

Vendor Bank-Change Verification Protocol

A one-page rule for any request to change where you send a vendor's money. Print it, sign it, tape it next to whoever pays the bills.

\$3.05B

reported business email compromise losses in 2025, from 24,768 complaints
FBI IC3 2025 Internet Crime Report

31%

of occupational fraud cases at organizations with fewer than 100 employees involved billing schemes
ACFE Occupational Fraud 2024

\$141K

median occupational fraud loss at organizations with fewer than 100 employees
ACFE Occupational Fraud 2024

Foxpedite does this automatically

This page is the manual protocol. In Foxpedite, the checks that matter are built into how vendors get paid:

- ✓ **Steps 3–4:** vendor bank details live on the vendor record with an audit trail, and approval workflows (Advanced plan) can require a second approver.
- ✓ **Red flags:** an invoice pays only when PO + receipt + invoice match, so a fake invoice with no PO stops at Gate 3.
- ✓ **One vendor record per supplier,** onboarded through the supplier portal, so new vendors and their bank details come in one way, not by email.

Try it free for 14 days: foxpedite.com/register →

The rule: no bank change without a callback and a second approver

- 1 Freeze.** Any request to change a vendor's bank account, remit-to address or payment method is put on hold. No payment goes to the new details until steps 2–5 are complete, however urgent the request sounds.
- 2 Call back on a number you already had.** Call the vendor using a phone number from your vendor file, a past contract or a signed PO - never the number, link or signature in the request. Ask for someone you've dealt with before. Confirm the old account's last 4 digits and the new account details read back to you.
- 3 Second person approves.** A second employee (not the person who took the call) reviews the call log and approves the change in writing. The person who enters bank details in your accounting system must not be the person who approves payments.
FOXPEDITE AUTOMATES THIS approval workflows (Advanced plan) can require a second approver before a vendor change counts.
- 4 Document it.** Log: date, who requested, how (email/phone/letter), number called, who confirmed, old vs new last-4, approver. Keep the original request email with full headers.
FOXPEDITE AUTOMATES THIS bank details sit on the vendor record, with an audit trail of who changed what and when.
- 5 Test and watch.** Send the first payment to the new account as a small amount or after a 24–48 h wait, then confirm receipt by phone. Tell the vendor's contact by phone that the change was made, so a fraudster can't hide it.

Red flags: stop and call

- Urgency or secrecy: "pay today", "don't call, I'm in meetings", "the CEO approved it".
- Lookalike email address or domain (one letter off, extra word, different ending).
- Request arrives right before a big payment, a holiday or month-end.
- New bank in a different state or country from the vendor's location.
- Reply-to address differs from the sender, or the thread was "forwarded".
- Invoice with new remit-to details that otherwise looks identical to the last one.
- Caller or emailer resists a callback or offers their own "verification" number.

If money already went out

1. Call your bank immediately and ask it to recall the transfer and contact the receiving bank.
2. File a complaint at ic3.gov with full transaction details, regardless of the amount.
3. Preserve the emails (with headers); reset passwords and turn on MFA on the email account involved.

Speed matters: in 2025 the IC3 Recovery Asset Team froze \$679M of \$1.16B in attempted theft it worked on (FBI IC3 2025).

Sign-off. We follow this protocol for every vendor payment-detail change, with no exceptions for executives or "urgent" requests.

Owner / CEO signature & date

Person who pays bills signature & date

Sources (verified Oct 18, 2026): FBI IC3, 2025 Internet Crime Report, pp. 8, 17, 26 - https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf · FBI, Business Email Compromise guidance (verify payment/account changes in person or by calling; don't use contact info from the request; report to ic3.gov and your bank) - <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise> · ACFE, Occupational Fraud 2024: A Report to the Nations, Fig. 22 & 24 - <https://www.ivey.uwo.ca/media/kijj5cy/2024-report-to-the-nations.pdf>. General guidance, not legal advice.