epcor
Electronic Payments Core of Knowledge

PAYMENTS INSIDER

The inside scoop on payments for businesses of all sizes

INSIDE THIS ISSUE

2023 *ACH Rules* Update for Corporate Originators and Third-Party Senders

As an Originator of ACH entries, it is important to stay current with the *ACH Rules*, including how updates and changes might impact your business. Phase 2 of the Micro-Entries Rule and the expiration of the grace period for Third-Party Sender Roles and Responsibilities are changes on tap for 2023. Get up to speed on these revisions and how they will affect your organization by downloading the *2023 ACH Rules Update for Corporate Originators and Third-Party Senders*. If you have any questions about how these changes may pertain to your existing Origination activities, contact your financial institution.

Is Your Business Ready for Faster Payments?

by Rachel Mindell, Modern Treasury

The following article originally appeared on ModernTreasury.com.

The speed and convenience of faster payments can make them feel effortless. A client presses a button and money moves instantly to their investment account. A company sends an e-invoice to their vendor and receives payment in seconds. Of course, the time, thought and tech that permit this experience aren't effortless. From enablement and execution to upkeep, faster payments like RTP® and FedNow℠ (forthcoming mid-year 2023) require solid preparation from the start.

4 Elements of Faster Payments Readiness

If you're implementing RTP®, prepping for FedNow℠, or both, there are four factors to prioritize during preparation. Spending time on each will make your company's route to quick, smooth payment experiences faster and easier the whole way through.

1. Strategy

To get the greatest advantage from faster payments, invest in research and strategic planning. Your roadmap for faster payments adoption should include the following:

- **Understand offerings and opportunities.** Each faster payment rail has unique qualities, requirements, limits and applications. This list of potential use cases for FedNow℠, as an example, will give you a sense for what is possible.
- **Consider alignment with your business goals.** Given the faster payments options (including business, commercial and internal uses), which

see FASTER on page 2

FASTER continued from page 1

use cases will you prioritize and how well does adoption match up with higher-level goals?

- **Weigh the opportunity costs.** Launching and managing faster payments is a commitment that requires both resources and retooling at multiple levels (see below). Will potential gains justify this investment?

2. Partnerships

Without the right financial institution partnership, your business won't be able to capitalize on faster payments.

While RTP® is currently available at more than 280 financial institutions, FedNow℠ is likely to have much wider coverage. As it stands, businesses interested in FedNow℠ should speak with their financial institution to see what plans (if any) are in place.

At launch, the 12 Reserve Banks and financial institutions in the FedNow℠ Pilot Program will offer FedNow℠. There are more than 120 organizations (financial institutions as well as payment processors and solution providers) in the pilot program, including JP Morgan Chase, Silicon Valley Bank and Wells Fargo.

Beyond banking relationships, you'll want to consider current partnerships that may be impacted by faster payment adoption—as well as potential partnerships this new technology could benefit from.

3. Technology

Faster payment rails, like any other rail, require technology to support the full cycle of each payment. Necessary capabilities and infrastructure using ISO 20022 include:

- Payment initiation and approvals
- Funds tracking and failure management
- Reconciliation, ledgering and controls

You may also need to manage counterparties and virtual accounts. And, given that faster payments are always on, this infrastructure has to function continuously and autonomously around the clock.

Building an in-house payment operations solution can be complex and costly, especially if you're just standing up a single rail. Modern Treasury estimates, based on client data, that it requires thousands of hours of devoted time to create an effective money movement solution. This data does not account for the need to build a compliance program or ongoing management, maintenance, reliability checks and improvements—an investment of hundreds of hours per year. It's also likely that breaks and errors will happen outside traditional working hours, putting extra pressure on teams to build (and maintain) diligently.

4. Processes and Tools

Faster payments require upgraded workflows. What works for finance and operation teams handling transactions in batches (daily, weekly or monthly) won't work for 24x7x365 payments. It's not feasible to staff these roles around the clock—it's also a poor use of team resources.

For offerings like RTP® and FedNow℠, you'll need systems that run around the clock, independently, and even on holidays. And given that over 75% percent of the hours in a week fall outside a standard workday—the most convenient time to complete personal transactions for most consumers—coverage is key.

Faster payments require that you fully automate your entire payments workflow, including the tasks currently done by staff that impact said flow.

As you consider processes affected by faster payments, examine the tools and software in your current tech stack—it may be time to add or consolidate solutions. For a new rail, if you engage a service provider, you'll want to seek out an API-based solution built for end-to-end money movement. If you're already managing multiple rails across financial institutions, it may be time to centralize these workflows within a single platform primed for faster payments.

If you have any questions or are interested in faster payments, reach out to your financial institution.

Source: Modern Treasury

New Third-Party Sender ACH Rule: Your Ducks Should Now Be in a Row!

by Emily Nelson, AAP, APRP, NCP, Manager, Payments Education, EPCOR

On September 30, 2022, the Third-Party Sender (TPS) roles and responsibilities under the *ACH Rules* were updated. The purpose of the amendments made, as addressed on page ORxxxv, was to clarify existing practices surrounding Nested TPS relationships and make explicit the requirement for a TPS to conduct a risk assessment. *Supplement #3-2021* also indicated a six-month grace period for certain aspects of each of the rules, but that grace period expires on March 31st.

Under these changes, as a TPS, it is now necessary for you to identify any Nested TPS relationships for which you process ACH transactions. You must determine if the client you are processing for is processing on its own behalf, or on behalf of others for whom the client has sold its services. If your client is processing on behalf of their clients, your client could qualify as a Nested TPS. You, the TPS with the direct relationship with the Originating Depository Financial Institution (ODFI), will want to ensure that you have an origination agreement in place with each Nested TPS and that your Nested TPS has an agreement with their client. This reflects the requirements of *Subsection 2.2.2.2, ODFI Must Enter Origination Agreement with Third-Party Sender*, and is an example of the "push down" effect for the chain of required agreements. As a best practice, it is recommended that these agreements are reviewed by your legal counsel.

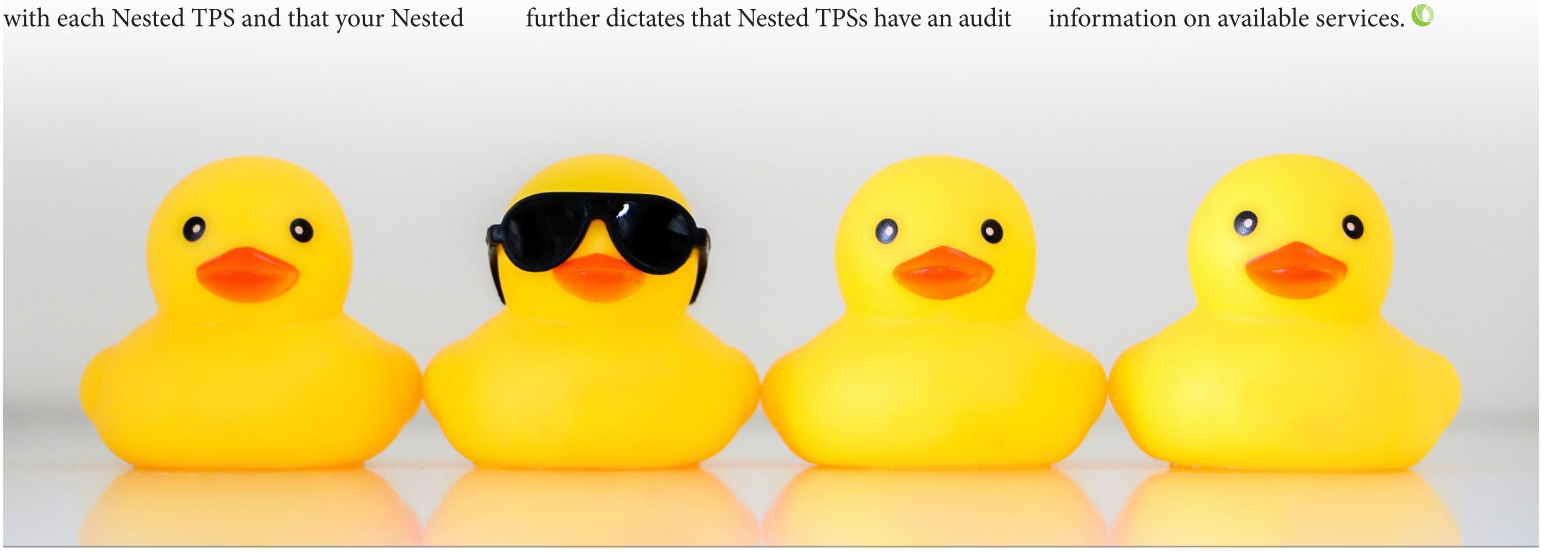
If you identify Nested TPSs, it is imperative that you make your ODFI aware immediately. Your ODFI needs to know how many Nested TPS relationships you are processing for and needs you to provide additional details regarding the Nested TPS's business information so updates can be made to Nacha's Risk Management Portal. In addition, any time you are made aware of staffing changes within your organization or your Nested Third-Party's organization, you will need to provide the updated contact information to your ODFI in a timely manner so your ODFI is able to update the registration information with Nacha within 45 days of the change, as prescribed in *Subsection 2.17.3.1, ODFIs with Third-Party Senders*.

The updated application of the *ACH Rules* further dictates that Nested TPSs have an audit conducted annually, both TPSs and Nested TPSs have a risk assessment conducted and due diligence be conducted by the TPSs on their Nested TPSs. Also, Nested TPSs must conduct due diligence on their clients.

Additionally, all new *ACH Rules* apply to TPSs and Nested TPSs. Annual ACH Rules Compliance Audits and periodic ACH Risk Assessments must be conducted by TPSs. TPSs also must ensure their Nested TPSs are aware of their audit and risk assessment obligations, as stated in *Supplement #3-2021*.

The ACH origination agreement between the TPS and the Nested TPS needs to address these obligations to protect both parties. As a TPS, you must ensure that your Nested TPS was able to attest to these items prior to transmitting any Entries. These updates largely impact TPSs and Nested TPSs but how these updates are handled on an ongoing basis by TPSs, in conjunction with their ODFI, will reflect in their successful transition for compliance.

If you have any questions, reach out to your financial institution. You can also visit EPCOR's Third-Party Sender User webpage www.epcor.org/tpsuser for free resources and information on available services.



Top 10 Fraud Trends in 2023

The following article originally appeared on Fraud.com.

Fraudsters will always seek new ways to exploit people's private information.

Cybercrime and fraud prevention is an ever-changing and evolving field based on varied tactics used by fraudsters. While fraudsters will always seek to conduct new fraud forms, you can be better prepared to mitigate their risks.

One place to start is being aware of the most frequent fraud attacks today. Here are the top 10 biggest fraud trends you need to know for 2023.

1. Automation

Automation makes it easier for criminals to exploit users' accounts while remaining undetected themselves, increasing the risk of fraud. With automation, fraudsters use software or bots to accomplish tasks that otherwise require human intervention, thus covering more ground. For example, credential stuffing is the act of testing stolen or leaked credentials on websites and services at scale to see if they work on any accounts.

2. Account Takeover

Account takeover (ATO) is a type of identity (ID) theft that occurs when a fraudster gains access to an individual's or company's computer accounts, email accounts and other personal information. In a typical ATO attack, hackers use phishing and malware methods to acquire legitimate user credentials or buy them from the dark web; they then use stolen credentials for account takeover.

Automated takeover attacks are carried out using stolen credentials, and organizations are particularly vulnerable to these attacks. A takeover can lead to a variety of crimes and direct financial losses, including:

- Bank account takeovers (current accounts, credit cards)
- Money laundering
- Stealing loyalty or rewards points
- Reselling subscription information

3. Adoption of New Digital Payments and Methods

Digital payment platforms and cryptocurrencies disrupt traditional payments, allowing consumers and businesses to make payments more quickly and efficiently. Technologies that enable new ways to pay are also open to new avenues of attack from fraudsters, as they use stolen credentials to carry out fraud and ID theft. Cryptocurrencies, while not quite mainstream in their use yet, are growing in popularity, and the anonymity provided by these currencies makes it easy for criminals to carry out illicit activities.

4. Ongoing Challenge of Balancing Fraud & Client Friction

Online businesses must balance risk and opportunity when mitigating fraud. In the case of online shopping, the amount of "friction" clients experience during the checkout process correlates with their conversion success.

The balance between friction and fraud becomes even more challenging across multiple channels, such as web, mobile and point of sale. Merchants and issuers seek alternative authentication solutions (such as passive behavioral biometrics and password-less authentication via biometrics with liveness detection) to attain this balance to improve customer experience and reduce risk.

5. Rise of Synthetic Identities

According to the McKinsey Institute, synthetic ID fraud is the fastest-growing type of financial crime in the United States and is also on the rise around the globe. Indeed, synthetic ID fraud comprises 85% of all fraud right now.

With this type of fraud, fraudsters create new identities by piecing together elements of a person's personal information and combining them with false identifiers. Essentially, they take bits of legitimate data, add fictitious information and create a new identity. Organizations are struggling to prevent synthetic ID fraud; after all, the whole point of synthetic ID fraud is to create a synthetic victim that does not exist in real life.

6. Escalating Cost of Fraud

The total cost of fraud is becoming a genuine concern, from fraud losses, prevention tools and headcount costs to the

see TRENDS on page 5

TRENDS continued from page 4

client lifetime value impact. It's estimated that fraud loss is $5.4 trillion globally; according to the University of Portsmouth, fraud accounts for approximately $185 billion in losses in the U.K. and a 9.9% increase in the cost of fraud for U.S. financial services firms.

Why the increase? As more and more people have turned to online and mobile channels to shop, fraudsters again have followed, thus the increase in fraud losses and associated costs with fighting fraud.

7. Growing Need for Multi-Layered Fraud Assessment

The digitization of e-commerce and banking is a well-established trend that shows no sign of abating; in parallel, fraud across these digital channels has remained a constant and relentless issue.

On the other hand, fraud prevention leaders are generally trying to defeat fraudsters with limited and siloed fraud management capabilities.

To achieve the best fraud prevention results, fraud prevention leaders must orchestrate all relevant data points, risk signals and client data to form a centralized and balanced response that reduces risk, client friction and associated prevention costs.

8. Targeted Attacks

Another growing threat is targeted attacks, which occur when cybercriminals compromise a target entity's entire infrastructure, including its network and computer systems. They can conduct such attacks anonymously and over a long period, gaining access to critical financial data and causing significant losses for institutions and constituents.

Targeted attacks occur in phases, thus are less likely of being discovered.

Although targeted attacks typically happen at the entity level and don't target specific consumers, these attacks put client information at risk and can harm an organization's reputation.

9. Heightened Need for Real-Time Risk Assessment

As online and mobile app usage increases, there's a growing need for comprehensive fraud detection, identity verification and authentication solutions to unite. Such solutions call for real-time risk assessment that leverages the latest AI, machine learning and fraud orchestration tools to manage the client's risk collectively and trust, utilizing all associated risk signals to drive fair and balanced client satisfaction.

10. Account Security

To protect against fraudsters, organizations need to take a layered approach to account security. The culprit behind system attacks is often single-factor authentication methods that result in unauthorized access to accounts, enabling client account fraud, identity theft, ransomware attacks and other fraudulent activity, notes the Federal Financial Institutions Examination Council.

With multi-factor authentication, institutions use more than one distinct authentication factor to successfully authenticate clients, such as behavioral biometrics, device ID and biometric authentication.

Get Ahead of Fraud Trends

Throughout the client journey, it's essential to incorporate safety measures that protect organizations and their users, prevent disruptions in the buying process and keep fraudsters at bay. If you have any questions, reach out to your financial institution.

Source: Fraud.com

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
2345 Grand Blvd., Ste. 1700, Kansas City, MO 64108
800.500.0100 | 816.474.5630 | fax: 816.471.7665