The Invoice Scam That Nearly Cost a Business $95,000

How vendor impersonation works, and the verification step that stopped a wire just in time.

$95,000	1 phone call	$0
wire at risk	stopped the fraud	lost

Cyber Fraud · Vendor Verification · Accounts Payable · Financial Controls

The situation

A manufacturing company received an email that appeared to come from a supplier it had used for years. The message said the supplier had changed banks and asked that the next payment go to a new account.

What almost happened

The email was convincing because the fraudster had studied real messages:

- **Real details** — it referenced an actual open invoice and the correct amount.
- **Look-alike address** — the sender's email differed from the real one by a single letter.
- **Urgency** — it warned of a late fee if payment wasn't sent that day.
- **Ready to send** — accounts payable updated the bank details and prepared a $95,000 wire.

How it was stopped

Before releasing the wire, the controller followed the company's written rule: any change to vendor bank details must be confirmed by calling the vendor at a number already on file, never one in the email. The real supplier said it had not changed banks. The wire was cancelled.

Red flags in the request

Red flag	Why it mattered
Bank change requested by email	The most common setup for payment fraud.
Pressure to pay the same day	Urgency is meant to skip verification.
Sender address slightly different	Look-alike domains are easy to miss on a phone.
New account in a different name or state	Legitimate changes rarely look like this.

What they did next

- Put the call-back rule for bank changes into the written payables policy.
- Required two approvers for wires and for any vendor bank change.
- Trained staff to spot phishing and look-alike email addresses.
- Turned on multi-factor authentication and external-email warnings.
- Reported the attempt to the bank and to the FBI's Internet Crime Complaint Center (ic3.gov).

The outcome

The company lost nothing. Staff now treat every bank-change request as suspicious until verified by phone, and the controller reviews a monthly report of all vendor master-file changes.

Fictional, composite educational scenario. Not an actual IAG client engagement and not legal, tax, or accounting advice. IAG is not a CPA firm or law firm.

© 2026 Integrity Advisory Group, LLC

Self-check: could this happen to you?

- ☐ How do you verify a request to change a vendor's bank details?
- ☐ Do wires and bank changes need two people?
- ☐ Have employees been trained on phishing this year?
- ☐ Would your team pause on an urgent request from a known vendor?
- ☐ Do you review changes to your vendor list each month?

Want to talk through what this means for you?

Integrity Advisory Group opens for client services in 2028. Until then, explore our free checklists, assessments and courses, and subscribe for new case studies each month.

integrityadvisorygroup.org/contact

Educational scenario. This case study is a fictional, composite scenario created for education. It is not an actual Integrity Advisory Group client engagement; names, figures and details are illustrative. It is not legal or accounting advice.

© 2026 Integrity Advisory Group, LLC