craft bank

4th QUARTER 2024

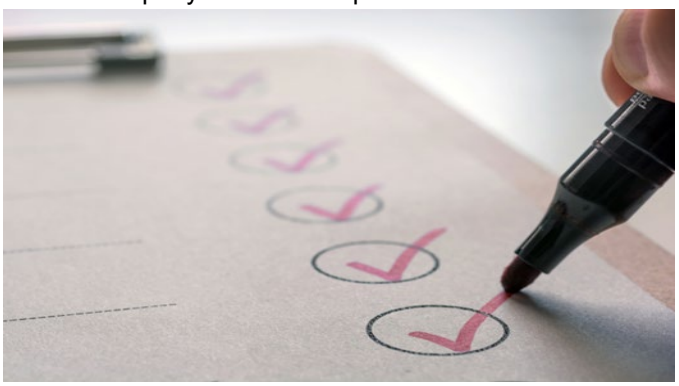
PAYMENTS NEWSLETTER

FOR TREASURY CUSTOMERS

Essential Fraud Prevention Checklist: Safeguarding Vendor Updates in Accounts Payable

Accounts payable fraud is a scam that targets a company's accounts payable department or the team responsible for paying suppliers and other vendors. Accounts payable fraud can be committed internally by employees, externally by vendors, the two parties working in concert, or, increasingly, by an outside party looking to gain access to the company's accounts payable systems.

Fraudsters try to gain access to account information a multitude of ways, including sending an invoice that looks like it is from a legitimate supplier but with instructions changed to a fraudulent account. Before you update any changes to a vendor or send funds to a new vendor, use the checklist below to ensure you are working with the correct company and contact person.



Verbal Authentication Checklist

A checklist should be required for all payment types, including ACH, checks, and wire transfers.

1. Make a phone call to the corporate phone number of the vendor or internal employee with the corporate phone number on the company website. *Do not call a cell phone or number provided in an email*.
2. Ask the vendor/employee to verbally read to you the bank account, bank name, Swift code, or check mailing address. *Do not provide the bank information to the vendor/sender to confirm.*
3. Ask the vendor to identify a unique item (PO number, invoice number, project name, your company's entity address, or key contact at your company)
4. Have a second person verify updated information.

The best way for you to protect yourself against AP fraud is by staying vigilant and closely monitoring transactions and financial statements for inconsistencies, hiring trustworthy employees, and fostering an ethical work environment in which they feel inclined to report fraudulent behavior. Other best practices include clearly defining employees' roles to separate duties among employees and strengthening internal controls to ensure that adequate verification is required to adjust financial statements.

'Tis the Season for Holiday Scams

Holiday scams take advantage of the increase in online shopping, travel, and charitable donations during the holiday season by trying to trick you into giving up sensitive information. Fraudsters understand that you and your teams may be short staffed due to scheduled time off. Beware of the warning signs below.

Warning signs of holiday phishing scams:

- You receive an unsolicited message about an invoice, investment, or online banking credentials. Any email or text message that you didn't request should be treated with caution.
- The message contains a strange link. Phishing scams try to get you to provide sensitive information or infect your device with malware. Always hover over links to see where they're taking you before clicking.

Warning signs of a holiday gift card scam:

- Never pay for goods, services, fees, fines, or taxes with gift cards. Scammers will impersonate your bank, government agencies, or other authoritative people and demand payment in gift cards.

- If you buy gift cards in a store, make sure that they haven't been tampered with. Run your finger over the back to see if the sticker has been scratched off or replaced. Get a receipt so that you can verify the purchase if your card is lost or stolen.

Warning signs of a fake delivery notification text:

- You're asked to enter sensitive information. FedEx, UPS, and other delivery companies won't ask for your SSN or credit card number to "find" your delivery.
- The link in the text takes you to a site that isn't on the official UPS, USPS, or FedEx domains.

How to Avoid Online Holiday Scams

- **Be wary of unfamiliar emails and texts.** Don't open attachments or click on links if you don't know the sender.
- **Never provide sensitive information through unsecured email.** Sharing routing and account numbers should only be done via a secure means.
- **Monitor your accounts**. During the holidays, it's easy to let money flow in and out of your accounts without paying much attention. Check your accounts daily for suspicious activity.
- **Ensure you are on a secure connection**. A lock icon should be on the far-left side of the address bar. This lock signifies a secure connection between you and the site. Click on the lock for more details about the website's security.
- **Don't let a good deal cloud your judgment.** If something seems too good to be true, it probably is. Stay diligent.

The holidays are a time for cheer and getting together with people you love. Don't let scammers ruin your holiday season by defrauding you or stealing your identity.

Properly Using Reversals in ACH

The Nacha Operating Rules are the foundation for every ACH payment, as they define the roles and responsibilities of financial institutions and establish clear guidelines for each Network participant. The Rules cover if and when a reversal is allowed. You can only reverse an exact payment from an account if the conditions satisfy Nacha reversal rules. The Rules dictate a payment may be reversed for the following reasons:

- **Duplicate payment**
- **Incorrect payment recipient**
- **Incorrect payment amount or wrong dollar**
- **Payment date earlier than intended**
- **Payment date later than intended**

Before submitting an ACH reversal entry or file, be sure to verify you have taken the steps below:

Identify the Error: Determine the nature of the error that necessitates a reversal.

Notify the Receiving Party: Inform the recipient of the erroneous transaction and the forthcoming reversal.

Initiate the Reversal Entry: The originator's financial institution will create a reversal entry using the correct SEC (Standard Entry Class) code and include the appropriate reversal transaction code.

Include "REVERSAL" in Description: It is mandatory to include the word "REVERSAL" in the Company Entry Description field of the reversal entry.

Compliance Check: Ensure that the reversal complies with Nacha rules, including the five-day timeframe and the specific conditions under which reversals are allowed**.**

If you are unsure of whether you can properly send a reversal, please reach out to us at: support@craft.bank

If you have questions about the newsletter or would like more information on fraud mitigation tools and service offerings, please contact:

Craft Bank Support:
support@craft.bank
678-736-5060
M-TH 8:30-5:00, F 8:30-4