# PAYMENTS NEWS
## FOR TREASURY CUSTOMERS

**2nd Quarter 2021**

## ACH ORIGINATOR RESPONSIBILITIES OBTAINING AUTHORIZATIONS

Obtaining a consumer's authorization is important to ensure the ACH Originator has the proof that the authorization was obtained in compliance with NACHA Rules and Regulation E (consumer protection). Below provides the ACH Originator with general information relating to Rules requirements specific to the authorization.

**CREDIT AUTHORIZATION:** Authorization of a credit Entry to a Consumer Account is not required to be in writing.

**DEBIT AUTHORIZATION:** Authorization of a debit Entry to a Consumer Account must:

- Be in writing and signed or similarly authenticated by the Receiver.
- Provide each Receiver with an Electronic or hard copy of the Receiver's authorization for all debit Entries to be initiated to a Consumer Account.

The following chart provides a breakdown of the types of authorizations that are compliant with the NACHA Operating Rules.

## DEBIT AUTHORIZATION FREQUENCY

| SINGLE AUTHORIZATION | RECURRING AUTHORIZATION | STANDING AUTHORIZATION |
|---|---|---|
| This type of authorization is for a one-time debit payment. | This type of authorization is for recurring debits based on a set timeframe (e.g., January 1, 2021 – January 1, 2023).<br><br>Requires no further action after the authorization is obtained up until the ending date of the authorization. | This type of authorization is for future debits based on a consumer's further action as distinct from recurring entries which require no further action and occur at regular intervals. *NOTE: This new type of authorization has been defined by NACHA and will take effect September 17, 2021.* |

### One-time Debit Authorizations

This type of authorization is obtained for a one-time payment. This type of authorization is to be used when an ACH Originator is debiting the account one time (e.g., a one-time purchase, a one-time dues payment, etc.).

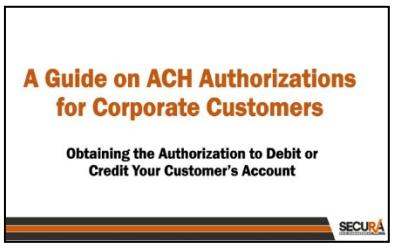
### Multiple, Non-Recurring Debits

Multiple but non-recurring debits are debits in which the amount and time frame for the initiation of the debits may vary. Examples of this type of debit include occasional catalog purchases from the same merchant or occasional purchases of securities with a broker. Originators do not need to obtain a written authorization for each individual debit entry. However, they must have obtained a written authorization up front that establishes a relationship between the Originator and consumer Receiver for this particular type of activity and to which all such entries would apply.

### Standing Authorizations –Authorization Definition Becomes a NACHA Rule September 17, 2021

A standing authorization is 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. NACHA rules allows for Originators to obtain Standing Authorizations in writing or orally. The NACHA Rules 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 Standing Authorization.

### COMPLIMENTARY TRAINING WEBINAR ON ACH AUTHORIZATIONS:




In preparation for the new Standing Authorization rule effective September 17, 2021, we are offering you a complimentary recorded webinar designed to train you on the

responsibilities for obtaining ACH authorizations from consumers and businesses. Contact us to obtain the webinar link and presentation.

## NEW NACHA RULES FOR REVERSING ACH FILES AND ENTRIES: Effective June 30, 2021

This Rule will explicitly address improper uses of reversals. As a reminder, a Reversal is a file or an entry that is reversed once the file or entry has been initiated. Once an entry or file of entries has been transmitted into the ACH Network, it cannot be recalled, but an erroneous or duplicate file may be reversed. If a single entry has been duplicated or originated erroneously, the ODFI may request the RDFI to return the entry. Reversal capability allows fast, efficient, and accurate recovery from an error. Various participants in the ACH Network can initiate a reversal, depending upon the reason for that reversal. This new rule will **expand the permissible reasons for a reversal to include a "wrong date" error**. Contact us if you have any questions on this new rule change.

## DATA SECURITY REQUIREMENTS FOR ACH ORIGINATORS AND THIRD-PARTY SENDERS

Category:
• ACH Quality and Risk

Attention Required:
• Technology/Systems
• Administrative

Nacha

Date Effective: June 30, 2021
Date Approved: November 19, 2018

End-user Briefing
Issue Date: July 10, 2020

**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 – effective June 30, 2021
  – Parties sending six million or more ACH payments per year
- Tier 2 – effective June 30, 2022
  – Parties sending two million or more ACH payments per year

**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.

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

**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

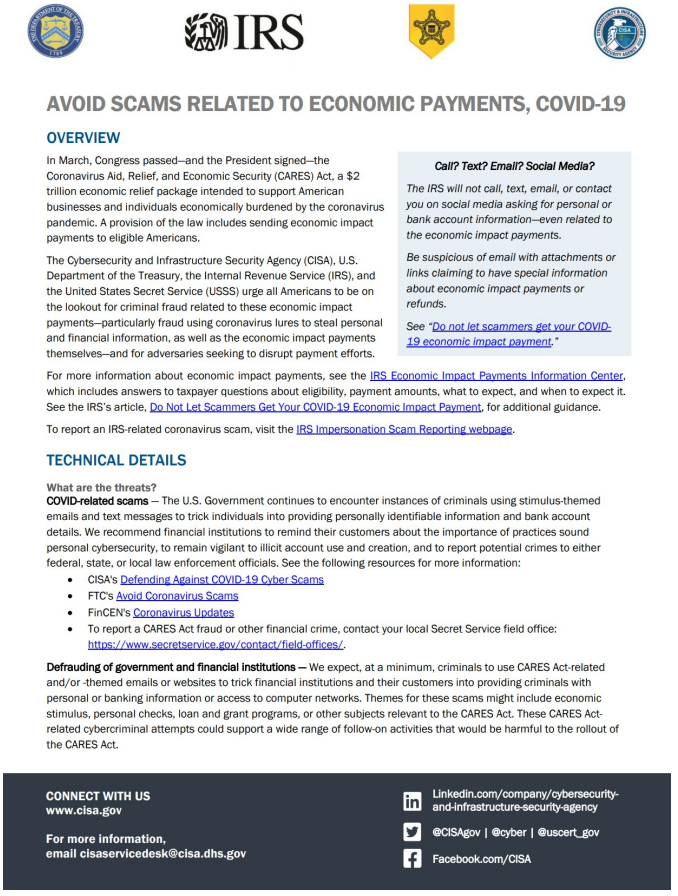
**The rule does not prescribe a specific method of protection**, but requires that a commercially reasonable method be used; options include but are not limited to:

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

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 and it electronically while not in use. NACHA has put out corporate customer quick reference information to better prepare large originators and third-party senders to protect their data. You can obtain additional information by visiting **End_User_Briefing_Supplementing_Data_Security_FINAL.pdf (nacha.org)**.

## TAKE THE TIME: Train Your Employees on Scams related to Economic Payments and COVID – 19

Through COVID-19, we learned of many scams that were attacking businesses and consumers. As fraud rises with contingency events, it is important to train your employees on these types of scams and ensure you have procedures in place to mitigate your fraud risks. In this issue, The Cybersecurity and Infrastructure Security Agency (CISA), U.S. Department of the Treasury, the Internal Revenue Service (IRS), and the United States Secret Service (USSS) teamed up to put together warnings of such attacks. Please take the time to share this with your employees. You can obtain additional information at Avoid Scams Related to Economic Payments, COVID-19 (cisa.gov)



IRS

**AVOID SCAMS RELATED TO ECONOMIC PAYMENTS, COVID-19**

**OVERVIEW**

In March, Congress passed—and the President signed—the Coronavirus Aid, Relief, and Economic Security (CARES) Act, a $2 trillion economic relief package intended to support American businesses and individuals economically burdened by the coronavirus pandemic. A provision of the law includes sending economic impact payments to eligible Americans.

The Cybersecurity and Infrastructure Security Agency (CISA), U.S. Department of the Treasury, the Internal Revenue Service (IRS), and the United States Secret Service (USSS) urge all Americans to be on the lookout for criminal fraud related to these economic impact payments—particularly fraud using coronavirus lures to steal personal and financial information, as well as the economic impact payments themselves—and for adversaries seeking to disrupt payment efforts.

***Call? Text? Email? Social Media?***

*The IRS will not call, text, email, or contact you on social media asking for personal or bank account information—even related to the economic impact payments.*

*Be suspicious of email with attachments or links claiming to have special information about economic impact payments or refunds.*

*See "Do not let scammers get your COVID-19 economic impact payment."*

For more information about economic impact payments, see the IRS Economic Impact Payments Information Center, which includes answers to taxpayer questions about eligibility, payment amounts, what to expect, and when to expect it. See the IRS's article, Do Not Let Scammers Get Your COVID-19 Economic Impact Payment, for additional guidance.

To report an IRS-related coronavirus scam, visit the IRS Impersonation Scam Reporting webpage.

**TECHNICAL DETAILS**

**What are the threats?**

**COVID-related scams** — The U.S. Government continues to encounter instances of criminals using stimulus-themed emails and text messages to trick individuals into providing personally identifiable information and bank account details. We recommend financial institutions to remind their customers about the importance of practices sound personal cybersecurity, to remain vigilant to illicit account use and creation, and to report potential crimes to either federal, state, or local law enforcement officials. See the following resources for more information:

- CISA's Defending Against COVID-19 Cyber Scams
- FTC's Avoid Coronavirus Scams
- FinCEN's Coronavirus Updates
- To report a CARES Act fraud or other financial crime, contact your local Secret Service field office: https://www.secretservice.gov/contact/field-offices/.

**Defrauding of government and financial institutions —** We expect, at a minimum, criminals to use CARES Act-related and/or -themed emails or websites to trick financial institutions and their customers into providing criminals with personal or banking information or access to computer networks. Themes for these scams might include economic stimulus, personal checks, loan and grant programs, or other subjects relevant to the CARES Act. These CARES Act-related cybercriminal attempts could support a wide range of follow-on activities that would be harmful to the rollout of the CARES Act.

**CONNECT WITH US**
**www.cisa.gov**

**For more information,**
**email cisaservicedesk@cisa.dhs.gov**

Linkedin.com/company/cybersecurity-and-infrastructure-security-agency
@CISAgov | @cyber | @uscert_gov
Facebook.com/CISA

***Contact us if you have any questions regarding NACHA Rules, fraud tips or other inquiries about your treasury services.***