

Payment Verification Policy

For any request to change bank details or send money

[Company Name] | Effective date: [date] | Owner: [name and title] | Version 1.0

Before you use this: This is a free template from Blue Tree Technology® to help your firm get started. It is not legal advice. Please review it with your attorney and adjust it to your firm, your industry and your obligations before you roll it out. Replace everything in [brackets], and delete this note.

Rule

Before we change any vendor's bank details or send a payment based on an email, we will call and confirm using a phone number we already have on file (not a number from the email or invoice).

What this covers

- New bank account details
- Changes to existing bank details
- “Urgent” payment requests from vendors, partners, or executives
- Links or attachments that ask us to update payment information

How we verify

1. Do not click links or update records from the email.
2. Look up the vendor's known phone number in our records (or call a number we have used before).
3. Call and confirm the request with the person we normally deal with.
4. Only proceed if the details match.
5. Note who we called, when, and what was confirmed.

No exceptions

- Urgency does not override this rule.
- “The boss said to do it” does not override this rule.
- A professional-looking email does not override this rule.

If something feels off

Pause and escalate. It is always safer to delay a payment than to send it to the wrong account.

If money has already been sent

Call our bank's fraud line immediately and report it.

One-line version for invoices or emails

“For your protection and ours, we will always call to confirm any change in bank details before processing a payment.”

Optional additions to discuss with your attorney

The first page is the core policy. The items below are optional ways to tighten it. Keep the ones that fit your firm and delete the rest.

Who this applies to

All employees, owners and contractors who can receive payment requests, update vendor or client records, or approve, release or send payments.

Who to call

Payment verification contact: [name, title, phone]. Escalation contact if that person is unavailable: [name, title, phone]. Bank fraud line: [phone number, kept in our records].

Second approver

Payments above [\$ amount] require approval from a second person who was not involved in the request.

Confirm the details out loud

When we call, we ask the other person to read the payee name, bank, account and routing numbers and the amount to us, rather than us reading them to them.

Voice and video requests

A phone call or video meeting that sounds or looks like a known person is not proof on its own, because voices and faces can be imitated. For high-risk requests from executives, we confirm using [a pre-agreed phrase or second question] and our standard callback.

Telling clients up front

We tell clients how we will and will not send payment instructions, for example: "We will never change wire instructions by email. If you receive a request that appears to come from us, call us on the number you already have."

Record keeping

We keep the verification note (who we called, on which number, when, and what was confirmed) with the payment record for [period, per your attorney and your retention policy].

Review and training

The policy owner reviews this policy at least [annually]. Everyone who handles payments is shown this policy when they start and [at least once a year] afterward, and signs below.

Acknowledgement

I have read and understand the Payment Verification Policy.

Name: _____ Signature: _____ Date: _____