PAYMENTS NEWS
FOR TREASURY CUSTOMERS

2ND QUARTER 2022

UPDATE ON UPCOMING NACHA OPERATING RULES -

There are some upcoming Nacha Rules ["Rules"] that are important to share with your internal teams. These Rules cover the micro-debit dollar amounts and the increase in the Same Day ACH item amount. Both of these Rules are significant in the modernization and improvement of the ACH network.

Account Validation: Micro-Credits

Micro-credits are used to test the validity of an account and are used as one of the ways Originators of WEB debits are validating the account as a fraud tool before initiating future WEB debits. In addition, micro-credits are also used to test the validity of accounts for online account opening. Nacha approved a Rule that will define and standardize practices and formatting of Micro-Entries. This new Rule defines Micro-Entries" as ACH credits of less than $1, and any offsetting debits, for account validation. This Rule will be rolled out in two phases including:

Phase 1 Effective Sept. 16, 2022:

- Requires that credit amounts must be equal to, or greater than, debit amounts, and must be transmitted to settle at the same time.
- Originators must use "ACCTVERIFY" in the company entry description field.
- Company name must be easily recognizable to Receivers and the same or similar to what will be used in subsequent entries.

Phase 2 Effective March 17, 2023:

- Originators must use commercially reasonable fraud detection. This includes monitoring forward and return Micro-Entry volumes.

Reminder of Same Day ACH Item to $1MM Effective March 22, 2022

As a reminder, the Same Day ACH dollar amount per item was increased to 1MM for each individual Same Day ACH entry and applies to both debits and credits. This limit is only for the Same Day ACH individual entries and not for next-day transactions. Entries submitted in a same-day processing window that is over $1MM will not be rejected by the ACH Operator but will be processed for next-day settlement in the next available processing window.

BUSINESS EMAIL COMPROMISE (BEC) HIGH ALERT!

Business email compromise continues to be the top cybercrime reported to the Federal Bureau of Investigation's Internet Crime Complaint Center and based on significant increases in fraud and sanctions, treasury customers need to be on the alert and take precautions if they identify suspicious behavior from any existing or future treasury client. Treasury customers are often the targets for these types of attacks. Fraudsters continue to take advantage of businesses and individuals by tricking them into surrendering account information and other sensitive information with the end goal of stealing money and information.

Please take some time and read the below procedures you and your teams can follow to prevent this type of crime.

1. Follow documented controls for the validation of new or revised payment information, and do not stray from these controls unless you escalate to the designated person.

2. Understand how BEC scams work to identify these types of scams.

3. Never trust emails, texts, or unsolicited phone calls to authorize payment requests or change contact information. Always verify.

4. Escalate all concerns if any payment (e.g., ACH, wires, checks, etc.) seems suspicious—even after confirming the payment. Always escalate.

5. Always be very suspicious if a vendor offers vague reasons for changes to a new account, such as tax audits or current events, e.g., "Due to the latest Ukraine disaster, we need to update our payment information to further protect your data."

THE IMPORTANCE OF OFAC: YOUR RESPONSIBILITY TO COMPLY

OFAC is charged with the enforcement of the economic and trade sanctions of the United States and the United Nations. These sanctions may prohibit or limit interactions with people, companies, or banking institutions around the world, and failure to comply with the sanctions and regulations can lead to substantial penalties and fines. While many people are generally aware of the U.S. Department of the Treasury's Office of Foreign Asset Control ("OFAC"), there is a common misperception that only banks need to comply with its rules and enforcement; however, businesses are required to comply to OFAC.

OFAC requirements are documented in your agreement with the financial institution and should be discussed with your internal teams. If you have any questions regarding your obligations to comply with OFAC requirements, please contact your designated account officer.

REMINDER OF YOUR RESPONSIBILITY TO NOT EXCEED UNAUTHORIZED ACH RETURN LEVELS - The current return rate threshold for unauthorized debit Entries is .05%. All Originators and Third-Party Senders that exceed this limit, are required to immediately reduce this percentage and maintain a below threshold return rate. These return reason codes include:

Return Code	Reason for Return
R05	Unauthorized Debit to Consumer Account Using Corporate SEC Code.
R07	Authorization Revoked by Customer
R10	Customer Advises Originator is Not Known to Receiver and/or Originator is Not Authorized by Receiver to Debit Receiver's Account.
R11	Customer Advises Entry Not in Accordance with the Terms of the Authorization.
R29	Corporate Customer Advises Not Authorized.
R51	Item Related to RCK Entry is Ineligible or RCK Entry is Improper.

ACH Originators should be aware of and train all new and existing staff on the importance of monitoring for unauthorized activity over a 60-day period. This becomes even more important based on external fraud threats. An ODFI that has an Originator that breaches this unauthorized threshold would be subject to the same obligations and potential enforcement as currently outlined in the Rules.

- To ensure you fall below this threshold, it is recommended to implement the following internal controls:
- Review/develop reporting to monitor and track unauthorized debit return rates
- Implement a monitoring/notification process with your ODFI when unauthorized activity is close to this threshold limit
- Report on any recurring unauthorized activity and resolve all unauthorized returns prior to initiating the live entry back into the network

For additional information regarding network unauthorized return threshold requirements, contact your designated account officer.