epcor®

2021

ACH Rules

Update for

Corporate

Originators

Nacha®
Direct Member

EPCOR, as a Direct Member of Nacha, is specially recognized and licensed providers of ACH education, publications and advocacy.

There are several changes to the *ACH Rules* which take effect in 2021. Here is a breakdown of the changes that apply to corporate users.

New Same Day ACH Processing Window
Effective March 19, 2021

This *Rule* creates a new processing window that enables ODFIs and Originators to originate same-day transactions for an additional two hours each banking day. The new window allows Same Day ACH files to be submitted to the ACH Operators until 4:45 PM ET (3:45 PM CT). RDFIs receive files from this third window by 5:30 PM ET (4:30 PM CT), with interbank settlement occurring at 6:00 PM ET (5:00 PM CT). RDFIs need to make funds available for credits processed in the new window by the end of their processing for that Settlement Date. All credits and debits, and all returns, are eligible to be settled in the new Same Day ACH window, except for International ACH Transactions (IATs), Automated Enrollment Entries (ENRs) and forward entries more than the pre-transaction dollar limit.

<u>Corporate ACH Originators, Third-Party Senders and Third-Party Service Providers:</u> These ACH participants should discuss with their financial institutions whether using the third Same Day ACH window is appropriate for their business.

<u>Corporate ACH Receivers:</u> Receivers, particularly non-consumer Receivers, should be prepared to receive ACH debits and credits later in the day. These participants should review their internal procedures to determine whether any changes are required.

Supplementing Fraud Detection Standards for WEB Debits
Effective March 19, 2021

Several years ago, to help prevent fraudulent payments from being initiated through ACH over the internet, Nacha implemented a requirement for WEB Originators to implement a commercially reasonable transaction detection system. The current requirement to screen WEB debits for fraud has been enhanced to make it explicit that "account validation" is part of a "commercially reasonable fraudulent transaction detection system." The supplemental requirement will apply to the first use of an account number or changes to the account number. For existing WEB debit authorizations, the rule will be effective on a going-forward basis. Originators will have to perform account validations as there are updates to account numbers in existing authorizations.

<u>Corporate ACH Originators:</u> Originators of WEB debits may need to re-tool their ACH fraud detection systems to comply with the *Rule*. Those Originators of WEB debits not currently performing any fraud detection will need to implement a system to do so.

<u>Corporate ACH Receivers:</u> This *Rule* should have little impact on Corporate ACH Receivers.

Limitation on Warranty Claims
Effective June 30, 2021

Under the current *ACH Rules*, an ODFI warrants that an ACH entry has been properly authorized by the Receiver. The *Rules* allow extended returns for unauthorized entries for limited periods but do not establish a time limit on the ODFI's warranties. That time is determined by statutes of limitations, which vary from state to state, and can be as long as ten years.

The Limitations on Warranty Claims Rule will limit the length of time an RDFI is permitted to make a claim against the ODFIs authorization warranty. For an entry to a non-consumer account, an RDFI may make a claim for one year from the Settlement Date of the entry. This time frame is like the one-year in UCC 4-406 that applies to checks and items charged to bank accounts.

For an entry to a consumer account, the limit will cover two time periods:
1. The RDFI may make a claim for two years from the Settlement Date of the Entry. This time is longer than the one-year period in Electronic Funds Transfer Act and allows for additional time for extenuating circumstances. (In other words, the RDFI can make a claim for unauthorized debits settling within the most recent two years from the date of the RDFI's claim.)
2. Additionally, an RDFI may make a claim for entries settling within 95 calendar days from the Settlement Date of the first unauthorized debit to a consumer account. The 95-day period is designed to allow RDFIs to make claims for all cases where they may be liable to their consumer under Regulation E, which requires a consumer to report unauthorized transfers within 60 days of the financial institution's transmittal of a statement to avoid liability for subsequent transfers.

<u>Corporate ACH Originators:</u> Originators should see a reduction in claims that fall outside the time periods established by the new *Rule* and may see liability for some older transactions shift to RDFIs and Receivers.

<u>Corporate ACH Receivers:</u> Receivers should review their statements and report unauthorized activity in a timely manner. The new *Rule* addresses consumer authorizations. Unauthorized returns for Corporate (CCD or CTX) debits have not changed. Terms of the debits should be outlined in the trade agreements executed between two corporate entities using the ACH network to pay for goods or services.

Supplementing Data Security Requirements

Effective June 30, 2021 (6 million or more ACH transactions)
Effective June 30, 2022 (2 million or more ACH transactions)

The Supplementing Data Security Requirements Rule expands the existing ACH Security Framework to explicitly require large, non-financial institution Originators, Third-Party Service Providers and Third-Party Senders to protect account numbers used in the initiation of ACH entries by rendering them unreadable when stored electronically. The *Rule* aligns with existing language contained in PCI requirements; thus, industry participants are expected to be reasonably familiar with the manner and intent of the requirement.

The *Rule* applies only to account numbers collected for or used in ACH transactions and does not apply to the storage of paper authorizations. The *Rule* also does not apply to depository financial institutions when acting as internal Originators, as they are covered by existing FFIEC and similar data security requirements and regulations.

Implementations of the Supplementing Data Security Requirements rule will begin with the largest Originators, Third-Party Service Providers and Third-Party Senders, and will initially apply to those with ACH volume of six million transactions or greater annually. A second phase will apply to those with ACH volume of two million transactions or greater annually.

Thresholds are based on annual ACH volume in 2019 (6 million) or 2020 (2 million). Originators are required to know their total ACH volume, regardless of the number of financial institution relationships they use for ACH origination.

<u>Corporate ACH Originators:</u> If you are considered a "large" Originator, based on the thresholds above, this *Rule* applies to you. If your ACH transaction volume exceeds the thresholds, ensure that you are adequately protecting any information you collect electronically. The account numbers must be rendered unreadable when collected and stored electronically. If you are not a large Originator, you may still consider using this practice of securely storing account numbers electronically as a sound business practice.

<u>Corporate ACH Receivers:</u> This *Rule* should have little impact on Corporate ACH Receivers.

Reversals

Effective June 30, 2021

Currently, the *ACH Rules* define a limited number of permissible reasons for Reversing Entries; however, they do not explicitly address improper uses of Reversals. The Reversals Rule will specifically state the initiation of Reversing Entries or Files for any reason other than those explicitly permissible under the *ACH Rules* is prohibited. The Reversals Rule will also explicitly define within the *ACH Rules* non-exclusive examples of circumstances in which the origination of Reversals is improper. Specifically:
* The initiation of Reversing Entries or Files because an Originator or Third-Party Sender failed to provide funding for the original Entry or File; and
* The initiation of a Reversing Entry or File beyond the time permitted by the *ACH Rules*.

The Reversals Rule will also:
* Establish additional formatting requirements for reversals in which the Company ID/Originator ID, SEC Code and Amount fields of the Reversing Entry must be identical to the original entry. The *Rule* will require the name of the Originator to reflect the same Originator identified in the Erroneous Entry to which the Reversal relates. (Minor variations to the Originator's name will be permissible for accounting or tracking purposes provided the name remains readily recognizable to the Receiver.) The contents of other fields may be modified only to the extent necessary to facilitate proper processing of the reversal.
* Explicitly permit an RDFI to return an improper reversal. Upon receiving a consumer claim, an RDFI may return an improper Reversing Entry using Return Reason Code R11. The RDFI will need to obtain a Written Statement of Unauthorized Debit from the consumer Receiver and return the entry in such time that it is made available to the ODFI no later than the opening of business on the banking day following the sixtieth (60th) calendar day following the Settlement Date of the improper Reversing Entry.
An RDFI may return an improper Reversing Entry to a Non-Consumer account by using Return Reason Code R17. These returns will need to be made in such time as to be made available to the ODFI no later than the opening of business on the second Banking Day following the Settlement Date of the improper Reversing Entry. RDFIs will also be permitted to user R17 to return an improper reversal that it identifies without client contact within the same 2-day return time frame.
* Expand the permissible reasons for a Reversing Entry to include an error in the effective entry date. These will include the reversal of a debit entry that was for a date earlier than intended by the Originator and the reversal of a credit entry that was for a date later than intended by the Originator.

<u>Corporate ACH Originators and Third-Party Senders:</u> Originators and Third-Party Senders may want to review their practices, policies and controls regarding the proper use and formatting of Reversals.

<u>Corporate ACH Receivers:</u> This *Rule* should have little impact on Corporate ACH Receivers.

Meaningful Modernization
Effective September 17, 2021

The five amendments comprising Meaningful Modernization are designed to improve and simplify the ACH user experience by facilitating the adoption of new technologies and channels for the authorization and initiation of ACH payments; reducing barriers to use of the ACH Network; providing clarity and increasing consistency around certain ACH authorization processes, and reducing certain administrative burdens related to ACH authorizations.

Specifically, the five *ACH Rules* will:
- Explicitly define the use of standing authorizations for consumer ACH debits;
- Define and allow for oral authorization of consumer ACH debits beyond telephone calls;
- Clarify and provide greater consistency of ACH authorization standards across payment initiation channels;
- Reduce the administrative burden of providing proof of authorization; and
- Better facilitate the use of electronic and oral Written Statement of Unauthorized Debit.

Standing Authorizations

The current authorization framework for consumer ACH debits incorporate recurring and single payments. Recurring payments occur at regular intervals, with no additional action required by the consumer to initiate the payment, and are for the same or a similar amount, for example, a monthly mortgage payment or utility bill. A single entry is a one-time payment and can be between parties that have no previous relationship, such as in a purchase; or between parties that can have a relationship, but the payment is not recurring, such as a single payment on a credit card account. ACH Originators that have, or want to use, a different model for ongoing commerce do not have specific rules for payments that are a hybrid, falling somewhere in between recurring and single entries. By defining a Standing Authorization, the Rule will fill the gap between single and recurring payments and enable businesses and consumers to make more flexible payment arrangements for relationships that are ongoing in nature.

The Standing Authorization Rule will define a standing authorization as an advance authorization by a consumer of future debits at various intervals. Under a Standing Authorization, future debits would be initiated by the consumer through further actions. The Rule will allow for Originators to obtain Standing Authorizations in writing or orally. The Rule also defines Subsequent Entries, which will be individual payments initiated in any manner identified in the Standing Authorization.

The *Rule* will allow Originators some flexibility in the use of consumer Standard Entry Class (SEC) Codes for individual Subsequent Entries. Originators will be able to use the TEL or WEB SEC Codes for Subsequent Entries when initiated by either a telephone call or via the Internet/wireless network, respectively, regardless of how the Standing Authorization was obtained. In these cases, the Originator will not need to meet the authorization requirements of TEL or WEB but will need to meet the risk management and security requirements associated with those SEC Codes.

In addition, the *Rule* will allow for optional formatting so an Originator may, at its discretion, identify an entry as having been originated under the terms of a Recurring, Single-Entry or Standing Authorization. The standard code values will be "R" for Recurring, "S" for Single-Entry, and "ST" for Standing Authorization. An Originator may choose to include these values in the Payment Type Code Field of a TEL or WEB entry or the Discretionary Data Field of a PPD entry. To accommodate this option, the *Rule* will remove the existing requirement that TEL and WEB entries be identified as either Recurring or Single Entries and will designate the Payment Type Code as an optional field. However, Originators may continue to use the Payment Type Code field to include any codes meaningful to them, including "R", "S" or "ST."

<u>Corporate ACH Originators:</u> Originators may choose to use Standing Authorizations and Subsequent Entries but will not be required to do so. Those Originators wanting to use this authorization method may need to modify or add to their authorization practices and language.

<u>Corporate ACH Receivers:</u> This *Rule* should have little impact on Corporate ACH Receivers.

Oral Authorizations

Currently, the authorization language in the *ACH Rules* does not provide for oral authorizations of an ACH payment outside of a telephone call. Only the Telephone-Initiated Entry (TEL) Standard Entry Class Code has requirements to address the risks specific to an oral authorization. The Oral Authorization rule will define and allow Oral Authorizations as a valid authorization method for consumer debits distinct from a telephone call. Enabling the broader use of Oral Authorizations will allow businesses to adopt ACH payments in transactional settings that make use of verbal interactions and voice-related technologies. The *Rule* will not change how existing TEL transactions are used and authorized.

Under the *Rule*, any oral authorization obtained via any channel will need to meet the requirement of an Oral Authorization. An Oral Authorization obtained over the Internet that is not a telephone call also will need to meet the risk and security requirements that currently apply to Internet-Initiated/Mobile (WEB) Entries and will use the WEB Standard Entry Class Code. The *Rule* will allow for Standing Authorizations to be obtained orally. In addition, the *Rule* will allow for Subsequent Entries initiated under a Standing Authorization to be initiated through voice commands, instructions, or affirmations.

<u>Corporate ACH Originators:</u> Originators may choose to use the expanded applicability of Oral Authorizations but will not be required to do so. Those Originators wanting to use Oral Authorizations will need to modify or add to their authorization practices and language to ensure they meet all the requirements for Oral Authorizations. Originators may find their digital storage needs impacted by using Oral Authorizations.

<u>Corporate ACH Receivers:</u> This *Rule* should have little impact on Corporate ACH Receivers.

Other Authorization Issues

In conjunction with the *Rules* on Standing Authorizations and Oral Authorizations, Meaningful Modernization includes the Other Authorization Issues Rule, which covers other modifications and re-organizations of the general authorization rules for clarity, flexibility, and consistency.

Clarity
- Re-organizes the general authorization rules to better incorporate Standing Authorizations, Oral Authorizations, and other changes.
- Defines "Recurring Entry" to complement the existing definition of Single Entry and the new definition of Subsequent Entry and to align with terms in Regulation E.

Flexibility
- Explicitly states authorization of any credit entry to a consumer account and any entry to a non-consumer account can be by any method allowed by law or regulation. Only consumer debit authorizations require a written authorization that is signed or similarly authenticated.

Consistency
- Applies the standards of "readily identifiable" and "clear and readily understandable terms" to all authorizations.
- Applies the minimum data element standards that are currently stated only in the *Rules* for Telephone-Initiated Entries for all consumer debit authorizations.

<u>Corporate ACH Originators:</u> Originators may need to review authorizations to ensure they meet the standards of "readily identifiable" and "clear and readily understandable terms." These participants may also need to review and revise consumer debit authorization language to ensure that it includes the minimum data elements.

<u>Corporate ACH Receivers:</u> This *Rule* should have little impact on Corporate ACH Receivers.

Alternative to Proof of Authorization

Under the current *ACH Rules*, an Originator is required to provide proof of authorization to its ODFI in such time the ODFI can respond to an RDFI request for proof of authorization within ten banking days. Some ODFIs and Originators report a "pain point" occurs when they provide proofs of authorization, but then debits are returned as unauthorized. To avoid this, some ODFIs and Originators would prefer to agree to accept the return of the debit rather than expend the time and resources necessary to provide proof of authorization.

The Alternative to Proof of Authorization Rule will reduce an administrative burden on ODFIs and their Originators for providing proof of authorization in every instance in which it is requested by an RDFI. By allowing an alternative, the *Rule* is intended to help reduce the costs and time needed to resolve some exceptions in which proof of authorization is requested. However, if the RDFI still needs proof of authorization, the ODFI and its Originator must provide the proof of authorization within ten days of the RDFI's subsequent request.

<u>Corporate ACH Originators:</u> Originators wanting to take advantage of the *Rule* may have to modify their business processes.

<u>Corporate ACH Receivers:</u> This *Rule* should have little impact on Corporate ACH Receivers.