LIMOGE | Consulting

THE RISK REPORT

limogeconsulting.com

Welcome to the first edition of *The Risk Report*

I'm excited to introduce *The Risk Report*, an annual publication from Limoge Consulting. This resource was created with one goal in mind: to help leaders like you strengthen financial operations through **clear, independent, and practical insights.**

In every edition you'll find:

Fraud and risk trends you need to know now
Treasury best practices that improve efficiency and resilience
Tools and resources to help you evaluate your own operations
Real-world lessons drawn from 20+ years of experience in treasury and banking

My hope is that *The Risk Repor*t becomes a resource you look forward to - not full of noise, but packed with ideas you can put to work right away.

Let's drive into the first edition, where we explore **the hidden costs of fraud** and how even small process changes can have a big impact on protecting your cash flow.

All the best,

Becky

CONTENTS

Feature Article

The Hidden Costs of Fraud: Why Every Dollar Lost Really Costs Four

When most leaders think about fraud, they focus on the immediate dollar amount stolen. A fraudulent check clears for $5,000, or a payment diversion scheme reroutes a $20,000 ACH. But the true cost of fraud is far higher than the face value of the loss.

According to the Association for Financial Professionals (AFP), **every $1 lost to fraud typically costs $4 or more** once you include investigation, recovery, reputational damage, and lost productivity.

The Ripple Effect of Fraud Losses

1. **Investigation & Remediation –** Time spent by your team, external auditors, or law enforcement isn't free. Even if funds are recovered, staff hours and legal fees accumulate quickly.
2. **Reputational Impact –** Fraud damages trust with donors, clients, vendors, and employees. Once confidence is shaken, it can take years to rebuild.
3. **Operational Disruption –** Fraud often halts normal processes. Vendors may not be paid on time, reconciliations pile up, and finance staff scramble instead of focusing on growth.
4. **Future Costs –** Organizations often overcorrect by layering on costly new systems after a fraud incident — investments that might have been implemented more strategically beforehand.

Hidden cost of fraud, cont.

Simple Defenses That Pay Off

The good news: you don't need expensive systems to reduce risk. The most effective protections are often straightforward:

- **Daily reconciliations** to catch anomalies quickly.
- **Dual approvals** for ACH and wire transactions.
- **Positive Pay and ACH filters** to block unauthorized items.
- **Regular reviews of user access** to online banking and financial systems.

Why This Matters Now

Fraud attempts are at record highs, and criminals are adapting as fast as technology changes. While you can't eliminate risk entirely, you can build resilience. Addressing vulnerabilities proactively ensures you don't just protect dollars — you **safeguard your time, your reputation, and your ability to focus on what matters most.**

The Risk Radar

Fraud Attempts are Rising: What 71% of Organizations Experienced Last Year

Fraud is no longer a rare event — it's the norm. According to the Association for Financial Professionals (AFP), 71% of organizations reported attempted or actual fraud in 2024. That means **nearly three out of four finance teams faced fraudsters trying to infiltrate their operations.**

The most common schemes? Business email compromise, check fraud, and unauthorized ACH transactions. Criminals are adapting quickly, exploiting faster payments, remote work, and human error to slip past defenses.

Even when attempts fail, they drain time and resources. Finance teams spend hours investigating alerts, reconciling accounts, and reassuring leadership. And if an attack succeeds, the fallout can **ripple far beyond the dollar amount** — damaging vendor trust, disrupting operations, and triggering costly remediation.

The takeaway: **fraud is no longer "if," but "when."** That's why proactive defenses matter more than ever. **Simple controls** — like daily reconciliations, Positive Pay, dual approvals, and strong user access reviews — remain the most effective way to stay ahead of the statistics.

Efficiency Spotlight

Faster Payments, Faster Risks: The Dark Side of Real-Time Transactions

The promise of faster payments is appealing: instant transfers, improved cash flow, and better customer experience. But speed comes with a cost — reduced time to detect and stop fraud.

In traditional payment channels, banks and businesses often have hours or even days to catch fraudulent items before funds clear. With real-time payments, the window is gone. Once money moves, it's often unrecoverable.

That's why organizations adopting faster payments need to pair the benefits with stronger defenses.

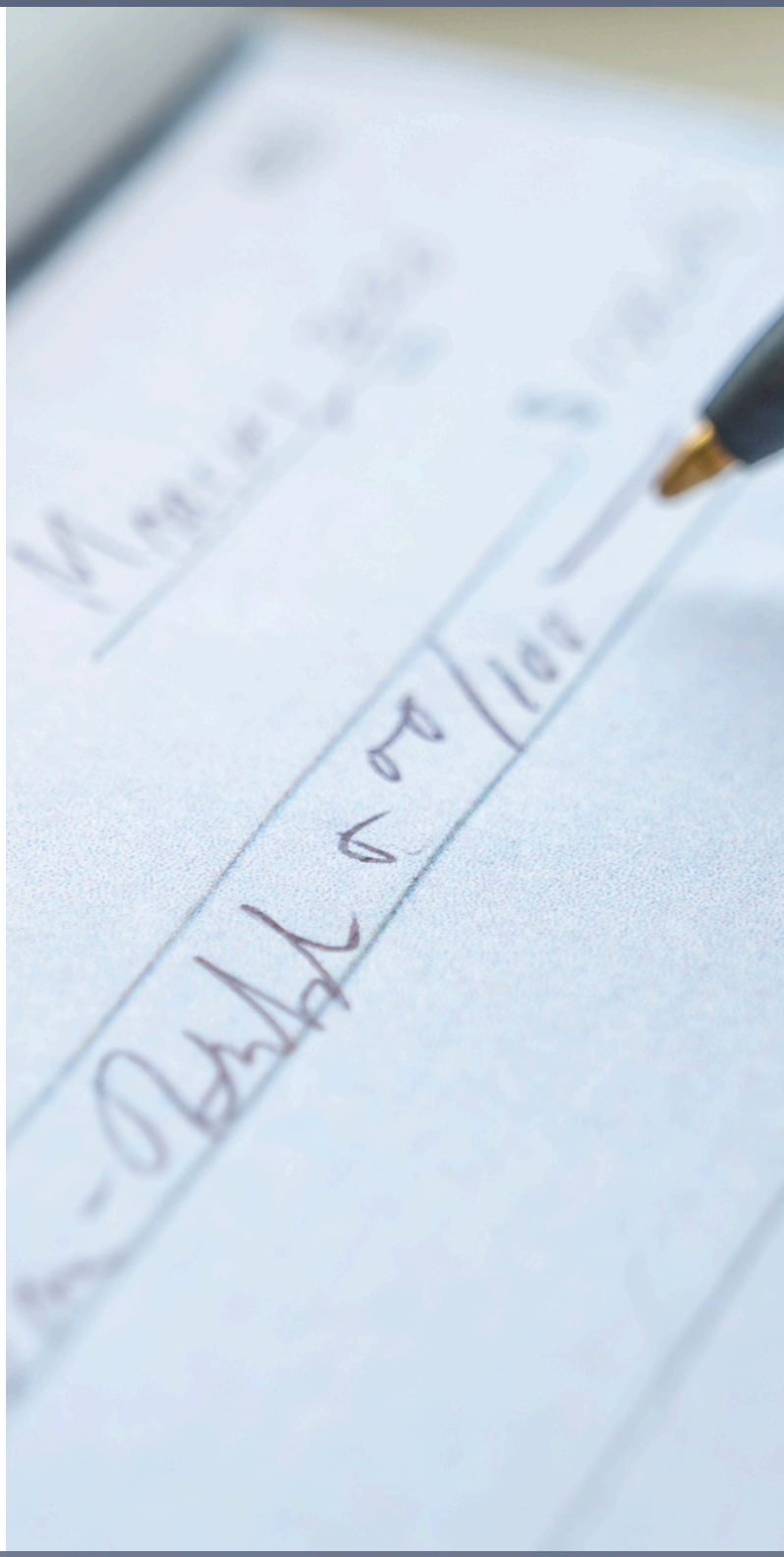
Consider:

- **Dual approvals** on all high-value transactions.
- **Real-time alerts** for outgoing payments.
- **Tighter user controls** over who can initiate or approve transfers.

Faster payments can improve your operations — but without proper safeguards, they can also accelerate fraud losses.

Quick Tip: frequently review your bank alerts and dual controls to ensure the right people are getting the right information.

Check Fraud Still #1 - Why Paper Isn't Going Away



It might surprise some, but despite the growth of digital banking, **check fraud remains the most common type of payment fraud.** Criminals continue to exploit checks through theft, forgery, and alteration, costing businesses millions each year.

Why are checks still such a big target?

- They contain **sensitive information:** account numbers, routing numbers, even addresses.
- They're **easily intercepted** in the mail.
- Many organizations still rely on checks for **vendors, refunds, or payroll.**

While volumes of checks may be declining overall, they continue to present outsized risk.

To reduce exposure:

- **Implement Positive Pay** with payee verification.
- **Shift recurring payments** to ACH or card programs where possible.
- **Educate staff and vendors** on the risks of mailing or accepting checks.

Paper isn't disappearing overnight — and until it does, **checks will remain a prime fraud target.**

Quick Tip: consider every check an invitation for fraud. Leverage secure electronic payment methods when possible.

Case in Point

Key takeaways

- Implement (and use!) Positive Pay services
- Check Positive Pay exceptions daily
- Reconcile daily
- Use and frequently review dual controls

Case in Point: The Cost of Weak Controls at a Nonprofit

A mid-sized nonprofit discovered that an employee had been quietly writing unauthorized checks to themselves over a period of more than a year. The fraud went undetected because the organization only performed bank reconciliations quarterly, and no one else reviewed check images.

By the time it was caught, the **losses exceeded $200,000**. Even after recovery efforts, the organization spent countless hours on investigations, audits, and reputational repair. Donors questioned the nonprofit's internal controls, and board members had to reassure the community that changes were being made.

What changed:

- The nonprofit moved to **daily reconciliations** instead of quarterly.
- It implemented **Positive Pay with payee verification** through its bank.
- It introduced **dual approvals** for disbursements, ensuring no single person had control.

The impact was immediate: fraud risk was cut dramatically, donor confidence returned, and the finance team had greater visibility into day-to-day cash flow.

This case underscores a crucial point: **fraud doesn't just cost money — it costs trust.** Simple internal controls can protect both your finances and your reputation.

Case in Point: When a School District Became a Target

A large U.S. school district recently fell victim to a payment diversion scheme that **cost more than $600,000.** Fraudsters impersonated a construction vendor, submitting what looked like legitimate emails and forms requesting an update to ACH payment instructions. The district's finance staff complied — **unknowingly sending multiple payments directly into the criminal's account.**

The fraud wasn't discovered until the real vendor followed up on unpaid invoices weeks later. By then, most of the money was **unrecoverable.** Beyond the financial loss, the district faced public scrutiny and had to divert staff time to explain what happened and rebuild trust with both vendors and taxpayers.

What changed afterward:

- The district implemented a **call-back verification policy** — requiring staff to confirm any vendor banking change by phone, using a number on file (not the one in the request).
- It added **dual approvals** for all vendor payment changes.
- Finance staff received targeted training to **recognize common red flags in payment fraud schemes.**

This incident shows that even well-staffed public entities are vulnerable. Strong controls — **especially around vendor changes** — are critical for preventing what's become one of the **fastest-growing types of fraud.**

Always, always (always!) call back vendors to confirm payment changes.

Remember to use a known contact on file - never reply to an email.

Tools & Resources

How exposed is your organization to fraud?

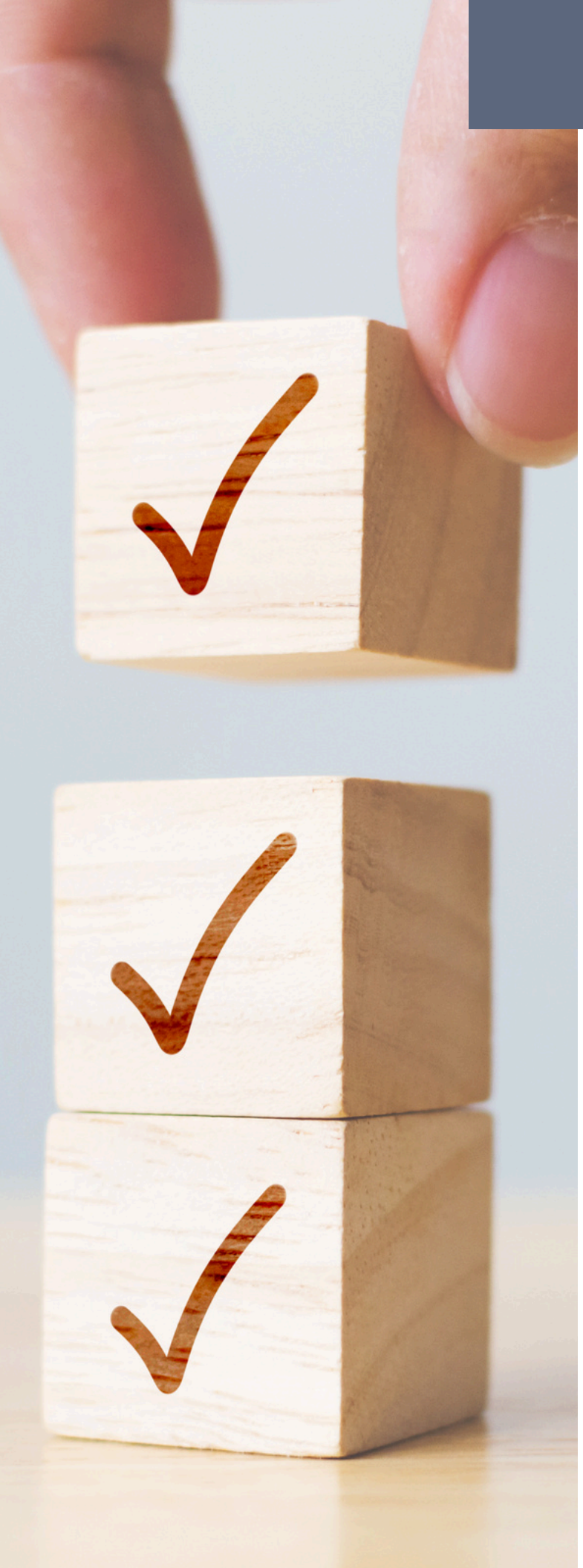
Fraud attempts are rising, faster payments carry faster risks, and checks remain the #1 target. The common thread: **every organization is vulnerable** — but not every organization is prepared.

Here are three quick self-checks you can put into practice right now:

- **Reconcile daily:** Are you reviewing accounts every day to spot anomalies quickly?
- **Dual approvals:** Do you require two sets of eyes on every ACH or wire transfer?
- **User access reviews:** When was the last time you checked who has authority in your online banking system?

If you answered “no” or “not sure” to any of these, that’s the best place to start. **Simple controls, consistently applied, remain the most effective defense against fraud.**

And if you aren’t sure where to go from here - let’s talk. Schedule a free introductory call on my website at www.limogeconsulting.com.



Future-Proofing Treasury Isn't About Prediction, It's About Resilience

If there's one lesson that comes through in this first edition of The Risk Report, it's this: **fraud isn't going away — it's evolving.** And while no organization can predict the next scheme, every organization can prepare.

Future-proofing your treasury operations isn't about seeing around corners; it's about **building resilience into the foundation.** Daily reconciliations, dual approvals, vendor verification calls — these aren't flashy solutions, but they're the safeguards that keep your mission intact when uncertainty strikes.

Resilience comes from **clarity, discipline, and the right partners in your corner.** That's how you protect cash flow today — and how you ensure your organization is **ready for tomorrow.**

To your continued resilience,

Becky Limoge
Founder, LIMOGE | Consulting

Stay Covered. Stay Prepared.

Fraud, risk, and financial complexity don't have to leave your organization exposed. At Limoge Consulting, I provide independent, bank-agnostic guidance to help you strengthen cash flow, reduce risk, and build resilience for the future.

Visit www.limogeconsulting.com to learn more — and let's start the conversation about how I can support your goals.