director, Marketing & Communications, EPCOR

Fraudsters are constantly finding new ways to trick clients into sharing sensitive information. One increasingly common tactic is double-sided spoofing, a sophisticated scam that allows criminals to impersonate both a trusted organization and a client simultaneously.

Understanding how this scam works can help you recognize the warning signs and better protect your accounts and personal information.

What Is Double-Sided Spoofing?

Double-sided spoofing occurs when a fraudster impersonates a legitimate organization, such as a financial institution, credit card company, utility provider or government agency, while simultaneously pretending to be the client when communicating with that organization. By controlling both sides of the conversation, scammers can create a convincing scenario that appears legitimate and trustworthy.

How the Scam Works

A double-sided spoofing attack often begins with a phone call, text message or email that appears to come from a trusted source. The fraudster may claim there is suspicious activity on an account, a security concern that requires immediate attention or another urgent issue that requires verification.

While communicating with the client, the scammer also contacts the legitimate organization and attempts to access the client's account. If additional authentication is required,

the organization may send a one-time passcode or verification code directly to the client.

The fraudster then asks the client to provide that code, often claiming it is needed to verify their identity or resolve the issue. Once the code is shared, the scammer can use it to gain access to the account or complete unauthorized transactions.

Why This Scam Is Effective

Double-sided spoofing can be particularly convincing because the verification code or security alert is real. The client receives legitimate communication from their financial institution or service provider, making it appear that the caller is genuine.

However, the code was generated in response to the fraudster's attempt to access the account. This tactic allows criminals to bypass security measures that are designed to protect clients from unauthorized access.

Victims of double-sided spoofing may experience unauthorized account access, financial losses, identity theft, fraudulent transactions and significant time and effort spent restoring account security.

How to Protect Yourself

- **Never Share Verification Codes.** One-time passcodes, authentication codes and security verification codes should never be shared with anyone who contacts you unexpectedly. Legitimate organizations generally will not ask you to provide these codes over the phone, by text message or through email.
- **Verify the Request Independently.** If you're contacted regarding an account issue, reach out to the organization directly using a phone number listed on its official website, mobile app, account statement or the back of your debit or credit card. Do not rely on the contact information provided in the suspicious message.
- **Be Cautious of Urgent Requests.** Scammers often create a sense of urgency to pressure victims into acting quickly. Be wary of messages that threaten account closure, service interruptions or financial loss if immediate action is not taken.
- **Use Multi-Factor Authentication.** Whenever available, enable multi-factor authentication (MFA) to add an extra layer of security to your accounts. While MFA is an important security tool, remember that authentication codes are intended for your use only and should never be shared with another person.
- **Stay Alert.** Fraudsters continue to adapt their tactics, making scams increasingly difficult to identify. Taking a moment to verify unexpected requests and safeguarding your authentication credentials can significantly reduce the risk of becoming a victim.

If you believe you have shared sensitive information or provided a verification code to a scammer, contact your financial institution immediately to report the incident and secure your accounts.

Keep Your Payments Education HOT All Summer Long!

Summer is heating up, and while plans may ease into vacation mode, payments education is still in the sizzlin' spotlight. This is the season to keep your knowledge sharp, your tools close and your compliance confidence steady.

Resources to Keep in Your Summer Lineup:

The ***ACH Quick Reference Guide for Corporate Users*** keeps the essentials right at your fingertips with a clear breakdown of key *ACH Rules* every Originator needs when things move fast.

Did You Know videos deliver quick, punchy bursts of learning that break down fraud trends, scam tactics and more in short clips that are easy to watch and remember. These videos are available on EPCOR's **website**, **LinkedIn** and **YouTube** channel.

The **Business User Webpage** and **Third-Party Sender Webpage** are excellent resources for tools, updates and videos you can access anytime.

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.

epcor.org
800.500.0100 | 816.474.5630