

Q3 2025

Payments Newsletter

For Treasury Customers

New Nacha ACH Rules: Standardized Company Entry Descriptions for PAYROLL and PURCHASE

The ACH Network is making strides to improve risk management, reduce fraud, and enhance the overall quality of ACH transactions. As part of a broader Risk Management Rules package, Nacha has introduced two new standardized Company Entry Descriptions: **PAYROLL** and **PURCHASE**. These changes, which take effect on March 20, 2026, aim to help financial institutions and other ACH participants better identify transaction purposes, mitigate fraud risks, and improve the recovery of funds in fraud scenarios.



What Are the New Rules?

PAYROLL – Entry Description for Payroll Payments

The new rule establishes a standardized PAYROLL entry description for PPD Credits involving wages, salaries, and similar compensation. Originators must include the description PAYROLL in the Company Entry Description field.

PURCHASE – Entry Description for E-Commerce Transactions

For e-commerce debit transactions authorized by consumers, the Company Entry Description field must contain the standardized term PURCHASE. These transactions include online purchases of goods, as well as recurring purchases initially authorized online.

Next Steps

Businesses that originate ACH entries should begin evaluating their transactions to ensure compliance with the new rules. While the effective date is March 20, 2026, early adoption is encouraged to align processes and reduce risks proactively. If you have questions about these new rules or need assistance implementing changes to your ACH files, contact us today. Staying ahead of these regulatory changes will ensure smooth operations and help safeguard your business against fraud risks.

ISO 20022 Implementation: Working Out the Kinks and Ensuring a Smooth Transition

The global adoption of ISO 20022 in July 2025 represents a significant advancement in financial messaging standards. Designed to improve the quality and richness of payment data, ISO 20022 enables faster and more accurate transactions, streamlines cross-border payments, and enhances compliance capabilities. While the transition has been largely successful across the industry, financial institutions — including ours — are committed to monitoring and addressing any minor challenges that may arise during the post-implementation phase.

How are we addressing post-implementation challenges? We are monitoring wire transfers to ensure ISO 20022 messages are processed accurately and efficiently. We are also working closely with technology vendors and payment network partners to identify and resolve any lingering issues. If you experience any disruptions or notice inconsistencies, please report them to us so we can escalate these concerns promptly.

While the implementation of ISO 20022 is a significant step forward, it's also an ongoing journey of improvement. As adoption deepens across the industry, we are committed to working with our partners and customers to ensure the system operates at its full potential.

Our goal is to make financial messaging smarter, faster, and safer for your business. If you have any questions or concerns about ISO 20022 or need assistance with your transactions, don't hesitate to contact us. Together, we can continue to embrace the benefits of this transformative standard.

The Rise of AI and Deepfakes: What it means for your Business

AI is transforming the way businesses operate. From streamlining processes to predicting market trends, AI offers significant advantages. However, with these advancements come new risks, and one of the most pressing concerns for businesses today is the rise of AI-powered threats like deepfakes. Deepfakes are realistic but artificially manipulated audio, video, or image content created using AI. While this technology can have legitimate uses in entertainment and education, it is increasingly being exploited for fraudulent purposes. For example, cybercriminals are using deepfake audio to impersonate executives, instructing employees to authorize fraudulent payments or transfer funds to unverified accounts — a tactic known as “audio impersonation fraud.”

As deepfake technology becomes more sophisticated, it's critical for businesses to stay one

step ahead. Below are tips to protect your operations and reduce the risk of fraud:

Strengthen Verification Processes: Rely on secure, documented processes and confirm changes to payment instructions via a trusted telephone number. **Never** contact an unknown number.

Educate Employees: Train your team to recognize potential deepfake schemes and to verify requests for payments or sensitive data independently.

Collaborate with Us: Stay connected with our treasury services team. We offer fraud prevention tools and best practices tailored to help your business mitigate emerging risks.

While AI and deepfake technology introduce risks, they also offer opportunities to improve fraud detection and operational efficiency. Together, we can ensure your business remains resilient in the face of evolving risks.



If you have questions about the newsletter or would like more information on fraud mitigation tools and treasury service offerings, please contact us at support@craft.bank or 678-736-5060.