epcor
Electronic Payments Core of Knowledge

PAYMENTS INSIDER

The inside scoop on payments for businesses of all sizes

INSIDE THIS ISSUE

Outsourced, Not Out of Mind: Navigating Third-Party ACH Risk ..... pg. 1

Countdown to Conversion: Preparing for the Fedwire® ISO 20022 Shift ..... pg. 3

Tokenization Tips: Managing Data Security with Fintech Partners ..... pg. 4

Outsourced, Not Out of Mind: Navigating Third-Party ACH Risk

by Amy Donaghue, AAP, APRP, NCP, Director, Advisory Services – Risk & Third-Party Services and Matthew T. Wade, AAP, AFPP, APRP, CPA, Senior Manager, Advisory Services

In today's interconnected business landscape, organizations are increasingly turning to Third-Party Service Providers (outside companies or vendors that handle specific operational tasks) to manage critical operations, including ACH transactions. This can include vendors to help with file creation, payroll processors, accounting firms or any entity you contract with to assist with your ACH processing.

While outsourcing can drive efficiency and reduce costs, it also introduces significant risks that must be carefully managed. Implementing robust Third-Party Risk Management practices—particularly around ACH Risk Assessments and Compliance Audits—is essential to maintaining operational integrity, regulatory compliance and financial security.

Why Third-Party Risk Management in ACH Processing is Critical

ACH transactions represent a significant portion of electronic payments in the United States, processing trillions of dollars annually. When you outsource a portion of your ACH processing to Third-Parties, you're essentially entrusting them with your organization's financial reputation and regulatory standing. A comprehensive risk assessment helps to identify potential vulnerabilities in systems, processes and controls before they impact any operations. These vulnerabilities could leave your organization exposed to service disruptions, data breaches or compliance violations that could severely affect day-to-day operations. Additionally, Originators and Third-Party Senders in the ACH Network must comply with the *ACH Rules*, U.S. law and various industry standards. Regulatory bodies expect all organizations participating in the ACH Network, including businesses, to maintain oversight of their Third-Party relationships, making due diligence not only a best practice but a compliance necessity.

Requesting Evidence of Completed Audits and Risk Assessments

When engaging with Third-Party Service Providers, it's important to request formal documentation such as annual ACH Risk Assessments conducted by qualified auditors, independent audits of ACH processing controls, compliance

certifications relevant to ACH operations and security assessments—including penetration testing and vulnerability assessments.

A request should include documentation specifying an executive summary of risk assessment findings, detailed audit reports with management responses, evidence of remediation for identified deficiencies, certifications from qualified auditors or assessment firms and documentation of ongoing monitoring and testing procedures. These materials demonstrate the vendor's commitment to continuous improvement and help validate the independence and credibility of their evaluation processes.

Requesting a comprehensive documentation package helps establish a clear understanding of the vendor's risk profile and provides a baseline for ongoing oversight. This formal approach ensures the necessary evidence is available to make informed decisions about the relationship and maintain appropriate documentation for your own regulatory compliance requirements.

Assessing the Adequacy of Third-Party Audits and Risk Assessments

When evaluating Third-Party Audit and Risk Assessment documentation, verify that assessments were conducted by firms with demonstrated knowledge of the *ACH Rules* and banking regulations. Look for evidence that the evaluation covered technical controls, including system security, access controls and data encryption, as well as operational controls such as transaction processing procedures and exception handling. Additionally, ensure the assessment addresses compliance controls adhering to the *ACH Rules* and regulatory requirements and business continuity measures, including disaster recovery and backup procedures.

Also, confirm assessments are conducted frequently (we recommend annually), updated when significant system or process changes occur and supplemented by ongoing monitoring activities. Watch for red flags, including:

- Vague or generic findings that lack specific detail,
- Absence of management responses to identified deficiencies,
- Limited scope that excludes critical ACH processing components,
- Outdated assessments or gaps in assessment frequency and
- Lack of independent verification, where only self-assessments were performed.

These indicators help determine whether the vendor's risk management practices meet your standards for partnership.

In summary, effective Third-Party Risk Management for ACH processing requires proactive engagement across multiple critical areas. You must first understand why Third-Party Risk Management over ACH processing is critical and recognize that outsourcing these functions exposes your organization to operational, compliance and reputational risks that could significantly impact your business. Once you appreciate these risks, take action by requesting evidence of completed audits and risk assessments from your vendors to ensure they can demonstrate their commitment to proper risk management through comprehensive documentation. However, simply receiving documentation isn't enough; you must also develop the expertise to assess the adequacy of Third-Party Audits and Risk Assessments, evaluating whether the scope, depth and quality of their risk management practices meet your standards and regulatory requirements.

By understanding the importance, requesting proper evidence and critically evaluating what you receive, you create a robust framework that protects your organization while enabling you to realize the benefits of strategic outsourcing partnerships.

Make Waves with Payments Education this Summer

As the days get longer and business planning heats up, now's the perfect time to refresh your payments education strategy. Whether you're training new staff, planning for retirements or looking to boost compliance, these tools will help you stay ahead:

ACH Quick Reference Guide for Corporate Users: This guide offers an easy-to-follow overview of key *ACH Rules* every Originator should know.

***Did You Know* Videos**: Short, animated videos that break down complex payments topics including common scams, fraud prevention, Third-Party Sender identification and so much more into quick, shareable clips. These videos are available on EPCOR's website, LinkedIn and YouTube channel.

Payments Insider: This semi-annual newsletter, which you're reading now, is always available on EPCOR's Corporate User webpage and delivers updates on payments trends and rule changes, including a special *ACH Rules* Update each April.

Corporate User Webpage: Your hub for up-to-date resources, rule change alerts, video links and more. Visit epcor.org/corporateuser.

Make a splash with your payments education — no pool floaties required!

Countdown to Conversion: Preparing for the Fedwire® ISO 20022 Shift

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

On July 14, 2025 the Federal Reserve Bank will transition its payments format from the Fedwire® Application Interface Manual (FAIM) to the ISO 20022 XML format, which is already adopted by over 70 countries and integrated with instant payment systems like the RTP® Network and the FedNow® Service. Think of this wire format change like switching from roller skating on pavement to ice skating on ice; there are different surfaces, but the same basic skills and precautions apply.

First, let's clarify participant labels. ISO uses different names for participants than those used in the FAIM format. See our comparison chart (right) for reference.

The account being debited is the "Debtor," while the account receiving the credit is the "Creditor." "Instructing" sends the payment, whereas the past tense "Instructed" is receiving it. There can also be "Ultimate" Debtors or Creditors—those who ultimately own or control the accounts involved, such as in Third-Party or complex ownership scenarios. These roles existed in the FAIM format as well.

Sending wires through the ISO 20022 format is a bit different than with the previous FAIM format. With FAIM, the name and address fields were free-form entry with four rows of data, 35 characters in length. ISO 20022, on the other hand, has a more structured format that requires different address elements to be in specific spaces. For example:

FAIM format:

- Field 1: John Doe
- Field 2: 123 Main Street
- Field 3: Columbus, OH 33333
- Field 4: (unused, remains blank)

ISO 20022 format:

- Name field: John Doe
- Street Name element: Main Street
- Building Number element: 123
- Post Code element: 33333
- Town Name element: Columbus
- Country Subdivision (state) element: OH or Ohio
- Country element: United States of America

Sending wires through the ISO 20022 format requires entering information in a precise, standardized way. Unlike the FAIM format, where name and address details were entered as free-form text across four lines, ISO 20022 breaks down each piece of data such as street name, building number, city, state, postal code and country into individual, designated fields.

If you're concerned about address data entry, the Federal Reserve's September 3, 2024 memorandum allows free-form entry for now, but only as an interim solution. Eventually, full ISO 20022 formatting may be required, so it could be wise to start adopting it early.

Since FAIM and ISO 20022 use different formats, particularly for address entry, Fedwire® and many other vendors likely won't be able to convert their existing templates. It's a good idea to check with your account representative and begin recording key recurring wires now to ensure a smooth transition on day one.

From what we can see in the Fedwire® documentation, wires sent to other businesses or consumers, settlement wires between financial institutions and drawdown wires (using the request-for-credit ISO process) will continue to function as they have—just in a different format. For exceptions, such as retrieving wires sent in error or due to fraud, or communicating with another financial institution via service messages, the Request for Return and investigation process should serve the same purpose as under the FAIM format, with the added benefit of ISO 20022's enhanced transparency and richer data to help clarify the type or subtype of situation may be occurring.

For more information, contact your Federal Reserve account representative or your vendor. Also, we encourage downloading the Fedwire® documentation from Swift's MyStandard's website, along with utilizing the Fedwire® implementation center website. At EPCOR, we have a recording of our *Getting to Know ISO 20022* webinar, as well as ISO 20022 vs. FAIM comparisons for 2025 in our *Wire Transfer Quick Reference Guide* publication.

Comparison of Participant Labels

FAIM Participant	ISO 20022 Participant
Originator	Debtor
Originating Financial Institution*	Debtor Agent*
Sending Financial Institution	Instructing Agent
Receiving Financial Institution	Instructed Agent
Beneficiary Financial Institution*	Creditor Agent*
Receiver	Creditor

**Used for correspondent FI situations*

Tokenization Tips: Managing Data Security with Fintech Partners

As organizations increasingly turn to Fintech platforms for efficiency and scale, many are relying on these providers to tokenize bank and credit union account information used in ACH transactions. While tokenization is a powerful security tool, improper implementation (particularly in ACH Origination) can cause operational disruptions, compliance gaps and reputational risk.

Tokenization replaces an account number with a surrogate value or "token" that can be used in place of sensitive data during processing to reduce the exposure of actual account numbers and help protect against fraud. In 2022, Nacha, the governing body for ACH, modified *Article One*, *Section 1.6* of the *ACH Rules* to require ACH Originators with transmission volume exceeding two million Entries annually to protect Depository Financial Institution (DFI) account numbers used in the initiation of Entries by rendering them unreadable when stored electronically. While the *Rules* don't define what technology should be used to render data unreadable, encryption is a popular option due to the flexibility, security and efficiency provided.

Companies using tokenization should also be mindful that tokenization practices align with other state and federal rules and regulations such as Anti-Money Laundering (AML) and Bank Secrecy Act (BSA) laws.

Here are some things to keep in mind:

- Tokenized data should remain traceable to the original account number. Data should remain available to resolve disputes, respond to fraud claims or support audits.
- Tokenization cannot be used to obscure the identity of the account holder or bypass compliance obligations.
- Secure data mapping and appropriate governance must be maintained throughout the token lifecycle.

What This Means for Your Organization

If you rely on a Fintech platform or service provider that uses tokenization when processing ACH payments, it's your responsibility to ensure they are following compliant tokenization practices. Improper use of tokenization can result in:

- Rejected transactions that disrupt vendor payments, payroll or consumer refunds.
- Increased fraud risk due to weak mapping or poor visibility.
- Findings of non-compliance during audits and regulator reviews.

To evaluate how your partners manage tokenized data, consider these steps:

- Review your vendor agreements and request documentation about their tokenization approach.
- Ask your Fintech provider how tokens are mapped to original account data, and how they ensure traceability and audit readiness.
- Educate appropriate staff members about tokenization risks and what to look for in provider due diligence.

As ACH fraud continues to evolve and attention mounts surrounding data security, tokenization should be seen as a security enhancement, not a shortcut. By partnering with providers that implement tokenization the right way, you can enhance your payment security posture without compromising on compliance.

Source: Nacha

June is Elder Abuse Awareness Month

Just because it's summer doesn't mean scammers are on vacation. Financial exploitation is the fastest-growing form of elder abuse, and being able to spot these red flags in your organization's operations can help protect those most vulnerable:

- Be cautious of unusual or urgent refund or payment requests tied to older customers or clients.
- Watch for new contacts attempting to change payment instructions or account details without clear explanation or authority.
- Take note if an older customer seems confused or unsure when discussing invoices, transactions or billing details.

EPCOR's *Did You Know* video on financial elder abuse is a quick, powerful way to spread awareness. Share it with your team or with clients to help support those who may be at risk. For even more tools to recognize and prevent abuse, check out the National Center on Elder Abuse.

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