

Verify-Before-You-Pay Policy

Office name _____ · Effective _____ Date _____ · Owner/approver: _____ Name and role _____

Before we send money, add a new payee or change anyone's bank details, we confirm the request by calling a phone number we already had. No exceptions for urgency, and no exceptions for who seems to be asking.

1. What this covers. Wires, ACH (an electronic bank-to-bank payment) or other bank transfers, checks, card payments, payment apps, and any change to a vendor's, client's or employee's bank or payment details (including payroll direct deposit). It also covers any request to buy gift cards.

2. The callback rule. For every covered request that arrives by email, text, chat, voicemail or phone:

- Don't reply, and don't use any phone number, link or contact details in the request.
- Call the person or company on a number we already had: our known-numbers list (_____), a past invoice or contract, or the official website looked up separately.
Where it's kept
- Confirm who asked, the amount, and the account details. Write down the date, time, number called and who confirmed: _____ .
Where the callback log is kept
- If it can't be confirmed, the payment or change doesn't happen.

3. Two-person approval. Two people are required for: any payment over \$ _____ ; any new payee; and any change to bank or payment details, whatever the amount. One person sets it up and does the callback. A second person (_____) checks the callback log and releases it. One person may not do both steps.
Amount
Role(s)

4. Gift cards. We never pay anyone, or buy cards for anyone, with gift cards because of an email, text or call. A request to buy gift cards and send the codes is treated as a scam, even if it seems to come from the owner.

5. Urgent requests. "Urgent", "confidential", "I'm in a meeting" or "don't tell anyone" never skips steps 2 to 4. Anyone who follows this policy and delays a real payment will not be blamed for the delay.

6. If something goes wrong. If money may have gone to the wrong place: call our bank at once (_____) and ask them to recall or reverse the payment; then tell
Bank fraud phone number

_____. The _____ reports it to the FBI's Internet Crime Complaint Center
Contact person Role
(ic3.gov) for business email scams and to ReportFraud.ftc.gov for scams. For gift cards, keep the cards and receipts and contact the card company.

7. Reporting suspicious requests. Report any suspicious payment request to _____ even if you didn't act on it.
Contact person

8. Review. This policy is reviewed every _____ months, and after any incident or near miss.
Months

Approved by: _____ · Signature: _____ · Date: _____
Name Signature Date

Not legal or financial advice. Check this policy against your bank's agreement, your insurance policy and any rules for your industry. Your bank may have its own verification steps; follow whichever is stricter. From the Small-Office Phishing Drill Kit, Tech Cheat Codes, v1.2. Need help? Visit techcheatcodes.com/support/