
8 Strategies
to Stop Financial
Losses Before
They Happen
Mechanics Bank®

Executive Summary

A manufacturing business lost $157,000 last Tuesday from a fake invoice. The CFO caught it two days later — too late to get the money back.

Fraud threats hit your business daily. These are not abstract risks but real attacks aimed at companies like yours. Scammers change tactics constantly, but your defense plan can be simple.

This guide shows you eight fraud controls that actually work.

You'll learn how to:

- Spot your weak points before criminals do.
- Build checks that close dangerous gaps.
- Protect your money without slowing your business.
- Catch wrong activity within hours, not weeks.

---

1 Spot Your Weak Points Before Criminals Do

Fraudsters target places where money moves, approvals happen, and checking falls short. Look at your business through a fraudsters eyes: Where would you strike to steal money?

Track how payments flow in and out. Note who handles each step. Find where one person controls too many steps. Most businesses worry about rare events while missing common threats like changed invoice details.

TO CHECK YOUR RISKS:

1. **Map money movement** from start to finish.
2. **Find single failure points** where one person has too much control.
3. **Test your checking steps** to expose gaps.
4. **Start with high-dollar processes** first.

You don't need experts — your accountant and operations manager can find most weak spots in one afternoon by asking: "How could someone steal money here?", "Who checks this?" and "What happens when approvers are out?"

Once you find weak spots, make it clear who watches each one.

2 Define the Responsibilities: Remove the Gray Areas

Unclear job duties create perfect fraud openings. When nobody clearly owns a step of the process, it often doesn't happen — especially with vendor payment changes.

Clear roles mean stating exactly who does what to prevent fraud. Your plan should spell out who can start payments, who must approve them, who checks the work, and who steps in when someone's away.

Many businesses use vague terms like "the accounting team will handle it." This creates far bigger problems than assigning clear duties.

TO SET CLEAR ROLES:

1. **Make a simple chart** showing which person handles each task.
2. **Split up duties** so the same person doesn't both create and approve.
3. **Write down who to tell** when something looks wrong.
4. **Name backups** for every key role.

Focus on your three riskiest areas first. Create a one-page list showing who owns each checking point, answering: "Who verifies vendor changes?" and "Who reviews unusual transactions?"

---

3 Establish Policies and Procedures: Create the Roadmap

Random processes create confusion, which opens doors for fraud. When employees each handle the same tasks differently — especially checking vendor details — fraudsters target the weakest approach.

Good policies set clear rules for handling money, approving payments, and checking information. These aren't thick manuals but short guides that remove the guesswork. Create solid policies to cover vendor management, payment approvals, banking changes, cash handling, and expense reports.

Most policies fail because they are too complex. When rules feel too burdensome, people create shortcuts that skip important checks.

TO CREATE POLICIES THAT WORK:

1. **Focus on high-risk areas first.**
2. **Keep steps simple** (five steps or less when possible).
3. **State clearly how to check** information.
4. **Plan for rush situations** without skipping all checks.
5. **Put policies where people will see them.**

Start with one-page checklists for your most important processes: vendor payment changes, wire transfers, and expense reports. Good policies balance protection with simplicity. If following a rule feels too hard, people will find ways around it.

---

4 Implement Approval Processes: Add the Checkpoints

When one person can handle an entire payment alone, fraud becomes easy. This happens most with expense reports, vendor payments, and account changes.

Good approval systems add checking at key points in your money workflows. They set dollar limits, require backup documents, and create records showing who approved what and when.

The most common breakdown? Rubber-stamp approvals when managers sign off without really checking, especially busy executives who don't review supporting documents.

TO BUILD APPROVAL STEPS THAT WORK:

1. **Set dollar thresholds** and require more approvals as amounts increase.
2. **Require two people** to check vendor banking changes.
3. **Build approvals into your software** instead of using email.
4. **Require supporting documents** matching the payment size.
5. **Test the process occasionally with a deliberate mistake.**

Focus your approval rules on new vendor setup, large payments, and unusual transactions. For most businesses, a simple system works best: regular payments need one approval, larger ones need two, and unusual ones need executive review.

5 Conduct Regular Audits: Verify What's Actually Happening

Most fraud continues for months because nobody's looking for it. Regular checks cut this time dramatically by making sure your controls actually work — not just exist on paper.

Good auditing means checking that people follow your rules and that the rules actually stop fraud. This includes planned reviews, surprise checks, outside confirmation, and looking for odd patterns.

Standard financial audits may miss fraud because they focus on getting numbers right, not catching theft. They sample random transactions instead of looking for patterns and often come with advance notice.

TO CHECK YOUR CONTROLS WELL:

1. **Focus on where money moves** most often.
2. **Do surprise checks** without warning.
3. **Confirm with outsiders,** like calling vendors directly.
4. **Look for unusual patterns** in timing, amounts, or frequency.
5. **Test your controls** by trying to get around them.

You don't need a special audit team. Start with quarterly reviews of vendor management, payment processing, and expense reports, plus random spot-checks in between.

6 Educate Your Employees: Create Your Human Firewall

Your people are your strongest defense against fraud — if they know what to watch for. Fraud succeeds because employees miss warning signs, like slightly changed email addresses or odd payment instructions.

Good fraud training isn't just annual compliance meetings. It creates real awareness about current threats for each job role. Include role-specific training, updates on new scams, clear reporting steps, real examples, and a no-blame policy.

Generic training fails because it doesn't connect to daily work. People can't apply theoretical concepts when real threats appear.

TO BUILD TRAINING THAT WORKS:

1. **Tailor to each department** (Accounts Payable faces different risks than sales).
2. **Use real examples** from your industry.
3. **Make it hands-on** with job-specific scenarios.
4. **Keep it current** as new scams emerge.
5. **Praise people who spot** threats.

Focus training on your three biggest risk areas, typically fake emails, social engineering tricks, and vendor impersonation schemes. Show concrete examples of warning signs for each person's job.

---

7 Invest in Cybersecurity: Your Digital Shield

Digital security isn't separate from fraud prevention — it's essential. Today's fraudsters hack emails, create fake websites, and use tech attacks that target payment processes. Most financial fraud starts online before becoming a stolen payment.

Focus your digital security on the places attackers target most: email accounts handling payment instructions, banking portals, vendor systems, and financial apps. The goal isn't perfect security — it's making your business harder to attack than others.

Many businesses buy complex security while skipping basics. An expensive threat system won't help if you haven't turned on two-factor authentication for your bank account.

TO SECURE YOUR DIGITAL WORLD:

1. **Turn on email authentication** (SPF, DKIM, DMARC).
2. **Use two-factor authentication** on all financial systems.
3. **Call to confirm** payment change requests.
4. **Create separate accounts** for financial tasks.
5. **Keep systems updated** with security patches.

Start with your banking portals and email accounts, which face the most attacks. Simple steps like two-factor authentication, callback verification for payment changes, and email filters that flag suspicious addresses cut your risk dramatically without high costs.

---

8 Monitor & Review: Keep Your Shield Strong

Static controls quickly become outdated as fraudsters adapt to find gaps. Even the best systems weaken without regular monitoring and updates to address new risks and business changes.

Good monitoring means regularly checking that your fraud controls still match your current risks and operations. This includes tracking whether people follow procedures, finding new weak spots as your business changes, spotting unusual patterns, and measuring how well controls work.

Most businesses initially set up strong controls but stop maintaining them. The monitoring feels like extra work with no immediate benefit—until fraud happens and reveals how protection has weakened.

TO MONITOR YOUR CONTROLS WELL:

1. **Review quarterly** across all eight control areas.
2. **Set up warning signs** that signal potential problems.
3. **Test your own defenses** by trying to bypass them.
4. **Learn from close calls,** not just actual fraud.
5. **Update your controls** based on findings and business changes.

Start with weekly checks of your highest-risk areas: review vendor payment information changes, check unusual transactions, verify approval documentation, and confirm appropriate system access. Good monitoring needs consistent attention, not big resources.

Build Your Financial Fortress

These eight controls work as a connected system, not as isolated tools. Risk checks inform your job assignments. Policies guide approval steps. Audits verify everything works. Training empowers people. Technology strengthens defenses. Monitoring keeps everything working.

The most fraud-proof businesses share one quality: they adapt. They constantly refine controls as their operations change and new threats emerge. They see near-misses as learning opportunities, not false alarms.

Start with your three highest-risk areas — typically vendor management, payment processing, and banking changes. Then expand gradually. You'll find that good fraud prevention protects your money and improves operations through clearer processes, better documentation, and stronger accountability. This lets you focus on growing your business instead of constantly defending it.

Discover how we safeguard your information, and get tips on ways to protect yourself and your business.

MechanicsBank.com/Security