

5 Signs Your Company's Resources Are Being Misused – and How to Catch It Early

Opinions expressed by Entrepreneur contributors are their own.

In 2023, Apple revealed a case of serious internal fraud. A longtime employee had exploited his access to procurement systems, diverting company funds, manipulating vendor relationships and approving fake invoices. The fallout: nearly \$19 million in losses.

This wasn't a Hollywood-style embezzlement. It was slow, quiet and unnoticed for years. It started with unchecked trust and processes that weren't built to flag abuse.

As entrepreneurs, we often think internal fraud is a big-company problem. It's not. It's a systems problem. If you're building a company, here are five warning signs your resources might be slipping through the cracks – and what you can do to stop it early.

Related: Deter the Inside Job. 5 Ways to Avert Employee Theft and Fraud.

1. Expenses that don't match the function

If you're seeing tools or services being expensed by departments that don't need them, that's a red flag. I once saw a marketing team regularly expensing high-end video editing software – all for one person. Turns out, it was being

used for a personal YouTube channel.

This type of misuse often flies under the radar because it doesn't look like employee theft. But it adds up.

What to do: Implement project-based expense tracking using tools like Divvy or Expensify. Use a hierarchical project code structure that ties expenses to teams, campaigns and dates. Review monthly reports by category to spot anomalies.

2. Unknown or unverified vendors

Fraud often hides in vendor lists. Fraudsters might create fake vendors or manipulate existing vendor accounts to siphon off funds under the guise of legitimate payments. In fact, over 60% of businesses reported facing attempted or actual payment fraud, much of it tied to vendor-related schemes like fake vendors, duplicate invoices and inflated billing.

What to do: Audit your vendor master list every quarter. Cross-check tax IDs, physical addresses (Google them) and contact details. Tools like Tealbook or Apex Portal can help streamline verification. Also, enforce dual authorization for any new vendor setup.

Flag vendors receiving more than three payments in 30 days or those with round-number invoices. These are patterns fraudsters rely on.

Related: 'Trust But Verify' Is How to Fight Back Against Employee Theft and Fraud

3. Employees who avoid oversight or vacation

One of the most overlooked signs is behavioral. People committing fraud often insist on "doing it all themselves" and never take leave – because they're afraid someone else will

uncover what they've been hiding.

What to do: Use role-based permissions and require peer review for all approvals. Platforms like SAP Concur or NetSuite allow audit trails and delegation during leave. Rotate key responsibilities annually, and encourage mandatory time-off. It's not just good for mental health – it protects your systems.

Also, foster a culture of transparency. If your team feels safe raising concerns, you'll hear about problems long before they show up in the books.

4. Recurring transactions that just slip below approval limits

This one's clever. A team member submits \$4,950 payments when the approval threshold is \$5,000. Once? Fine. Monthly? That's a red flag.

What to do: Adjust approval limits every quarter. Use transaction velocity monitoring in your ERP to flag repeat vendors or payees with high-frequency, low-value invoices. Set alerts for anyone trying to split invoices or payments.

In QuickBooks or Oracle NetSuite, for example, you can set workflow rules to escalate anything with unusual frequency, or sudden vendor activity spikes.

5. Missing documents or vague paper trails

When people start “losing” receipts or submitting retroactive justifications, you may have a problem. Fraud isn't always about what's visible – it's about what conveniently isn't.

What to do: Move to a cloud-based documentation system like

DocuWare or Zoho WorkDrive. Require receipts to be uploaded within 48 hours of a transaction. Implement a digital approval chain and audit logs. If documentation is delayed more than once, escalate.

Why good people go rogue

Not all misuse is malicious. Sometimes, it's pressure. Financial stress, feeling overlooked or just seeing others get away with it can trigger someone to justify poor decisions. That's why creating a transparent and fair environment matters just as much as having strong controls.

Talk about integrity openly. Make ethics part of performance conversations. And make it clear that your systems aren't about suspicion – they're about fairness and sustainability.

The role of tech in staying ahead

Beyond accounting software, smart companies are using:

- **AI-powered anomaly detection** (e.g. MindBridge, DataSnipper)
- **Real-time dashboards** tracking spend per department (e.g. Datarails, Cube)
- **Policy enforcement bots** in Slack or Microsoft Teams that remind users of rules when they submit expense-related queries (e.g. Compliance.ai)

You don't need all of these. But you do need systems that grow with your business.

Related: The 5 Most Common Fraud Scenarios for Small Businesses

Prevention is cheaper than cleanup

Resource misuse rarely starts with outright theft. It starts with small allowances, unchecked assumptions and leaders being

too busy to notice.

If you're reading this, take one action this week. Run a vendor audit. Update your approval policies. Review your expense categories. Just pick one.

Because the truth is, it's a lot easier to fix a leak than to mop up a flood.

In 2023, Apple revealed a case of serious internal fraud. A longtime employee had exploited his access to procurement systems, diverting company funds, manipulating vendor relationships and approving fake invoices. The fallout: nearly \$19 million in losses.

This wasn't a Hollywood-style embezzlement. It was slow, quiet and unnoticed for years. It started with unchecked trust and processes that weren't built to flag abuse.

As entrepreneurs, we often think internal fraud is a big-company problem. It's not. It's a systems problem. If you're building a company, here are five warning signs your resources might be slipping through the cracks – and what you can do to stop it early.

The rest of this article is locked.

Join Entrepreneur+ today for access.

<https://www.entrepreneur.com/money-finance/5-signs-of-internal-company-theft-and-how-to-catch-it/491051>