FIRM POLICY | PAYMENT VERIFICATION

Firm name

Payment-Change Verification Policy

How our firm handles any request to change where or how we send money.

EFFECTIVE DATE

POLICY OWNER

NEXT REVIEW

Scope. This policy applies to everyone at the firm and to any request, whoever it appears to come from, to change a bank account, routing number, payee name or address, or payment method for anyone we pay.

The rules

1. **No changes by email alone.** We never update payment details based on an email, attachment, text, or a call the other party started. Every request is verified first, however routine it looks.
2. **Call back on a number we already had.** Use the number in our records from before the request arrived, or one we look up ourselves. Never use a phone number, link, or contact named in the request.
3. **Two people for every change.** The person who receives the request does not approve it alone. One of the approvers below confirms the callback happened and was recorded before the record is updated.
4. **Two approvals for large payments.** Any single payment above our threshold amount below needs approval from a second person before it is released, even when no payment details have changed.
5. **Urgency does not skip a step.** Requests marked urgent, confidential, or "just this once" get the same check. Anyone may pause a payment to verify it, and leadership will back that decision.
6. **Confirm the first payment.** After an approved change, confirm with the payee, through the verified contact, that the first payment to the new account arrived.

APPROVER

APPROVER

BACKUP IF BOTH ARE OUT

SECOND-APPROVER THRESHOLD (AMOUNT)

REPORT SUSPICIOUS REQUESTS TO

Calling a vendor or client: a short script

"Hi, this is [your name] from [firm]. We received a request to update your payment details. Before we change anything, can you tell me what changed, including the bank and last four digits?"

Let them give the details. Do not read the new details to them first. Note the date, time, number called and where it came from, and who you spoke with.

If they say nothing changed: do not update anything, and send the request to the contact above.

If a payment has already gone to the wrong account

- Call our bank's fraud line right away and ask for a recall of the payment. Time matters.
- Report it at **ic3.gov** with the full transaction details, whatever the amount.
- Keep every email, attachment, and record related to the request. Do not delete anything.
- Contact the real payee at a number we already had, and notify the internal contact below.

BANK FRAUD LINE

INTERNAL CONTACT (NAME AND PHONE)

ADOPTED BY (NAME AND TITLE)

SIGNATURE

DATE

Template provided by CyberNest Hub (cybernesthub.com). Guidance based on the FBI Internet Crime Complaint Center (Public Service Announcement I-091124-PSA) and the Nacha Payments Innovation Alliance Business Email Compromise Response Action Plan. Educational template, not legal advice. Review before use.