Vendor fraud: the schemes, and the control that catches each

For the controller and the AP manager, with the internal auditor reading along: each scheme's shape in the ledger, the agent that flags it and the floor it tests.

Published 23 November 2026

Vendor fraud is a payment to a supplier for something the supplier never earned, or to an account the supplier does not hold. An employee can run it alone or with someone outside the company. Each scheme leaves a shape in your AP data before the payment run, a record or a pair of bills that does not fit the rest. Vendor fraud prevention means reading for those shapes while the bill is unpaid, with a named control on each.

Rever reads your ERP, bank and payment records through their APIs and never writes to them. Its agents raise each issue as a finding for a person on your team to decide in the Inbox. The table's last column names the operating floor in Rever's terms of service and acceptable-use policy that each scheme tries to get around. Your internal auditor can read it as a test plan.

SCHEME	WHAT IT LOOKS LIKE IN THE LEDGER	AGENT THAT FLAGS IT	WHAT YOUR TEAM DOES	FLOOR IT TESTS
A vendor set up twice	Two master records for one supplier; one invoice under each	Spend Guard, on the duplicate bill	Approves the hold or sends it back; your master-data owner merges the records	Recorded approval: the approver signs each bill without seeing its twin
A bank-detail change by email	A new bank account on a live supplier, close to a payment run	Sentinel, with a callback to a known-good contact	A person makes the call; a second person approves the change	Preparer is never approver
Two bills under the approval line	Two same-day bills from one vendor, each under your threshold, over it combined	Sentinel	Routes the pair to the approver the total needs	Approval thresholds and dual approval on material amounts
A vendor that does not exist	A bill with no purchase order or receiving record behind it	Matcher; Investigator refers the indicator to Sentinel	Asks for the receipt; confirms the vendor from records held before its first bill	Preparer is never approver
Price drift on a real vendor	Unit prices above the contract or order, a little higher each bill	Spend Guard	Disputes the error, or takes the growth to purchasing	None; the test is the agreed price

A vendor set up twice

A supplier that sits twice in your vendor master can collect twice on one invoice. If your ERP's duplicate-bill check compares invoice numbers within one vendor, the second copy passes it under the second record.

Rever leaves your vendor master as it is and looks for the effect before the run pays it. Spend Guard detects "exact and near duplicates across budgets, allocation entries, requisitions, purchase orders, bills, claims and payments, including different identifiers for the same economic item". Your AP manager gets Spend Guard's finding with its evidence. Spend Guard requests a hold before the payment run, and its page sets the rule: "Every payment hold needs Inbox approval before it is recorded in Rever; your team is then told on Slack and email and applies it in the payment run." The merge stays with your master-data owner; duplicate vendor records, and the payments they cause covers the master-file controls.

A bank-detail change by email

The sender names a real supplier and real approved invoices, and asks your team to change one field. For a bank-detail change, Sentinel "prepares an independent human callback using a previously trusted contact and known-good details, and never relies on contact details supplied with the change." A person on your team makes the call.

Your approver keeps the payment decision after Sentinel's flag. Sentinel's page says: "A Sentinel pass never substitutes for human authorisation to move funds." If your team wants the supplier out of the run until someone makes the call, Sentinel's page sets the order: "Every proposed payment hold, including a temporary or urgent one, needs Inbox approval before it is recorded in Rever, and your team applies it in the payment run."

Two bills under the approval line

Your threshold sends a bill above a set amount to a senior approver. A vendor, or the employee who orders from it, splits one purchase into two same-day bills, each below the line, and each passes the threshold check on its own.

Sentinel groups related payments, vendors, requesters, dates and descriptions to detect "splitting below approval thresholds", and raises the pair as a finding for a person to review. Its page adds: "Indicators alone do not establish intent or fraud." Your team sends the pair to the approver the combined amount calls for.

Auditor tests the agents themselves. It keeps explicit tests for "duplicate detection, ungated hand-backs, self-approval, approval-floor bypass and unauthorised hold release", so your internal auditor can see whether Spend Guard's duplicate screen worked and whether any agent action skipped an approval.

Add a row for this scheme to your segregation of duties matrix: bills from one vendor in one period, read against the threshold as one. Sentinel flags the pair, an approver with authority for the total signs, and Sentinel's finding with the Inbox decision fills the record column.

A vendor that does not exist

A fictitious vendor bills for goods nobody delivered. The bill looks right, with a plausible name and coding that matches a real expense. The gap sits behind the amount: no purchase order and no receiving record.

Matcher "Verifies that every transaction is supported by the correct, contractually consistent documents", and its page adds that "Amount equality alone never makes a match." A bill with no receipt behind it stays open as missing evidence. If the missing receipt looks like more than a lost document, Investigator passes it on: "A suspected fraud indicator is referred to Sentinel, not declared proven."

Your team asks the warehouse for the receipt and confirms the vendor through records your company held before its first bill. The floor under test is the preparer rule. Rever applies it to each action it records, and your matrix can carry it back to vendor setup: the person who set up the vendor and keyed its bill does not approve its payment.

Price drift on a real vendor

A real supplier can overcharge in small steps: a unit price above the contract on one line, then a little higher on the next order. Each bill clears approval because its total looks like the month before.

Spend Guard compares unit prices, totals and expected discounts with purchase orders, contracts and prior transactions, "separating price drift from volume, mix, currency and timing changes". Its page keeps growth apart from error: "Vendor growth may be a negotiation opportunity rather than an accounting error, and is labelled as such." Your AP manager disputes an error with the supplier and hands a negotiation point to purchasing.

No floor applies to a real bill from a real vendor; the control is the contract price Spend Guard reads each bill against.

The schemes, on your own records

Inside a free Proof of Value, the zero-day scan runs on a limited period of your data that you agree up front. On AP, the scan checks for duplicate payments and for price drift against the order or contract. Set its findings beside two lists from your own files for the same period: the changes to vendor bank details, and the same-day bills from one vendor that each sat under your threshold.

Questions

What is vendor fraud?

Vendor fraud is a payment to a supplier for something it never earned, or to an account it does not hold. The schemes include a vendor set up twice, a bank-detail change, bills split under an approval threshold, a fictitious vendor and price drift. Each leaves a shape in your AP data before the payment run.