

Category:

- ACH Quality and Risk

Attention Required:

- Technology/Systems
- Administrative

**Nacha**[®]*End-user Briefing*

Issue Date: July 10, 2020

*Updated: June 2022***Date Effective: June 30, 2021**

Date Approved: November 19, 2018

Supplementing Data Security Requirements

Does this rule impact me?

This rule applies to all merchants, billers, businesses, governments and third parties that send two million or more ACH (electronic) payments per year, debits or credits, regardless of financial institution(s) used for sending. Tier 1 parties (six million or more ACH payments annually) became subject to this rule effective June 30, 2021. The rule becomes effective for all others June 30, 2022. Going forward, if a party's annual volume reaches the two million threshold, they must be compliant by June 30th of the following year.



For more detailed information, including FAQs, see nacha.org/rules/supplementing-data-security-requirements

What is the purpose of this rule?

The existing security framework for the ACH Network is being supplemented to require parties with large volumes to protect an account number that is used in an ACH payment. The account number must be rendered unreadable anywhere the sender has stored it electronically while not in use.

What is the rule?

The rule expands the existing ACH Security Framework rules to explicitly require large senders of payments to protect account numbers by rendering them unreadable when stored electronically.

- Aligns with existing language in the Payment Card Industry Data Security Standard (PCI DSS).

What does the rule NOT cover:

- Data beyond the account number
- Payment methods other than ACH

The rule does not prescribe a specific method of protection, but requires that a commercially reasonable method be used; options include but are not limited to:

- Encryption
- Truncation/Masking
- Tokenization
- Financial Institution-hosted storage solutions

How and when do I prepare for this change?

Determine:

- ACH payment volume for 2020 (by number of payments; not by dollars processed)
 - Total volume, regardless of number of financial institutions used for sending
 - Implement a process to monitor annual volumes to determine if this rule applies to your organization in the future
- All systems that store account numbers used in an ACH payment
- Current account number protection status/IT capabilities

Contact your financial institution(s) and/or payments and technology vendors

- Do they offer or recommend any protection method?

Begin consulting with IT staff or partners on any suggested upgrades/implementations

- Prepare an implementation plan that starts with technology selection
- Review implementation and testing timelines if using a customized solution
- Update policies, procedures, and documentation

June 30, 2021

Parties with six million or more ACH payments in 2019 went live with data protection.

June 30, 2022 and future years

Parties with two million or more ACH payments in 2020 and thereafter must be live with data protection.

Parties that reach 2 million or more ACH payments beginning 2022 and any year thereafter have until June 30 of the following year to come into compliance with the Rule.

