2021 SUMMARY OF NACHA RULES CHANGES

The objective of this document is to provide a summary-level description of the 2021 Revisions to *Nacha Operating Rules and Guidelines*. This is NOT intended to be an inclusive summary of all of the Rules. Please refer to *2021 Nacha Operating Rules and Guidelines* for additional detail.

Effective March 19, 2021:

NEW SAME DAY ACH PROCESSING WINDOW

The New Same Day ACH Processing Window rule will create a new processing window that will enable ODFIs and their customers to originate same-day transactions for an additional two hours each banking day.

Key Components:

- The new window will allow Same Day ACH files to be submitted to the ACH Operators until 4:45 p.m. ET. RDFIs will receive files from this third window by 5:30 p.m. ET, with interbank settlement occurring at 6:00 p.m. ET.
- RDFIs will 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, will be eligible for settlement in the new Same Day ACH window, with the exception of International ACH Transactions (IATs), Automated Enrollment Entries (ENRs), and forward entries in excess of the $100,000 per-transaction dollar limit.

Impact to Participants:

- Originators, TPS and TPSP should discuss with their financial institutions whether using the third Same Day ACH window is appropriate for their businesses.
- Provident Same Day ACH cutoff times will be 2:30 p.m.
- ODFIs will need to update their internal processing applications and procedures to accommodate returns processed in the last window.
- RDFIs will need to update their internal processing applications and procedures to accommodate receiving late-window Same Day ACH files and sending late-window returns. RDFIs will also need to provide availability for credits received in this window by the end of their processing for that Settlement Date.
- 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.

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, making 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.
  - Possibilities include:
    - An ACH pre-notification
    - ACH micro-transaction verification
    - Commercially available validation service
  - For more information, please see Nacha's **Account Validation Resource Center**.
- RDFIs may start receiving a greater volume of ACH pre-notification, micro-transactions, or other account validation requests.

Effective April 1, 2021:

DIFFERENTIATING UNAUTHORIZED RETURN REASONS (PHASE 2)

Under Phase 1 of the Differentiating Unauthorized Return Reasons Rule, Return Reason Code R11 (Customer Advises Entry Not in Accordance with the Terms of the Authorization) was re-purposed to be used for the return of a debit in which there is an error, but for which there is an authorization. R11 returns have the same processing requirements and characteristics as R10 returns. They are unauthorized under the Rules.

With the implementation of Phase 2 of the Rule, the higher existing Unauthorized Entry Fee will apply to ACH debit entries returned bearing Return Reason Code R11.

Key Components:

- This part of the Rule will be implemented by the ACH Operators, and as with the current fee, will be billed/credited on financial institutions' monthly statements of charges.

Impact to Participants:

- ACH Operators will need to update their systems to accommodate the application of Unauthorized Entry Fees.
- Originators, TPS, and TPSP will be charged the unauthorized fee for returns with the R11 reason code.

Effective June 30, 2021:

LIMITATION ON WARRANTY CLAIMS

Under the current Nacha 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 limit is determined by statutes of limitations, which vary from state to state, and can be as long as ten years.

The Limitation on Warranty Claims Rule (the Rule) will limit the length of time an RDFI is permitted to make a claim against the ODFI's authorization warranty.

Key Components:

- 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 period is analogous to the one-year rule 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 periods:
  - The RDFI may make a claim for two years from the Settlement Date of the Entry. This period is longer than the one-year period in EFTA and allows for additional time for extenuating circumstances.
  - 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 customers under Regulation E, which requires a consumer to report unauthorized transfers within 60 days.

Impact to Participants:

- Originators and ODFIs should see a reduction in claims that fall outside the periods established by the new Rule, and may see liability for some older transactions shift to RDFIs and Receivers.
- RDFIs should examine their processes for handling claims for unauthorized transactions. They may need to make changes to ensure that they only claim entries settling within the periods permissible under the Rules.

SUPPLEMENTING DATA SECURITY REQUIREMENTS

The Supplementing Data Security Requirements rule expands the existing ACH Security Framework to explicitly require large, non-financial institution Originators, TPS, and TPSP 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.

Key Components:

- 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.
- Implementation of the Supplementing Data Security Requirements rule will begin with the largest Originators, TPS, and TPSP and will initially apply to those with ACH volume of 6 million transactions or greater annually.
- A second phase will apply to those with ACH volume of 2 million transactions or greater annually. The effective date for this phase is June 30, 2022.

Impact to Participants:

- ODFIs will need to inform their Originators, TPS, and TPSP of their direct compliance obligation with respect to the rule.
- Originators, TPS, TPSP that are not currently compliant with the rule will need to implement changes to bring their systems into compliance.

Effective January 1, 2021

RULES ENFORCEMENT

The Enforcement rule change defines an egregious violation within the context of rules enforcement as:

Key Components:

- A willful or reckless action by a Participating DFI, Originator, Third-Party Service Provider, or Third-Party Sender, and
- One that involves at least 500 Entries or involves multiple entries in the aggregate amount of at least $500,000.
- The Enforcement Rule allows the ACH Rules Enforcement Panel to determine whether a violation is egregious, and to classify whether an egregious violation is a Class 2 or Class 3 rules violation. The rule expressly authorizes Nacha to report Class 3 rules violations to the ACH Operators and to federal and state banking, consumer protection, and other appropriate regulators and agencies.

Impact to Participants:

- Originating Depository Financial Institutions (ODFIs) and Receiving Depository Financial Institutions (RDFIs) need to be aware of the changes to Nacha's enforcement capabilities.
- Originators, Third-Party Senders (TPS) and Third-Party Service Providers (TPSP) should be aware of the changes since the ACH contract with Provident indicates they comply with Nacha rules.

Effective June 30, 2021:

REVERSALS

Currently, the 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 that the initiation of Reversing Entries or Files for any reason other than those explicitly permissible under the Rules is prohibited. The Reversals Rule will also explicitly define within the Rules non-exclusive examples of circumstances in which the origination of Reversals are improper.

Key Components:

Rules updated to include the following improper reasons:

- 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 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.
- 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 as long as 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 be permitted to user R17 to return an improper reversal that it identifies without customer

contact within the same 2-day return timeframe.

- 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.

Impact to Participants:
- Originators, TPS, TPSP, and ODFIs may want to review their practices, policies and controls regarding the proper use and formatting of reversals.
- RDFIs that want to take advantage of the return process should review policies and practices to facilitate the return of an improper reversal.

Effective August 1, 2021:

ACH CONTACT REGISTRY (PHASE 2)

With the implementation of the first phase of the ACH Contact Registry Rule, all ACH Participating Depository Financial Institutions are required to register contact information for their ACH operations and fraud and/or risk management areas. Registration is done via Nacha's Risk Management Portal.

Key Components:
- Phase 1 became effective on July 1, 2020, the date on which the registration portal was opened for Participating DFIs to begin to submit and query contact information. All Participating DFIs were required to complete their registration by October 30, 2020.
- Under Phase 2, Nacha's enforcement authority for the Rule becomes effective. ACH Participating Depository Financial Institutions that do not register their contact information with Nacha may be subject to a rules enforcement proceeding and fines at the Class 2 violation level.

Impact to Participants:
- ODFIs and RDFIs will be required to register contact information with Nacha, and keep that information up to date. ODFIs and RDFIs will have to establish procedures to ensure that their contact registry information stays current. Financial institutions will need to determine contact information for the purpose of registration and how to route inquiries internally. All ODFIs and RDFIs will need to consider and address the circumstances under which they will use the registry, as well as how to handle and respond to any inquiries they receive.

Effective September 17, 2021:

MEANINGFUL MODERNIZATION

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 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 Statements of Unauthorized Debit.

All Meaningful Modernization Rules will be effective September 17, 2021. Each topic within the group of rules comprising the Meaningful Modernization changes is listed separately below.

MEANINGFUL MODERNIZATION – STANDING AUTHORIZATIONS

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.

Key Components:

- The Standing Authorizations Rule (the 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 Originators to obtain Standing Authorizations in writing or orally.
- The Rule also defines Subsequent Entries, which will be individual payments initiated based on a Standing Authorization. Subsequent Entries will be able to be initiated in any manner identified in the StandingAuthorization.
- 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. In order to accommodate this option, the Rule will remove the existing requirement that TEL and WEB entries must be identified as either Recurring or Single Entries, and will designate the Payment Type Code as an optional field. However, Originators may continue to us the Payment Type Code field to include any codes that are meaningful to them, including “R,” “S,” or “ST.”

Impact to Participants:

- Originators may choose to use Standing Authorizations and Subsequent Entries, but will not be required to do so. Those Originators that want to use this authorization method may need to modify or add to their authorization practices and language.

    ODFIs: Since some volume of Subsequent Entries may have a different SEC Code than under the existing rules, ODFIs should prepare for a potential impact on the application of risk management practices specific to SEC Codes and on the tracking of SEC Code volume, returns and return rates.

MEANINGFUL MODERNIZATION – ORAL AUTHORIZATIONS

Currently, the authorization language in the Nacha Operating 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 Authorizations rule (the 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.

Key Components:

- Under the Rule, any oral authorization obtained via any channel will need to meet the requirement of an Oral Authorization.
- Examples of how Oral Authorizations can be used include:
    - Voice interactions with home digital assistants ("Alexa, pay my bill")
    - Oral authorization of a bill payment via the Internet that is not a telephone call (Facetime, Skype, etc.)
    - A consumer provides a Standing Authorization on a telephone call, and initiates subsequent payments online
- 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.

Impact to Participants:

- Originators may choose to use the expanded applicability of Oral Authorizations, but will not be required to doso. Those Originators that want to use Oral Authorizations will need to modify or add to their authorization practices and language to ensure they meet all of the requirements for Oral Authorizations. Originators may find that their digital storage needs will be impacted by using Oral Authorizations.
- ODFIs: Since some volume of existing TEL volume may migrate to WEB, ODFIs should prepare for a potential impact on the application of risk management practices specific to SEC Codes and on the tracking of SEC Code volume, returns and return rates.
- RDFIs should have no impacts to their receipt and posting of entries.

MEANINGFUL MODERNIZATION – OTHER AUTHORIZATION ISSUES

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

Key Components:

Clarity

- The Rule will re-organize the general authorization rules to better incorporate Standing Authorizations, Oral Authorizations, and other changes.
- The Rule will define "Recurring Entry" to complement the existing definition of Single Entry and the new definition of Subsequent Entry and to align with term in Regulation E.

Flexibility

- The Rule will explicitly state that 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 writing that is signed or similarly authenticated.

Consistency

- The Rule will apply the standards of "readily identifiable" and "clear and readily understandable terms" to all authorizations.
- The Rule will apply the minimum data element standards that are currently stated only in the rules for Telephone-Initiated Entries for all consumer debit authorizations.

Impact to Participants:

- Originators and ODFIs 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.
- RDFIs should have no impacts to their receipt and posting of entries.

MEANINGFUL MODERNIZATION – ALTERNATIVE TO PROOF OF AUTHORIZATION

Under the current Rules, an Originator is required to provide proof of authorization to its ODFI in such time that the ODFI can respond to an RDFI request for proof of authorization within ten banking days.

The Alternative to Proof of Authorization rule (the 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.

Key Components:

- The Rules will allow an ODFI to agree to accept the return of an entry as an alternative to providing proof of authorization.
    - Example – An RDFI requests proof of authorization for a PPD debit; the ODFI would have the option within 10 banking days to either provide proof or agree to accept a return. If the ODFI chooses to accept the return, the RDFI would have 10 banking days to make that return.
- In situations in which the ODFI has accepted, or agreed to accept, a return in lieu of providing proof of authorization, but the RDFI still needs such proof, the RDFI would still retain the ability to obtain it from the ODFI. The ODFI and its Originator must provide the proof of authorization within ten days of the RDFI's subsequent request.

    Example – After an ODFI and RDFI agree on the return of a debit, the RDFI needs to obtain the proof of authorization as part of litigation.
- 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 in requested.

Impact to Participants:

- Originators and ODFIs that want to take advantage of the Rule may have to modify their business processes.
- RDFIs may receive different responses to their request for proof of authorizations. RDFIs will need to develop practices and procedures to send subsequent requests for proofs of authorization in cases where a copy is still needed when ODFI has agreed to accept the return in lieu of providing the copy.

MEANINGFUL MODERNIZATION – WRITTEN STATEMENT OF UNAUTHORIZED DEBIT VIA ELECTRONIC OR ORAL METHODS

Under the Rules, an RDFI is responsible for obtaining a consumer's Written Statement of Unauthorized Debit (WSUD) prior to returning a debit as unauthorized. However, the current Rules do not explicitly address electronically or orally provided WSUDs.

Key Components:

- The Rules clarifies and makes explicit that an RDFI may obtain a consumer's WSUD electronically or orally.
- The WSUD via Electronic or Oral Methods rule (the Rule) will reduce an administrative burden on RDFIs and their customers.
- The Rule clarifies and makes explicit that an RDFI may obtain a consumer's WSUD as an Electronic Record, and an RDFI may accept a consumer's Electronic Signature, regardless of its form or the method used to obtain it.
- These changes will emphasize that WSUDs may be obtained and signed electronically, which could include the same methods permissible for obtaining a consumer debit authorization.

Impact to Participants:

- ODFIs that request copies of WSUDs might receive these documents in various formats.
- RDFIs that want to take advantage of accepting WSUDs by electronic and oral forms will need to incorporate new procedures and technology. These RDFIs will need to be able to meet the requirement to provide a copy of the WSUD upon request.