

Nacha New Rule Changes - 2026

Session 1 | September 2025

Webinar Series
2025

Disclaimer

Compliance with Nacha Rule changes is the responsibility of the client and not JPMC, and clients should consult with their Legal and Compliance representatives. Clients remain subject to and solely responsible for compliance with their obligations under applicable Nacha and other payment network rules.

Agenda

	Page
1 Overview	4
2 2026 Rule Changes Definition	9
3 Transaction Analysis	15
4 Proposed Approach	17
5 Appendix	21

What Significance Do the Rule Changes Carry?

- On March 15, 2024, Nacha's Voting Membership approved 15 ballots to reduce fraud attempts and improve the recovery of funds after fraud has occurred
- Six Minor Topic Rule Changes were implemented on June 21, 2024, and four Risk Management-related Rule Changes were implemented on October 1, 2024
- The remaining five Rule Changes are applicable 2025 & 2026 and primarily focus on:

Detect Fraud Attempts



- ✓ Strengthening the ability of the ACH Network to detect fraud attempts

Reduce Fraud Attempts






- ✓ Take necessary steps to reduce the incidents of successful fraud attempts

Improve Recovery of Funds



- ✓ Improve Recovery of Funds when fraud has actually occurred

Overview: June 2024 through April 2025

		
1st Compliance Date	2nd Compliance Date	3rd Compliance Date
Effective : June 21 st , 2024	Effective : October 1 st , 2024	Effective : April 1 st , 2025
<div><div>1. General Rule/Definition of WEB Entries</div><div>2. Definition of Originator</div><div>3. Originator Action on Notification of Change</div><div>4. Data Security Requirements</div><div>5. Use of Prenotification Entries</div><div>6. Clarification of Terminology – “Subsequent Entries”</div></div>	<div><div>1. Codify Use of Return Reason Code R17</div><div>2. Additional Funds Availability Exceptions</div><div>3. Timing of Written Statement of Unauthorized Debit (WSUD)</div><div>4. RDFI Must Promptly Return Unauthorized Debit</div></div>	<div><div>1. Expanded Use of ODFI Request for Return/R06</div></div>

Overview: 2026

4th Compliance Date

RULE 01

RULE 02

RULE 06

RULE 07

Effective :
For Rule #01 & #02
March 20, 2026, for all ODFIs and non-Consumer Originators, TPSPs, and TPSs with annual ACH origination volume of 6 million or greater in 2023
June 22, 2026, for all non-Consumer Originators, TPSPs, and TPSs that did not fall under the requirement threshold (2023 is the baseline year for the volume thresholds)

Effective :
For Rule #06 & #07
March 20, 2026

1. Fraud Monitoring by Originators, TPSPs and ODFIs

2. RDFI ACH Credit Monitoring

3. Standard Company Entry Description - PAYROLL

4. Standard Company Entry Description - PURCHASE

Why Should You Know About Nacha Rule Changes 2026

Compliance



- **Compliance Maintenance:** Stay updated with 2026 Nacha rules to avoid penalties and promote secure ACH transactions.

Operations



- **Operational Improvements:** Streamline processes to align with updated standards, reducing errors and enhancing transaction speed.

Strategy



- **Strategic Positioning:** Implement best practices to strengthen reputation and build trust with partners and customers.

Finance



- **Financial Advantages:** Help avoid financial losses from non-compliance and optimize processes for cost savings.

Agenda

		Page
1	Overview	4
2	2026 Rule Changes Definition	9
3	Transaction Analysis	15
4	Proposed Approach	17
5	Appendix	21

Overview of 2026 Nacha Rule Changes



Fraud Monitoring by Originators, TPSPs and ODFIs

- **Implementation of Risk-Based Processes:** Originators, Third Party Service Providers (TPSPs), and ODFIs must establish risk-based processes to identify unauthorized entries
- **Annual Review:** Processes should be reviewed annually to address evolving risks



RDFI ACH Credit Monitoring

- **Establishment of Monitoring Procedures:** RDFIs must implement procedures to identify unauthorized credit entries
- **Annual Review:** Procedures require annual updates to remain effective



Standard Company Entry Descriptions

- **Payroll and E-Commerce Purchase Descriptions:** Establishes standard descriptions for payroll ("PAYROLL") and e-commerce ("PURCHASE") entries for clarity and consistency

Standard Company Entry Description – **PAYROLL**

RULE 06

EFFECTIVE DATE	NACHA RULES & ASSOCIATED GUIDANCE
Effective March 20, 2026	<p>Language has been added to disclaim any representation or warranty about actual employment status:</p> <ul style="list-style-type: none">■ “The use of the term “PAYROLL” in this field is descriptive and by use of the word, neither the Originator, nor the ODFI (or any Third-Party Service Provider acting on behalf of an Originator or ODFI), makes any representation or warranty to the RDFI or the Receiver regarding the Receiver’s employment status. <p>Language also has been added to disclaim obligation on the part of ODFIs to “police” Originators’ correct use:</p> <ul style="list-style-type: none">■ “The ODFI has no obligation to verify the presence or accuracy of the word “PAYROLL” as a description of purpose or employment status.”■ RDFIs that monitor inbound ACH credits will have better information regarding new or multiple payroll payments to an account. <p>For more details, please refer to the Nacha website. The usage of the term "PAYROLL" is explained in the FAQ section of the Nacha website.</p>

Standard Company Entry Description – **PURCHASE**

RULE 07

EFFECTIVE DATE	AMENDMENT AS PER NACHA
Effective March 20, 2026	<p>Language for the definition of e-commerce purchases now considers:</p> <ul style="list-style-type: none">■ “For this purpose, an e-commerce purchase is a debit Entry authorized by a consumer Receiver for the online purchase of goods, including recurring purchases first authorized online. An e-commerce purchase uses the WEB debit SEC Code, except as permitted by the rule on Standing Authorization to use the PPD or TEL debit SEC Code.” <p>Language has also been added to disclaim obligation on the part of ODFIs to “police” Originators’ correct use</p> <ul style="list-style-type: none">■ “The ODFI has no obligation to verify the presence or accuracy of the word “PURCHASE” as a description of purpose.”■ “For this purpose, an e-commerce purchase is a debit Entry authorized by a consumer Receiver for the online purchase of goods, including recurring purchases first authorized online. An e-commerce purchase uses the WEB debit SEC Code, except as permitted by the rule on Standing Authorization to use the PPD or TEL debit SEC Code.” <p>For more details, please refer to the Nacha website. The usage of the term "PURCHASE" is explained in the FAQ section of the Nacha website.</p>

Fraud Monitoring by Originators, TPSPs and ODFIs

RULE 01

EFFECTIVE DATE	NACHA RULE AMENDMENTS
<p>Phase 1: March 20, 2026 For all ODFIs and non-Consumer Originators, TPSPs, and TPSs with annual ACH origination volume of 6 million or greater in 2023.</p> <p>Phase 2: June 22, 2026 For all non-Consumer Originators, TPSPs, and TPSs that did not fall under the requirement threshold for Phase 1. <i>(2023 is the baseline year for the volume thresholds)</i></p>	<p>Each Non-Consumer Originator, ODFI, and Third-Party Service Provider (TPSP) or Third-Party Sender (TPS) acting on behalf of an Originator, Third-Party Sender or ODFI, must:</p> <ul style="list-style-type: none">■ Establish and implement risk-based processes and procedures relevant to the role it plays in the authorization or Transmission of Entries that are reasonably intended to identify Entries that are suspected of being unauthorized or authorized under False Pretenses; and■ At least annually review such processes and procedures and make appropriate updates to address evolving risks.

RDFI ACH Credit Monitoring

RULE 02

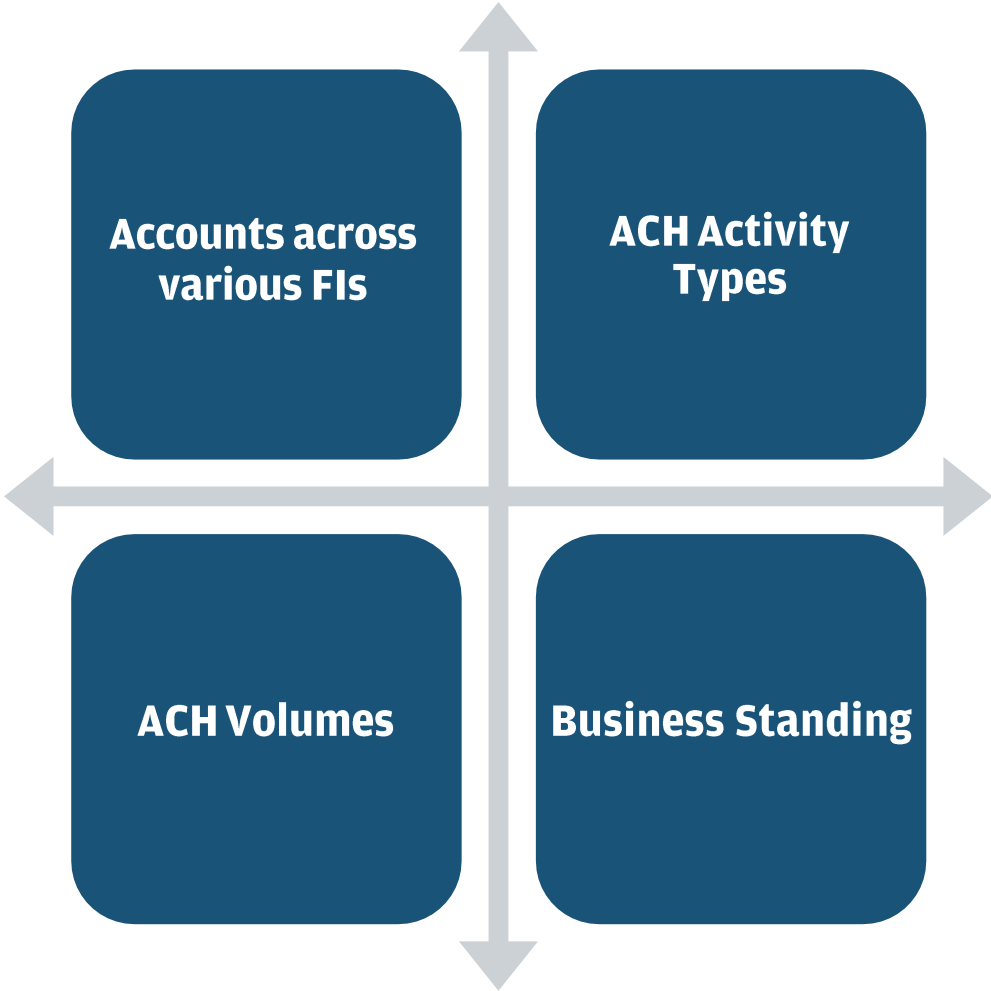
EFFECTIVE DATE	NACHA RULE AMENDMENTS
<p>Phase 1: March 20, 2026 For RDFIs with annual ACH receipt volume of 10 million or greater in 2023</p> <p>Phase 2: June 22, 2026 For all RDFIs that did not meet the threshold requirement for Phase 1. (2023 is the baseline year for the volume thresholds)</p>	<ul style="list-style-type: none">■ “Each RDFI must: Establish and implement risk-based processes and procedures relevant to the role the RDFI plays in connection with the receipt of credit Entries that are reasonably intended to identify credit Entries that are suspected of being unauthorized or authorized under False Pretenses, including processes and procedures for responding when credit Entries are identified as potentially unauthorized or authorized under False Pretenses; and■ At least annually review such processes and procedures and make appropriate updates to address evolving risks.■ These processes and procedures do not require the screening of every ACH Entry individually, and do not need be performed prior to the processing of Entries.

Agenda

		Page
1	Overview	4
2	2026 Rule Changes Definition	9
3	Transaction Analysis	15
4	Proposed Approach	17
5	Appendix	21

What Factors To Consider To Define Rule Applicability?

Prior to strategizing any action on any of the rule changes, it is imperative to review the following:



Examples

- RULE 01**
Use-Case 1
If you are a non-consumer originator and have originated ACH transactions below 6 million in volume as of 2023, then:
 - The Rule Change #01 will be applicable and
 - You will need to comply with the Rule change by 22nd June 2026
 - For those with ACH Origination transaction volume (2023) is above 6 million, then you'd need to comply by 20th March 2026
- RULE 06**
Use Case 2
If you are originating any number of PPD Credit, then:
 - Identify the reason of such originations. If it is for payment of wages, payroll then:
 - You will need to comply with Rule Change #06
 - You will need to add the word "PAYROLL" in the description of the transaction
 - The word "PAYROLL" should be left-aligned and the remaining spaces can be used for any other character
- RULE 07**
Use Case 3
If you initiate ACH transactions that are debit authorization for e-commerce purchases by a consumer receiver and the transactions use WEB debits or PPD or TEL Debits (in exception scenarios), then:
 - You will need to comply with Rule Change #07
 - You will need to add the word "PURCHASE" in the description of the transaction
 - The word "PURCHASE" should be left-aligned and the remaining spaces can be used for any other character
 - This is only for cases where goods are purchased and not for paying bills, etc.

Agenda

		Page
1	Overview	4
2	2026 Rule Changes Definition	9
3	Transaction Analysis	15
4	Proposed Approach	17
5	Appendix	21

Points to Consider in the Evolving Payments Landscape

1 Conduct a Compliance Review

- **Document the current process to identify unauthorized entries and entries authorized under false pretenses**
- **Review current processes:** Assess all existing ACH processes, including third-party relationships, to identify gaps in compliance with the new rules
- **Identify areas for improvement:** Determine and address which areas may need changes or enhancements to meet the new requirements

2 Enhance Fraud Monitoring and Prevention

- **Implement risk-based monitoring:** Implement risk-based processes to identify and mitigate fraudulent transactions
- **Leverage fraud detection tools:** Invest in technology and tools that can detect anomalies in transaction data and evolving threats

3 Educate and Train Employees

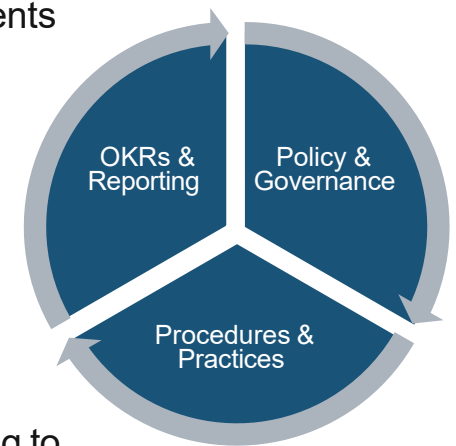
- **Conduct Training :** Provide training for employees on the new NACHA rules and compliance requirements
- **Compliance Culture:** Foster a culture of compliance within the organization to ensure everyone understands the importance of adhering to the rules

4 Implement Continuous Monitoring and Review

- **Review Compliance Processes:** Establish a schedule for at least annual reviews of compliance efforts to ensure ongoing adherence to the rules.
- **Adjust Strategies as Needed:** Be prepared to adjust strategies based on changes in the regulatory environment or business operations.

5 Seek Legal Advice

- **Legal Consultations:** Consult with your Legal or Compliance experts to gain insights and advice on Nacha Rules and navigating the changes.



ACH Monitoring Best Practices Across Payments Lifecycle

Identity & Onboarding

Key Risk Areas: Fraudulent entities, synthetic identities, account takeover, and unauthorized account usage.

What to Consider*

1. Multi-Layered Identity Verification

Use **real-time API integrations** to verify:

- ✓ Name, address, phone number, and email validity.
- ✓ SSN/TIN verification against government databases.
- ✓ Sanctions and watchlist screening.
- ✓ Device intelligence and geolocation checks.
- ✓ Real-time MFA authentication

2. Behavioral & Predictive Analytics

- ✓ Use machine learning to **detect patterns of suspicious behavior & synthetic identities** based on inconsistencies in identity data.

3. Account Ownership & Payment Information Matching

- ✓ Deploy bank account verification processes to confirm that account details match the entity's legal registration.
- ✓ Cross-check payment information with known high-risk accounts or flagged entities.

Change Management

Key Risk Areas: Account takeovers, impersonation fraud, unauthorized changes to payment details.

What to Consider*

1. Multi-Factor Authentication (MFA) for Account Changes

- ✓ Require step-up authentication (e.g., OTPs, biometric verification, knowledge questions)
- ✓ Red-flag requests that involve bank account changes, payment rerouting, PII data, email changes or unusual disbursements.
- ✓ Use a secondary communication channel (e.g., SMS, phone call, email) to confirm high-risk change requests.

2. Automated Monitoring & Alerts for Unusual Activity

Deploy real-time monitoring to track:

- ✓ Sudden changes in volume of account inquiries.
- ✓ Disbursements to new or high-risk accounts.
- ✓ Large-value payments inconsistent with past behavior.
- ✓ Sanctions screening changes

Payments & Disbursements

Key Risk Areas: ACH credit fraud, unauthorized disbursements, billing fraud, vendor impersonation scams.

What to Consider*

1. Real-Time Account Status & Risk Screening

Integrate bank account validation APIs to check if an account is:

- ✓ Open, active, and in good standing.
- ✓ Associated with past fraudulent activity.

2. Account Ownership Verification for Outbound Payments

- ✓ Require business verification matching for ACH disbursements (e.g., does the business name and TIN match the account owner?).
- ✓ Use risk-scoring for new payees—especially for large-value ACH credit transactions.

3. Transaction Limits & Velocity Monitoring

- ✓ Deploy automatic monitoring to detect rapid-fire disbursements or unusual payment patterns.

JPMC to Help ACH Originators, Third-Party Service Providers and Third-Party Senders



Account Confidence Score*

What:

- Account Confidence Score is an AI-based machine learning score
- It indicates the probability that a beneficiary account is anomalous or fraudulent

When:

- This score can be used at the point of onboarding, registration, in advance of the payment instruction

How:

- The Account Confidence Score is a derivation of the in-house fraud screening model, translated into a numerical indicator. This may allow you to evaluate the likelihood of fraud on a beneficiary's account



Identity & Account Validation*

What:

- AVS (Account Validation Service) provides the ability to validate the status and ownership of an account
- EVS (Entity Verification Service) provides verification of individual or business data from trusted data sources and third-party regulatory vendors

When:

- This service can be used at the point of onboarding, registration, or payment instruction

How:

- AVS validates the account status and ownership prior to the payment lifecycle
- EVS verifies the beneficiary identity using data from trusted sources and vendors

Your feedback is important to us!

J.P.Morgan

<https://jpmc.surveymonkey.com/r/RGBNW6V>

Feedback Survey - 2026 Nacha Rule Changes

Scan the QR to take the survey



* 1. How satisfied are you with the overall training session?

- ☐ Highly satisfied ☐ Moderately satisfied ☐ Somewhat satisfied ☐ Not satisfied

* 2. What is your company name?

* 3. How clear and understandable was the training content delivered during the session?

- ☐ Very clear ☐ Mostly clear ☐ Somewhat clear ☐ Not clear

* 4. How relevant and applicable was the training content to your current role/function?

- ☐ Highly relevant ☐ Moderately relevant ☐ Somewhat relevant ☐ Not relevant

Done

Appendix

False Pretense

Rules #1 and #2 include references to a newly defined term, False Pretenses.

New language

“False Pretenses

the inducement of a payment by a Person misrepresenting

- (a) that Person’s identity,
- (b) that Person’s association with or authority to act on behalf of another Person, or
- (c) the ownership of an account to be credited.”

This definition covers common fraud scenarios such as:

- (a) Business Email Compromise (BEC),
- (b) vendor impersonation,
- (c) payroll impersonation, and other payee impersonations

The definition complements language on “unauthorized credits” (account takeover scenario). It does not cover scams involving fake, non-existent or poor-quality goods or services.

As a new definition, False Pretenses also would be referred to in Rules language for Rules #3 (Codifying Expanded Use of R17); and #5 (Additional Exceptions to Funds Availability).

Rule #01

Ballot #1-2024: Fraud Monitoring by Originators, Third-Party Service Providers, Third-Party Senders, and ODFIs

(proposed effective date – Phase 1: March 20, 2026; Phase 2: June 19, 2026)¹

ARTICLE TWO – RIGHTS AND RESPONSIBILITIES OF ODFIS, THEIR ORIGINATORS, AND THIRD-PARTY SENDERS

SECTION 2.2 Prerequisites to Origination

Subsection 2.2.4 Identification of Unauthorized Entries or Entries Authorized Under False Pretenses (New Section)

Each Non-Consumer Originator; each Third-Party Sender; each ODFI; and each Third-Party Service Provider that performs any functions of ACH processing on behalf of an Originator, Third-Party Sender, or ODFI must:

- (a) establish and implement risk-based processes and procedures relevant to the role it plays in the authorization or Transmission of Entries that are reasonably intended to identify Entries that are suspected of being unauthorized or authorized under False Pretenses; and
- (b) at least annually review these processes and procedures and make appropriate updates to address evolving risks.

These processes and procedures do not require the screening of every ACH Entry individually and do not need to be performed prior to the processing of Entries. An ODFI's processes and procedures may take into account the processes and procedures implemented by other participants in the origination of Entries.

This Subsection 2.2.4 does not modify or create, and shall not be interpreted to modify or create, in any way, rights or obligations of any Person under Article 4A. An agreement to comply with the Rules or this Subsection 2.2.4 does not, and shall not be interpreted to, constitute agreement to a "security procedure" for purposes of Article 4A unless

otherwise specifically designated as such in an agreement with the ODFI. The obligation to comply with this Subsection 2.2.4 is enforceable solely by the National Association in accordance with Appendix Nine (Rules Enforcement) of these Rules and does not create or imply any other duty to any other Person.

ARTICLE EIGHT – DEFINITIONS OF TERMS USED IN THESE RULES

Section 8.42 "False Pretenses" (new section)²

the inducement of a payment by a Person misrepresenting (a) that Person's identity, (b) that Person's association with or authority to act on behalf of another Person, or (c) the ownership of an account to be credited.

Rule #02

Ballot #2-2024: ACH Credit Monitoring by RDFIs

(proposed effective dates – Phase 1: March 20, 2026; Phase 2: June 19, 2026)³

ARTICLE THREE – RIGHTS AND RESPONSIBILITIES OF RDFIS AND THEIR RECEIVERS

SECTION 3.1 General Rights and Responsibilities of RDFIs

SUBSECTION 3.1.10 Identification of Unauthorized Credit Entries or Credit Entries Authorized Under False Pretenses (New Subsection)

Each RDFI must:

- (a) establish and implement risk-based processes and procedures relevant to the role the RDFI plays in connection with the receipt of credit Entries that are reasonably intended to identify credit Entries that are suspected of being unauthorized or authorized under False Pretenses, including processes and procedures for responding when credit Entries are identified as potentially unauthorized or authorized under False Pretenses; and
- (b) at least annually review these processes and procedures and make appropriate updates to address evolving risks.

These processes and procedures do not require the screening of every ACH Entry individually and do not need to be performed prior to the processing of Entries.

This Subsection 3.1.10 does not modify or create, and shall not be interpreted to modify or create, in any way, rights or obligations of any Person under Article 4A. The obligation to comply with this Subsection 3.1.10 is enforceable solely by the National Association in accordance with Appendix Nine (Rules Enforcement) of these Rules and does not create or imply any other duty to any other Person.

ARTICLE EIGHT – DEFINITIONS OF TERMS USED IN THESE RULES

Section 8.42 "False Pretenses" (new section)

the inducement of a payment by a Person misrepresenting (a) that Person's identity, (b) that Person's association with or authority to act on behalf of another Person, or (c) the ownership of an account to be credited.

Rule #06

Ballot #6-2024: Company Entry Description – “PAYROLL”
(proposed effective date – March 20, 2026)⁴

APPENDIX THREE – ACH RECORD FORMAT SPECIFICATIONS

Part 3.2 Glossary of ACH Record Format Data Elements

SUBPART 3.2.2 Glossary of Data Elements

Company Entry Description: 10 Positions – Company/Batch Header Record – Mandatory (all batches)

The Originator establishes the value of this field to provide the Receiver with a description of the purpose of the Entry. For example, “Gas bill,” “Reg. Salary,” “ins. prem.,” “Soc. Sec.,” “DTC,” “Trade Pay,” “PURCHASE,” etc.

This field must contain the word “ACCTVERIFY” when the batch contains Micro-Entries.

This field must contain the word “NONSETTLED” when the batch contains Entries that could not settle.

This field must contain the word “RECLAIM” when the batch contains Reclamation Entries.

This field must contain the words “RETRY PYMT” when the batch contains Reinitiated Entries. For any Reinitiated Entry, the description “RETRY PYMT” must replace the original content of the Company Entry Description field transmitted in the original Entry, including content otherwise required by these Rules.

This field must contain the words “RETURN FEE” when the batch contains Return Fee Entries.

This field must contain the word “REVERSAL” when the batch contains Reversing Entries.

ADV: The Originator, i.e., the Originating ACH Operator, uses this field to describe to the institution receiving the ADV File the type of activity to which the accounting information relates.

CCD: This field must contain the word “HCCLAIMPMT” when the batch contains Health Care EFT Transactions.

ENR: This field must contain the word “AUTOENROLL” when the batch contains Automated Enrollment Entries.

PPD: This field must contain the word “PAYROLL” when the batch contains credits for the payment of wages, salaries, or similar types of compensation. The use of the term “PAYROLL” in this field is descriptive and by use of the word, neither the Originator, nor the ODFI (or any Third-Party Service Provider acting on behalf of an Originator or ODFI), makes any representation or warranty to the RDFI or the Receiver regarding the Receiver’s employment status. The ODFI has no obligation to verify the presence or accuracy of the word “PAYROLL” as a description of purpose or employment status.

Rule #07

Ballot #7-2024: Company Entry Description – “PURCHASE”
(proposed effective date – March 20, 2026)⁵

APPENDIX THREE – ACH RECORD FORMAT SPECIFICATIONS

Part 3.2 Glossary of ACH Record Format Data Elements

SUBPART 3.2.2 Glossary of Data Elements

Company Entry Description: 10 Positions – Company/Batch Header Record – Mandatory (all batches)

The Originator establishes the value of this field to provide the Receiver with a description of the purpose of the Entry. For example, “Gas bill,” “Reg. Salary,” “ins. prem.,” “Soc. Sec.,” “DTC,” “Trade Pay,” “PURCHASE,” etc.

This field must contain the word “ACCTVERIFY” when the batch contains Micro-Entries.

This field must contain the word “NONSETTLED” when the batch contains Entries that could not settle.

This field must contain the word “PURCHASE” when the batch contains e-commerce purchases. For this purpose, an e-commerce purchase is a debit Entry authorized by a consumer Receiver for the online purchase of goods, including recurring purchases first authorized online. An e-commerce purchase uses the WEB SEC Code, except as permitted by the rule on Standing Authorization to use the PPD or TEL SEC Code. The ODFI has no obligation to verify the presence or accuracy of the word “PURCHASE” as a description of purpose.

This field must contain the word “RECLAIM” when the batch contains Reclamation Entries.

This field must contain the words “RETRY PYMT” when the batch contains Reinitiated Entries. For any Reinitiated Entry, the description “RETRY PYMT” must replace the original content of the Company Entry Description field transmitted in the original Entry, including content otherwise required by these Rules.

Disclaimer

This material was prepared exclusively for the benefit and internal use of the J.P. Morgan client to whom it is directly addressed (including such client's subsidiaries, the "Company") in order to assist the Company in evaluating a possible transaction(s) and does not carry any right of disclosure to any other party. In preparing this material, we have relied upon and assumed, without independent verification, the accuracy and completeness of all information available from public sources or which was provided to us by or on behalf of the Company or which was otherwise reviewed by us. This material is for discussion purposes only and is incomplete without reference to the other briefings provided by J.P. Morgan. Neither this material nor any of its contents may be disclosed or used for any other purpose without the prior written consent of J.P. Morgan.

J.P. Morgan, JPMorgan, JPMorganChase, Chase, Chase Merchant Services, and Chase Payment Solutions are marketing names for certain businesses of JPMorganChase and its subsidiaries worldwide (collectively, "JPMC"). Products or services may be marketed and/or provided by commercial banks such as JPMorgan Chase Bank, N.A., securities or other non-banking affiliates or other JPMC entities. JPMC contact persons may be employees or officers of any of the foregoing entities and the terms "J.P. Morgan", "JPMorgan", "JPMorganChase", "Chase", "Chase Merchant Services" and "Chase Payment Solutions" if and as used herein include as applicable all such employees or officers and/or entities irrespective of marketing name(s) used. Nothing in this material is a solicitation by JPMC of any product or service which would be unlawful under applicable laws or regulations.

Investments or strategies discussed herein may not be suitable for all investors. Neither J.P. Morgan nor any of its directors, officers, employees or agents shall incur in any responsibility or liability whatsoever to the Company or any other party with respect to the contents of any matters referred herein, or discussed as a result of, this material. This material is not intended to provide, and should not be relied on for, accounting, legal or tax advice or investment recommendations. Please consult your own tax, legal, accounting or investment advisor concerning such matters.

Not all products and services are available in all geographic areas. Eligibility for particular products and services is subject to final determination by JPMC and or its affiliates. This material does not constitute a commitment by any JPMC entity to extend or arrange credit or to provide any other products or services and J.P. Morgan reserves the right to withdraw at any time. All products and services are subject to applicable laws, regulations, and applicable approvals and notifications. The Company should examine the specific restrictions and limitations under the laws of its own jurisdiction that may be applicable to the Company due to its nature or to the products and services referred herein.

Any mentions of third-party trademarks, brand names, products and services are for referential purposes only and any mention thereof is not meant to imply any sponsorship, endorsement, or affiliation.

Notwithstanding anything to the contrary, the statements in this material are not intended to be legally binding. Any products, services, terms or other matters described herein (other than in respect of confidentiality) are subject to, and superseded by, the terms of separate legally binding documentation and/or are subject to change without notice.

Changes to Interbank Offered Rates (IBORs) and other benchmark rates: Certain interest rate benchmarks are, or may in the future become, subject to ongoing international, national and other regulatory guidance, reform and proposals for reform. For more information, please consult: https://www.jpmorgan.com/global/disclosures/interbank_offered_rates.

JPMorgan Chase Bank, N.A. Member FDIC. Deposits held in non-U.S. branches are not FDIC insured. Non-deposit products are not FDIC insured.

JPMorgan Chase Bank, N.A., organized under the laws of U.S.A. with limited liability.

© 2025 JPMorgan Chase & Co. All Rights Reserved.