



ACH Operations Bulletin #4-2020

Nacha Extends Effective Dates of Data Security Rule; Affirms Effective Dates of Other Rules

March 26, 2020

Executive Summary

The upcoming effective dates of the Rule on Supplementing Data Security Requirements are extended by one year, to June 30, 2021 and June 30, 2022, respectively. The effective dates of other approved and upcoming Rules remain in effect.

Discussion

Supplementing Data Security Rule

In November 2018, the Nacha membership approved a set of rule changes related to ACH quality and risk management. Included as part of these rules changes is a supplement to the existing Rules on data security.¹ Under the new Rules, ACH Originators and third-parties will be required to further protect account information while at rest.

In response to requests from some covered parties for additional time to come into compliance with the Rule requirements, Nacha is extending each of the two effective dates by one year:

- Phase 1 of the Rule, which applies to ACH Originators and Third-Parties with more than 6 million ACH payments annually, is now effective on June 30, 2021.
- Phase 2 of the Rule, which applies to ACH Originators and Third-Parties with more than 2 million ACH payments annually, is now effective on June 30, 2022.

Covered parties are urged to become compliant with the new Rule as soon as circumstances permit, but no later than these new effective dates.

Existing Nacha Rules require financial institutions, Originators, Third-Parties Service Providers and Third-Party Senders to establish, implement and update, as appropriate,

¹ The original rule language was provided and explained in Supplement #2-2018 to the Nacha Operating Rules (issued on November 11, 2018, and also published in the 2020 Nacha Operating Rules & Guidelines on Page OR4, with explanation in the preface at Page ORxxx).

security policies, procedures, and systems related to the initiation, processing and storage of ACH transactions.² These policies, procedures, and systems must:

- Protect the confidentiality and integrity of Protected Information;
- Protect against anticipated threats or hazards to the security or integrity of Protected Information; and
- Protect against unauthorized use of Protected Information that could result in substantial harm to a natural person.

The new Rule supplements these existing Rules by requiring ACH Originators and Third-Parties to protect account information used in ACH payments by rendering it unreadable when stored electronically. See Nacha's web site for additional information about the Rule at <https://www.nacha.org/rules/supplementing-data-security-requirements>.

Other Upcoming Rules

Nacha wants to alert ACH participants that the effective date of two other Rules will remain in effect:

- April 1, 2020 – Differentiating Unauthorized Return Reasons – Beginning on the effective date, RDFIs may begin to use return reason code R11 for a debit for which there is an error, but for which there is an authorization. This differentiates R11 returns from those using R10, which will still mean that a consumer claims a debit was not authorized.

As the effective date of this rule is imminent (as of the publication date of the Bulletin), and ACH participants have had nearly one year to prepare, it is not being extended. RDFIs that are not ready to use R11 as of April 1 should continue to use R10.

- October 30, 2020 – ACH Contact Registry – Financial institutions participating in the ACH Network are required to register limited contact information with Nacha by October 30, 2020. While the ACH Contact Registry itself will become available earlier on July 1, 2020, Participating DFIs are not required to register by this date. Therefore this effective date also is not being extended.

² See Section 1.6 Security Requirements, Page OR3.