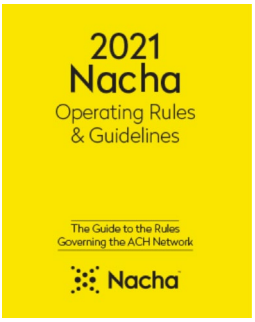
PAYMENTS NEWS
FOR TREASURY CUSTOMERS

1st Quarter 2021

Complying with NACHA Rules



The National ACH Association serves the purpose of administering and operating rules for ACH payments, which define the roles and responsibilities of financial institutions and other ACH Network participants. As a part of being able to participate in the ACH Network, all participants must comply with the NACHA Operating Rules. The Rules apply to all participants that use the ACH network for depositing ACH files such as payrolls, and other types of payments. This means that you as an ACH business customer must comply with *NACHA Operating Rules*. Failure to comply may result in termination from the network making it difficult and, in most cases, impossible to transmit ACH payments. When you signed your ACH agreement with us, you agreed to comply with *NACHA Operating Rules* and all U.S. laws. This means you must follow *NACHA Operating Rules* and comply with U.S. law when sending and/or receiving ACH entries.

New Same Day ACH Deadline becomes Effective March 19, 2021

A new deposit deadline for Same Day ACH will go into effect on March 19, 2021.. This rule provides Originating Financial Depository Financial Institutions (ODFIs) and their ACH Originators and Third-Party Senders an additional ACH same day deposit deadline. The new deadline for Same Day ACH payments is 4:45 p.m. EST. The Same Day deadlines are as follows:

Same Day ACH Operator Deadline	
Same Day Deposit Deadline #1	**10:30 a.m. EST**
Same Day Deposit Deadline #2	**2:45 p.m. EST**
Same Day New Deposit Deadline #3	**4:45 p.m. EST**

An RDFI will be required to make funds available for Same Day ACH credits in this new Same Day ACH processing window no later than the end of its processing day. An RDFI could decide to make funds available sooner than the deadline. For more information regarding Same Day ACH origination and/or your Same Day ACH originating deadlines, contact your account officer.

Consumer Authorization Requirements

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 autohrization.

- **CREDIT AUTHORIZATIONS** - The Originator of a credit entry to a consumer account may be obtained in any manner permitted by applicable legal requirements.

- **DEBIT AUTHORIZATIONS** - All debits to consumer accounts must be authorized by the consumer via a writing that is signed or similarly authenticated by the consumer, with the exception of ARC, BOC, and RCK entries. The authorization requirements for ARC, BOC, RCK, and TEL entries to consumer accounts.

Retention of Authorization.

The Originator must retain an original or copy of a written authorization, and readily and accurately reproducible records evidencing any other form of authorization. The record of authorization must be retained by the Originator for a period of two years following the termination or revocation of the authorization. The authorization may be retained as an electronic record that includes the following:

(1) accurately reflects the information in the record, and (2) is capable of being accurately reproduced for later

reference, whether by transmission, printing, or otherwise.

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 – New NACHA Rule effective 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. With respect to a Standing Authorization, these minimum standards for a consumer debit authorization may be met through a combination of the standing authorization and the receiver's affirmative action to initiate a subsequent entry.

Beware of Business Email Compromise and Vendor Impersonation Fraud

With BEC, legitimate business email accounts are either compromised or impersonated, and then used to order or request the transfer of funds. The fraudster will often compromise one of the business's officers and monitor their account for patterns, contacts and information. The fraudster will often wait until the officer is away on business to use the compromised email account to send payment instructions. This makes the payment instructions more difficult to verify, and at the same time, seemingly more legitimate. The payment instructions will direct the funds to an account controlled by the fraudster.

Fraudsters may create email addresses that are similar to the actual email address making it difficult to spot. Written correspondence may appear to be printed on legitimate letterhead or stationery. Although victims of these scams range from small businesses to large corporations, any business entity could be the target of this form of social engineering. In particular, public-sector entities seem to be targeted because their contracting information is typically a matter of public record. The same is true for vendor fraud. The fraudster will trick the individual into believing they owe the vendor for services rendered and often state that the invoice(s) is overdue and will result in an additional fee if not paid.

Sound Business Practices for Businesses and Public-Sector Entities - Every business, nonprofit, government agency or other public-sector entity should evaluate its internal processes and controls to understand its vulnerabilities to these social engineering frauds. Solid internal controls are key to guarding against these scams. Examples of sound business practices include:

- **Understand** that these types of social engineering attacks are not conducted solely online; the vectors for these attacks can be internet-based or by phone calls, faxes or letters in the mail.
- **Educate** and train employees to recognize, question, and independently authenticate changes in payment instructions, requests for secrecy, or pressure to act quickly.
- **Authenticate** requests to make payment or change payment information. Use known contact information to authenticate payment or change requests, rather than contact information provided with the change request. For example, use an already known telephone number instead of a number provided in a change request.

For more information on this type of fraud, visit the Current Fraud Trends Section of the National Automated Clearing House Association's website at www.nacha.org.

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