Early Warning®

Nacha's New Operating Rules Changes

A PRACTICAL GUIDE FOR FINANCIAL INSTITUTIONS

ACH is experiencing a heyday.

Businesses and consumers alike are embracing the payment channel as a quick and easy way to send and receive money.

Indeed, the ACH Network processed:

33.5 billion

in payments in 2024, totaling over

$86 trillion[1]

But the explosive growth has not gone unnoticed by fraudsters, who've been successfully executing schemes that take advantage of ACH vulnerabilities. Examples include:

- Exploiting faster payment systems to move funds quickly before the fraud is detected
- Employing social engineering tactics to manipulate valid account holders into making fraudulent transactions
- Using mule accounts to obscure the origin or destination of funds

And this ACH fraud can be costly for banks as they often end up compensating consumer accounts for fraudulent ACH transactions.

In response to the growing risks, Nacha has once again updated its Operating Rules. In general, the updates aim to strengthen fraud detection, prevention and recovery across the ACH Network. More specifically, many of the changes focus on mitigating risks associated with credit-push fraud—and add new responsibilities for Receiving Depository Financial Institutions (RDFIs).

Read this guide to **understand the key changes**, **what they mean for financial institutions** (FIs) and **tips for staying compliant**.

Key things banks and credit unions should know about the Nacha's new rules

Nacha's Operating Rules are more than compliance mandates. They can also serve as a roadmap of sorts, to help FIs better understand and protect against growing fraud threats.

This latest set of updates, for example, can help FIs better protect against credit-push fraud. In these schemes, criminals use social engineering techniques and manipulation to trick valid account holders into authorizing fraudulent transactions. While many banks have controls in place to protect against fraud involving unauthorized ACH transactions, fraud that involves authorized transactions can be more difficult to detect and prevent.

According to a 2024 Datos Insights survey,

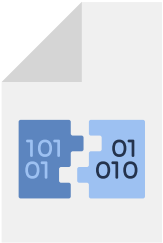
37% of FIs

report being concerned about their ability to adequately detect ACH fraud attacks.[2]

Nacha's latest rules changes focus on helping FIs detect ACH fraud earlier and recover funds more effectively. Crucial updates include:

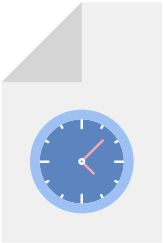
EXPANDED FRAUD MONITORING FOR RDFIS

RDFIs must implement risk-based processes to scrutinize incoming credit transactions for signs of fraud. This reflects the growing threat of credit-push fraud and the need for RDFIs to play a more proactive role in fraud prevention.



GREATER FLEXIBILITY WITH RETURN REASON CODE R17

RDFIs can now use this code to return any transaction they deem "questionable" or potentially fraudulent, without being constrained by previously strict definitions.



EXEMPTIONS FOR FUNDS AVAILABILITY

RDFIs may delay funds availability (within Regulation CC limits) for credits they believe are unauthorized or initiated under false pretenses. This gives receiving banks more time to review suspicious transactions before making funds accessible.

CLARIFIED USE OF ODFI REQUEST FOR RETURN

Originating Depository Financial Institutions (ODFIs) can request returns from RDFIs for a broader range of reasons. While RDFIs can still decide whether or not to return the funds, they must respond to ODFI requests within 10 days.

Tips for building a resilient fraud prevention strategy

These key strategies can help your institution improve compliance and mitigate fraud risks:

Implement risk-based monitoring: Develop processes to assess the risk of both incoming and outgoing ACH transactions. Focus on identifying anomalies, such as unusual transaction patterns, unexpected recipient details or suspicious activity.

Monitor dynamically: Regularly update your fraud models to account for emerging threats. Monitoring systems that analyze account data in real time are crucial to staying ahead of fraudsters.

Use predictive analytics: Prioritize high-risk transactions using predictive intelligence tools that determine the likelihood of potential fraud.

Collaborate with stakeholders: Effective fraud prevention requires collaboration and shared responsibility across the ACH Network. Strengthen relationships between your FI, originators and third-party providers to align on expectations and ensure clear communication.

Invest in training and education: Equip your fraud teams with the knowledge they need to keep up with compliance rules and stay informed about emerging threats. Training is not a one and done venture. It should be an ongoing effort, incorporating real-world examples of the latest fraud trends.

Plan for rapid incident response: Document procedures for handling flagged ACH transactions and confirmed fraud incidents. Prepare your teams to act quickly, using tools like Return Reason Code R17 and Nacha's Risk Management Portal to recover funds efficiently.

Common red flags

To combat increasingly sophisticated ACH fraud tactics, FIs need tools that can detect potential fraud before the transaction is posted against the account.

Common red flags include:

Transaction anomalies: Unusually high-value or high-volume credits to new or inactive accounts.

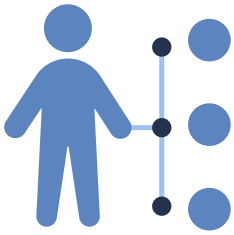
Account ownership mismatches: Discrepancies between the recipient's name in the payment entry and the actual account holder's name at the receiving institution.

Velocity issues: Repeated transactions from the same account within a short timeframe.

Proactive steps that can ease compliance as Nacha rules evolve

1

Conduct a gap analysis: Identify vulnerabilities in your current fraud monitoring procedures and determine where updates or improvements are needed to comply with new Nacha rules.



2

Get leadership buy-in: Engage leaders at your institution to prioritize compliance efforts. Allocate necessary resources for things like system upgrades, staff training and process improvements.

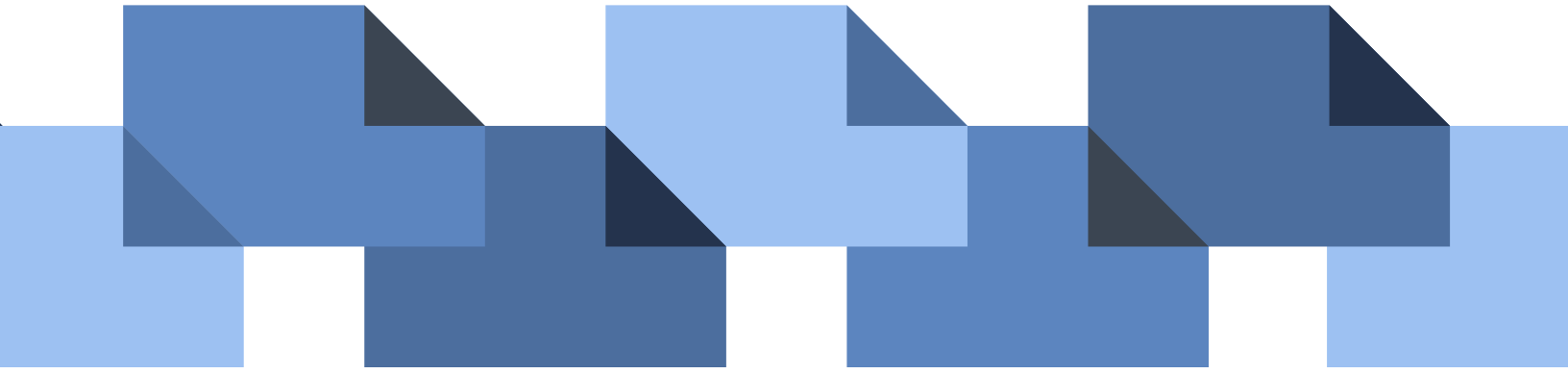
3

Ensure your systems can support effective monitoring: Implement or upgrade systems to enable ongoing, risk-based monitoring. Ensure your processes can adapt to emerging ACH fraud tactics and evolving compliance requirements.

How FIs benefit from Nacha's Operating Rules

Complying with Nacha's evolving Operating Rules is not always easy. But FIs that put the right systems in place can simplify compliance while improving their fraud prevention strategies. In so doing, they can:

- **Protect against fraud losses:** ACH transactions are a growing target for sophisticated schemes like credit-push fraud. Nacha's updated rules ensure FIs take the steps to detect and prevent fraud more effectively.
- **Maintain a strong reputation:** Customers rely on their FIs to keep their money and personal information secure. A single fraud incident can erode that trust, potentially leading to customer attrition. FIs that keep up with Nacha's rules changes will be better positioned to fight back against new ACH fraud trends, safeguard customers and avoid reputational damage.
- **Improve operational efficiency:** Successful fraud incidents require significant time and resources to resolve, from investigating transactions to recovering funds and assisting affected customers. Effective fraud prevention and adherence to Nacha's rules reduce the frequency of these incidents, freeing up resources and allowing teams to focus on core operations and customer service.



How Early Warning® can help

As a Preferred Nacha Partner, Early Warning® offers real-time tools like Payment Chek® and Verify Account that can help minimize fraud risk and support compliance.

LEARN MORE

To learn more about how Early Warning can help your bank or credit union, visit our website.

Sources

1 ACH Network Volume and Value Statistics, Nacha, 2025
2 Trends in Fraud for 2024 and Beyond, Datos Insights, February 2024

ABOUT EARLY WARNING

Early Warning Services, LLC, is a fintech company owned by seven of the country's largest banks. For more than thr ee decades, our identity, risk and payment solutions have been empowering financial institutions to make confident decisions, enable payments and mitigate fraud. Today, Early Warning is best known as the owner and operator of the Zelle Network®, a financial services network focused on transforming payment experiences.

With a partner like Early Warning, FIs are empowered with an accurate, comprehensive solution that:

- Provides breadth and depth of deposit data, enabling a holistic view of a consumer's banking behavior
- Leverages real-time, predictive analytics that enable better-informed decisions
- Ensures faster decisions and reduced friction which translates to a better customer experience.