Company Name

Vendor payment fraud awareness

For accounts payable and anyone who handles vendor requests

Fraudsters impersonate vendors to redirect payments. They can do it inside a real email thread, with real names, logos and invoice numbers. The request looks ordinary: "we have changed banks, please update our details."

Treat every request to change bank details, payment method or remittance address as unverified until it has been checked. **Urgency, or pressure to skip a step, is a warning sign.**

1 Get the change in a proper document

For a new bank account or a bank change, obtain **one** of these:

- The company's completed, signed **Payment Change Form**
- A **bank notice** that identifies the account
- The vendor's **official payment instructions** on letterhead

Bank details typed into an email are not a document.

2 Get a phone number you can check yourself

A verifiable vendor phone number is required with **every** request.

- Check the number against the vendor's official website or an invoice already on file.
- The new email, and anything attached to it, does not count.
- Cannot verify it? Pause, and ask the vendor for a number that can be verified.

3 Submit it, then wait for confirmation

Send the documents and the phone number through the internal request process. The Vendor Team calls to verify **every** new bank account, including first-time setups. A call that comes in from the "vendor" does not replace this check.

Only the Vendor Team enters or changes bank details. Do not use new payment details until the change is confirmed.

Keep the team inbox internal

- Do not give the internal address to vendors or copy vendors on messages to it.
- Write a separate internal message, and check the recipients before sending.
- Remove internal discussion from anything forwarded to a vendor.

! If you suspect fraud

Pause the request and keep the original message. Do not click its links or open its attachments. Tell your supervisor and the Vendor Team, and report it through the security reporting process. **If money may already have been sent, say so immediately** so the bank can be contacted.

This is a reference resource, not official policy. It follows widely published guidance on business email compromise, including the FBI's advice to confirm payment changes by phone using a number already known to be genuine.

Company Name

Bank change checklist

Before you submit a request · print and keep by your desk

Three steps, every time

1 Choose ONE document

- [ ] Completed, signed Payment Change Form
- [ ] Bank notice identifying the account
- [ ] Vendor's official payment instructions on letterhead

2 Get a verifiable vendor phone number

- [ ] It appears on the vendor's official website, or
- [ ] It appears on an invoice already on file

Cannot verify it? Ask the vendor for one you can verify before submitting.

3 Submit the complete request internally

- [ ] Documents attached
- [ ] Phone number included, and where you found it

The Vendor Team makes the verification call. A call from the vendor does not replace it.

Four signs to slow down

"We changed banks."
The most common opening. Real vendors change banks rarely, and they understand being checked.

"This is urgent."
A deadline, a late fee, a threat to stop shipping. Pressure is there to make you skip a step.

A new contact or a new address
An email address one letter off, a reply-to that differs, a person you have not dealt with.

"Call me on this number."
A number that appears only in the request proves nothing. Use one you found yourself.

The one rule to remember: never confirm a bank change using contact details that came with the request.