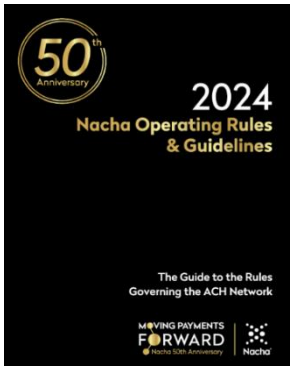
1st QUARTER 2024

PAYMENTS NEWSLETTER

FOR TREASURY CUSTOMERS

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 previously had the acronym NACHA (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 include 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 a Nacha violation 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 OBLIGATIONS: NOTIFICATIONS OF CHANGES AND STEPS AFTER RECEIPT

A Notification of Change (NOC) is a Non-Monetary Entry transmitted by a Receiving Depository financial institution (RDFI) for distribution back to the Originator through the Originating Depository Financial Institution (ODFI). It is created when the RDFI receives a prenotification or a live dollar entry that contains incorrect information. A Notification of Change:

- Identifies the entry that has been received at the RDFI
- Pinpoints the specific information on the entry that is incorrect
- Provides the correct information in a precise format so the Originator can make the change
- Notifications of Change have a unique Standard Entry Class Code, COR, and a unique Addenda Type Code, "98"

Notifications of change occur when a financial institution posts an ACH transaction but is notifying you that any subsequent transactions between you and the receiver should be updated. Information that should be updated will be provided in the NOC. Common NOCs include:

- C01 - Incorrect Account Number
- C02 - Incorrect Routing Transit Number (RTN)
- C03 - Incorrect Routing Transit Number (RTN) and Incorrect Account Number
- C05 - Incorrect Transaction Code (e.g., change from checking to savings or savings to checking)
- C06 - Incorrect Account Number and Incorrect Transaction Code
- C07 - Incorrect RTN, Incorrect Account Number, and Incorrect Transaction Code

For a full list of Nacha Notifications of Change Codes, refer to the most recent Nacha Rules Book.

NEXT STEPS

In most cases when you receive an NOC, your ACH transaction has processed as expected. After receiving an NOC, you will need to update your records and any associated templates to reflect the change to the receiver's account information and ensure that future ACH transactions can be processed correctly. To comply with the Nacha rules, you must make changes to your customer records within six days of receiving an NOC.

Reach out to the receiver to validate the information and, if applicable, get a new authorization with the updated information.

AN ESSENTIAL GUIDE TO ACCOUNTS PAYABLE FRAUD

Accounts payable fraud is a common type of fraud that targets a company's accounts payable department, which is responsible for paying suppliers and other vendors.

Accounts payable fraud can be committed internally by employees, externally by vendors, the two parties working together, or, increasingly, by an outside fraudster looking to gain access to the company's accounts payable systems. Accounts payable fraud is a silent threat faced by many companies.

Accounts payable fraud impacts thousands of businesses both large and small every year. This is due to several factors, including how easy fraud is under traditional AP processes and increased sophistication on the part of fraudsters. In many cases, AP fraud is perpetrated right under the noses of businesses and, in many cases, with their unknowing cooperation.

What types of fraud should your business be on the lookout for?

CHECK FRAUD

In February of 2023, FinCEN issued an alert about a nationwide surge in mail theft-related check fraud scams targeting the U.S. mail. Check fraud occurs when a criminal manipulates a physical check to redirect payments to unauthorized accounts. Check fraud might include adjusting the amount a check is made out for, changing the payee, or writing checks for personal expenses from a business account.

ACH FRAUD

ACH fraud is the process of electronically transferring funds from your company's bank account to an unauthorized account through the ACH network. This can be done through phishing, business email compromise, data breaches, or installing malicious software.

INTERNAL FRAUD

Internal AP fraud is when the business is defrauded by an internal employee at the company. Internal fraud can be committed through submitting false expense reports, altering invoices, setting up fake vendors, and using business funds for personal gain.

10 TIPS FOR FRAUD PREVENTION AND DETECTION

Identifying and preventing cases of Accounts Payable (AP) fraud should be top priority for businesses across all industries. Here are ten tips for fraud prevention and detection.

1. Be proactive — conduct regular audits, monitor key performance indicators (KPIs) closely, watch for red flags, and always check bank statements.
2. Set up a tip line and other ways for employees to report fraud and establish a set of guidelines for protecting them once they do.
3. Conduct background checks on all employees and verify their references.
4. Implement a written code of ethics. This code should be easily digestible and resonate with the industry and business culture. It should include policies outlining conflicts of interest.
5. Implement clear policies for expense reimbursement. Enforce them at the highest levels of the organization.
6. Segregate duties and define roles. At the basic level, divide bookkeeping and check signing authority. Don't have the same person cut the checks, sign the checks, and reconcile the bank accounts.
7. Educate employees on threats posed by phishing attempts and how to identify them.
8. Implement policies for providing appropriate verification of any changes to existing invoices, bank deposit information, and contact information.
9. Check and update the vendor files regularly to keep all vendor information current.
10. Automate the AP process to ensure security and segregation of duties.

While preventing fraud is an ongoing process for many businesses, being aware of the red flags and implementing the right internal controls can help businesses detect and prevent fraud in the future.

For more information on fraud mitigation tools and service offerings please contact:

treasurymanagement@securityfederalbank.com
OR 803-641-3000