2020 NACHA OPERATING RULES CHANGES

FIRST HORIZON

OBJECTIVE

The objective of this document is to provide a summary-level description of the 2020 Revisions to *NACHA Operating Rules and Guidelines*. This is NOT intended to be an inclusive summary of all of the Rules. Please refer to pages ORxxv-ORxxxvii of the *2020 NACHA Operating Rules and Guidelines* for additional detail.

Effective March 20, 2020:

INCREASING THE SAME DAY ACH DOLLAR LIMIT

This new rule increases the Same Day ACH maximum per-transaction dollar limit to $100,000.

Key Components:

- The current per-transaction maximum limit is $25,000.
- The cutoff times for Same Day ACH will remain unchanged.
    - In order to meet the Federal Reserve processing times, First Horizon has established the following cutoff times:
        - 12:45 PM Eastern Time – Business Banking Online
        - 1:30 PM Eastern Time – Direct Transmission

Impact to Participants:

- Originators, Third-Party Service Providers (TPSPs) and Third-Party Senders (TPSs) should discuss with their financial institution whether originating up to $100,000 same day transactions is appropriate for their business.
- This increases the possible use cases for same day ACH.
    - B2B ACH payments, which tend to involve higher per-transaction amounts.
    - Claim Payments, which are typically for larger dollar amounts and are time sensitive in nature.
    - Increases the pool of transactions for Reversals, which are eligible for same day processing.
- Originating Depository Financial Institutions (ODFIs) and Receiving Depository Financial Institutions (RDFIs) will need to determine what system and operational changes need to be made to accommodate the increased limit.

Effective April 1, 2020:

DIFFERENTIATING UNAUTHORIZED RETURN REASONS

This new rule will better differentiate between unauthorized return reason codes for consumer debits. This differentiation will provide ODFIs and Originators clearer information when a customer claims that an error occurred with an authorized payment. ODFIs and Originators will be able to react differently to claims of errors and potentially avoid taking more significant action with respect to such claims.

Key Components:

- The rule re-purposes an existing reason code (R11) that will be used when a receiving customer claims that there was an error with an otherwise authorized payment.
- Return Reason Code R11 will be defined as "Customer Advises Entry Not in Accordance with the Terms of the Authorization." The use of a distinct reason code (R11), will allow for the receiver to convey a meaning of "error" instead of "no authorization" and will be used for:
    - The debit entry is for an incorrect amount.
    - The debit entry was debited earlier than authorized.
    - The debit entry was part of an incomplete transaction.
    - The debit entry was improperly reinitiated.
    - For ARC or BOC entries:
        - The source document was ineligible.
        - Notice was not provided to the Receiver.
        - The amount of the entry was not accurately obtained from the source document.
- Currently, return reason code R10 is used as a catch-all for various types of underlying unauthorized return reasons, including some that have a valid authorization.
- Return Reason Code R10 will be defined as "Customer Advises Originator is Not Known to the Receiver and/or Originator is Not Authorized by Receiver to Debit Receiver's Account" and will be used for:
    - Receiver does not know the identity of the Originator.
    - Receiver has no relationship with the Originator.
    - Receiver has not authorized the Originator to debit their account.
    - For ARC or BOC entries, the signature on the source document is not authentic or authorized.
    - For POP entries, the signature on the written authorization is not authentic or authorized.
- R11 returns will have many of the same requirements and characteristics as R10 returns and will be considered unauthorized under the Rules.
- A key difference between R10 and R11 will be that with an R11 return, the Originator will be permitted to correct the error, if possible, and submit a new entry without being required to obtain a new authorization.
- Written statements of unauthorized debits will need to be restated to align with the revised return reasons.

Impact to Participants:

- ODFIs will need to educate their Originators on the changes for return reason codes R10 and R11.
- The rule will provide ODFIs and Originators with more precise reasons for return.
- The rule will allow for better corrective action/resolution.
- Could avoid more significant action when the underlying problem is an error (e.g. obtaining a new authorization or closing account).
- ODFIs will need to make changes to return reporting to reflect the re-purposed code.
- RDFIs will need to update processes and procedures to properly use the repurposed return reason codes.
- The rule will change the 2-day timeframe for R11 to a 60-day return timeframe.
- Potential system changes for ODFIs, RDFIs and Originators.

Effective July 1, 2020:

ACH CONTACT REGISTRY

All ACH Network financial institutions will be required to register contact information with NACHA. This information will include all personnel or departments responsible for ACH operations and fraud/risk management. This information will be made available to all the participating financial institutions, Payment Associations, ACH Operators, and NACHA. Use of the registry will be for proof of authorization requests, ACH-related system outages, erroneous payments, duplicates, reversals, fraudulent payments, etc.

Key Components:

- Beginning July 1, 2020 all ACH network financial institutions will be required to register contact information.
- All financial institutions must register by October 30. 2020.
- Registration will be done via the NACHA risk management portal.

Impact to Participants:

- ODFIs and RDFIs will be required to add contact information by the due date stated above.
- ODFIs and RDFIs will be required to implement procedures to keep the information up-to-date.

Effective March 19, 2021:

SUPPLEMENTING FRAUD DETECTION STANDARDS FOR WEB DEBITS

The existing rules require Originators of WEB debit to use a "commercially reasonable fraudulent transaction detection system" to screen WEB debits for fraud. With the implementation of this rule, the current screening requirement will be enhanced to make it explicit that "account validation" is part of a "commercially reasonable fraudulent transaction detection system."

Key Components:

- The requirement will apply to all new WEB debit authorizations on a going forward basis and any changes to the existing WEB debit account number authorizations.

Impact to Participants:

- Originators of WEB debits may need to update their fraud detection systems to comply with the rule and perform account validation. These changes could increase the cost of originating WEB debits.
- Originators that do not currently perform any fraud detection will need to implement a system to do so.
- RDFIs may start receiving a greater volume of ACH prenotification, micro-transactions, or other account validation requests.

Effective March 19, 2021:

EXPANDING SAME DAY ACH

This new rule expands access to Same Day ACH by allowing Same Day ACH transactions to be submitted to the ACH Network for an additional two hours every business day. The new Same Day ACH processing window will go into effect on March 19, 2021.

Key Components:

- Currently, the latest that an ODFI can submit files the ACH Operators with same day ACH transactions is 2:45 PM ET.
- The new window will allow same day ACH transaction to be submitted to the ACH Operators until 4:45 PM ET.
- RDFIs will receive files from this third window by 5:30 PM ET. Funds received in this third window will need to make the funds available to receivers by their end of day processing.
- All debits, credits, and returns will be eligible to be processed in the new same day window, with the exception of International ACH Transactions, Automated Enrollment Entries, and entries that exceed the $100,000 limit.

Impact to Participants:

- Originators should discuss with their financial institution whether using this third window will be appropriate for their business.
- ODFIs will need to determine whether to implement origination in the third window. If so, they will need to update their systems and procedures to accommodate same day processing. ODFIs will need to establish processing deadlines for their Originators to ensure they meet the ACH Operator's deadline.
- RDFIs will need to update their processing systems and procedures to handle same day transactions received in the third window, including making funds available by end of day processing.

Effective June 30, 2021:

SUPPLEMENTING DATA SECURITY REQUIREMENTS

This change to NACHA Operating Rules will enhance the quality and improve risk management within the ACH Network by supplementing the existing account information security requirements for large volume Originators and Third Parties.

Key Components:

- The existing NACHA data security requirements will be updated to require large, non-financial institution Originators, TPSPs and TPSs to protect deposit account information by rendering it unreadable when it is stored electronically in their systems.
- This will be implemented in two phases:
    - Phase 1 – Compliance required by June 30, 2021 for Originators, TPSPs, and TPSs with ACH transmission volume greater than 6 million entries in the 2020 calendar year.
    - Phase 2 – Compliance required by June 30, 2022 for Originators, TPSPs, and TPSs with ACH transmission volume greater than 2 million entries in the 2021 calendar year.

- Third Parties must consider the combined volume of entries processed for all of its various clients when determining if it meets the annual volume thresholds.
- If an account number is used for any ACH payment (consumer or corporate), it must be rendered unreadable while stored electronically.
- Although the new rule does not apply to the storage of ACH account information in physical, paper form, the requirement to render the account information unreadable DOES apply if these paper authorizations or other documents containing ACH account numbers are scanned for electronic record retention and storage purposes.
- While PCI standards are not required to be compliant with this rule, PCI DSS includes specific requirements related to protecting data while at rest. Utilizing one of these prescribed methods of data protection for ACH-related account numbers, in such a manner as to be compliant with the standard, should meet the commercially reasonable requirement for this Rule.

Impact to Participants:

- Qualifying Originators, TPSPs, and TPSs will need to become compliant by the due dates listed in each phase above.
- For Originators, TPSPs, and TPSs, accounts payables and accounts receivables systems will be impacted, as may be other systems (for example, claims management systems for insurance companies). This also includes systems on which authorizations are obtained or stored electronically, as well as databases or systems platforms that support ACH entries.
- ODFIs will need to inform their qualifying originators of their requirements and ensure they have made the necessary changes to comply with the rule.
- Non-financial-institution Originators that do not meet the requirements are still encouraged to voluntarily adopt these standards as a sound business practice.