TRACEWELL ADVISORY

Vendor bank-detail changes: a one-page check for firms that pay client bills

When a client's vendor says "we've changed banks," the riskiest payment is the next one your team releases. Six questions: would your process catch a redirected payment, and could you show that it did?

PART A: THE RULE (stops the outside request: a fake vendor email)

1. **Call-back.**
   Is every bank-detail change confirmed by calling the vendor at a number you already had on file, not one from the email or the new invoice?

2. **Second person.**
   Does someone other than the person who entered the change approve it before the next payment?
   And who approves when the request comes from the client's owner?

3. **Who can ask.**
   Is it written down who at the client may request a vendor change, and does your team know to set aside requests from anyone else?

PART B: THE EVIDENCE (shows the rule held, including for changes made inside)

4. **The list.**
   Could you produce last quarter's bank-detail changes, with who entered and who approved each one?
   In QuickBooks Online, the Audit Log records that a vendor was edited, but not which field changed. The list usually has to come from your bill-pay tool, the bank portal, or your own change log.

5. **Change, then payment.**
   For each change, how soon was the first payment to the new account made?
   A change followed by a payment within days is the first pattern to look at.

6. **Every time.**
   Has anyone checked that the second approval actually happened on every change, rather than only that the rule exists?

> **How to read your answers.** "No" or "not sure" on questions 1 to 3 is a gap in the rule. "No" or "not sure" on questions 4 to 6 means the rule may work, but nobody could show it.

WHY IT MATTERS

- Redirected payments are not only an outside scam. The ACFE counts an employee re-routing a vendor payment to their own account as "check and payment tampering." In organizations with fewer than 100 employees it appeared in 18% of cases, against 8% in larger ones. Its median loss across all cases was USD 114,000.
- Only 17% of those small organizations used proactive data monitoring, against 58% of larger ones.
- Schemes caught within six months had a median loss of USD 40,000; those that ran 25 to 36 months, USD 250,000.

Source: *Occupational Fraud 2026: A Report to the Nations*. Copyright 2026 by the Association of Certified Fraud Examiners, Inc. Fig. 24, p. 34; definition, p. 106; Fig. 5, p. 15; Fig. 30, p. 44; Fig. 7, p. 17.

Lucas Kulisz, Tracewell Advisory · tracewelladvisory.com · lucas@tracewelladvisory.com

I'm building a monthly analysis of client payment data for bookkeeping and CAS firms. This checklist is free to use and share.

I am not a US CPA, and Tracewell Advisory is not a CPA firm. General information, not advice for a specific client.