The $48,000 Fraud That Started with One Missing Signature

How weak payment approvals and trust without verification created an opening for fraud, and how it could have been prevented.

$48,000
paid on false invoices

14 months
before it was detected

1 person
entered, approved and paid bills

Internal Controls | Fraud Prevention | Vendor Payments | Financial Oversight

The situation

A multi-location service company with 35 employees was growing quickly. The owner trusted a long-time office manager to handle vendor payments and the books. Payments required only one signature, and no one else reviewed the bank statements.

What happened

Over 14 months, the office manager used the gap to pay herself through the company's own vendor process:

- **Fake vendor** — she set up a look-alike supplier name with a bank account she controlled.
- **Duplicate invoices** — real supplier invoices were copied, changed slightly and paid a second time to the fake vendor.
- **No second look** — she entered the bills, approved them and released the payments herself.
- **Hidden in the books** — the payments were coded to supplies, where a rise in spending went unnoticed.

How it was discovered

During a bank's routine loan review, the owner was asked why supply costs had grown faster than sales. A review of 12 months of payments found two vendors with nearly identical names, one with no physical address. A forensic review of the full period quantified the loss at $48,000.

Red flags that were missed

Red flag	Why it mattered
One person entered, approved and paid bills	No one else could catch a false payment.
A vendor with no physical address	Shell vendors often use a P.O. box or a home address.
Supply costs rising faster than sales	Spending did not match business activity.
Bank statements never reviewed by the owner	Unfamiliar payees went unseen.

Controls that would have prevented it

- Require two people for every payment: one to prepare and one to approve.
- Have the owner review bank statement images each month.
- Verify every new vendor's address, tax ID and bank details before the first payment.
- Separate who adds vendors from who pays them.
- Compare spending by category to the budget and to prior years each month.

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

The outcome

The company recovered $18,400 through its crime insurance policy, removed the fake vendor and moved to dual approval for all payments. The owner now reviews the bank statement and a vendor change report every month, which takes about 30 minutes.

Self-check: could this happen to you?

- ☐ Does any one person enter, approve and pay bills?
- ☐ Who outside the bookkeeping role reviews your bank statements?
- ☐ How do you verify a new vendor before paying it?
- ☐ Would you notice two vendors with nearly identical names?
- ☐ Do you have crime or fidelity insurance, and do you know what it covers?

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