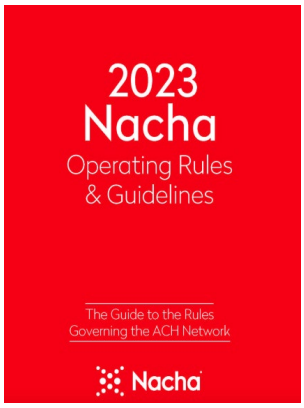
craft bank

PAYMENTS NEWS
FOR TREASURY CUSTOMERS

1ST QUARTER 2023

WHO IS NACHA? As a participant in the ACH Network (ACH Originator or Third-Party Sender), you are required to comply with the NACHA Rules. The Nacha Rules provide the rules framework for ACH network compliance. Nacha was previously the acronym NACHA, which stood for National Automated Clearing House Association.



Nacha's Rule Book is published on an annual basis, and rules are updated through the year. This document outlines rules for ACH participants, which includes ACH Originators, payment processors, financial institutions, and the ultimate user of the ACH network.

It is important to stay informed of the Rules and updates to these Rules, as your agreement with our financial institution binds you to the Nacha Rules and could result in Nacha violations if not followed. We will provide you with quarterly newsletters to keep you informed of the Rules. If you would like a physical copy of the Nacha Rules or an electronic version, visit www.nacha.org.

NACHA RULES ALERT ON MICRO-CREDIT VALIDATION – Micro-credits are used to test the validity of an account and are one of the ways Originators of WEB debits are validating the account as a fraud tool prior to initiating future WEB debits. This Rule defines Micro-Entries as ACH credits of less than $1, and any offsetting debits, for account validation. The first phase went into effect on September 16, 2022, and required the following:

- 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 as or similar to what will be used in subsequent entries

As a reminder, the second phase will become effective March 17, 2023, requiring Originators to use a commercially reasonable fraud detection system to validate the account. Stay tuned for more details on upcoming Nacha Rules.

IMPORTANCE OF POSITIVE PAY SERVICES IN LIGHT OF INCREASED FRAUD

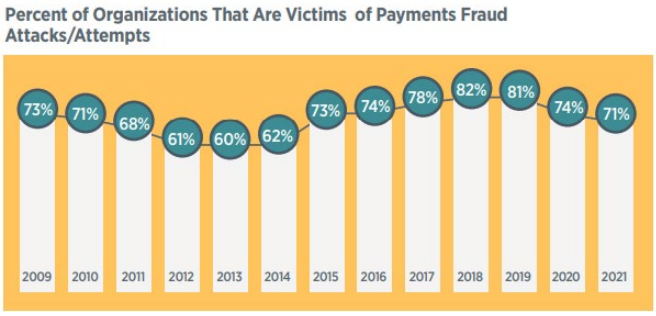
Positive pay is a feature in your cash management system that is an automated service used to deter check and/or ACH fraud. Positive pay is used to match the checks and ACH debits a corporate customer issues/originates with those it presents for payment. Typically, any check and/or ACH considered suspect is sent back to the business customer for examination.

Why sign up for positive pay?

Positive pay provides the tool to protect you from checks and/or ACH presented for payment so you can determine which checks and/or ACH should be paid or rejected. As there is a short window to return any unauthorized entries (24 hours), timing is of the essence, and the use of the positive pay system allows a business client to stay in control of authorized vs. unauthorized payments. With increased fraud and corporate account losses, this tool benefits you and protects your money from being stolen.

FRAUD WATCH: BE INFORMED AND PREPARED

Businesses continue to be the targets of payment fraud attacks. Based on the AFP Payments Fraud Survey, it was noted that *payments fraud activity had been increasing steadily since 2013 and in 2018 reached a new peak. More than 80% of financial professionals reported that their organizations were targeted by fraudsters.*



[source – AFP Payments Fraud Survey).

What can you do to protect your account from fraud?

- Review your authentication practices and discuss with your account officer regarding other available tools
- Train your employees not to click on unknown links or surrender sensitive information to unknown parties
- Sign up for alert services to notify you when funds are withdrawn from your account
- Sign up for positive pay services
- Do not respond to emails and/or act on instructions from an email without validating the authenticity of the request
- Train your internal accounts payable/receivable area on trends in fraud (e.g., emails from CEO/CFO requesting to be paid by unknown vendors)
- Be aware of the latest fraud scams.

Cash Management Administ rators : Importance of Access Reviews

One of the biggest risks to corporate clients is when employees leave the company and access is not deleted by the administrator or access is given to a user who does not need it based on their job responsibilities. Access management is critical based on external fraud threats leading to unauthorized access. The failure to perform user access reviews on a regular basis will place a company at a higher risk for:

- A terminated employee gaining remote access to the network or email system
- Misuse of a dormant administrative account that is still active
- System compromise through the use of terminated user ID and passwords that never expire

REMINDER OF YOUR RESPONSIBILITY WHEN RECEIVING UNAUTHORIZED ACH ENTRIES - The current return rate threshold for unauthorized debit entries is .5%. All Originators 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 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 set forth in the Rules.

In accordance with the Nacha Rules, when receiving unauthorized entries, Originators are prohibited from reinitiating entries without obtaining a new authorization. If Originators re-originate the entries without obtaining a new authorization, this is a direct violation of the Nacha Rules (excluding situations for uncollected and/or NSF which allow Originators to reinitiate an additional two times for collection).