LIMOGE | Consulting

THE RISK REPORT 2026

Navigating Risk in an Era of Intelligent Fraud

limogeconsulting.com

Welcome to the second edition of *The Risk Report*

Last year, we focused on a simple idea: fraud isn't a matter of *if*, but *when*.

That hasn't changed—but the way fraud is evolving has. In 2026, fraud is more intelligent, more convincing, and harder to detect. Advances in AI, faster payments, and gaps between policy and practice are creating new vulnerabilities.

Across organizations, one pattern is clear: there isn't just a rise in fraud attempts—it's a growing disconnect between the controls in place and how they're actually used day to day. That gap is where risk lives.

Inside, you'll find:

- Key **shifts in today's fraud landscape**, including AI-driven schemes
- The **growing tension** between speed and control
- Practical ways to strengthen controls so they **work in practice, not just on paper**

The goal remains the same: clear, independent insights you can put to work right away. Because resilience isn't built through policy alone—it's built through consistent execution.

I'm glad you're here.
Becky

CONTENTS

Feature Article

The New Face of Fraud:
Harder to Spot, and Easier to Believe

The Risk Radar

What's Changing Right Now

Where Organizations Are Most Exposed

Efficiency Spotlight

From Policies to Practice: Making Controls Actually Work

Daily Visibility: Your Simplest Fraud Defense

Case in Point

Case in Point: Case in Point: When "Routine" Led to a $25 Million Loss

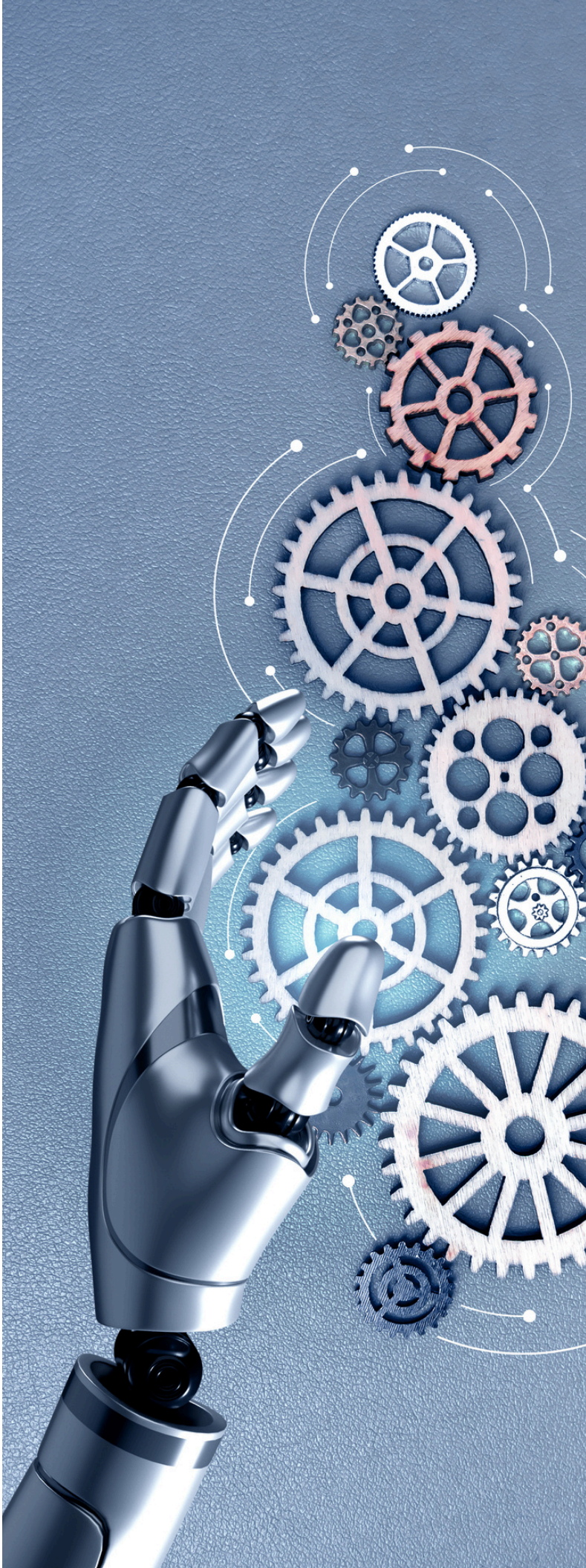
Case in Point: A Simple Email, a Changed Account, and a Six-Figure Loss

Tools & Resources

A Simple Check on Your Current Risk Exposure

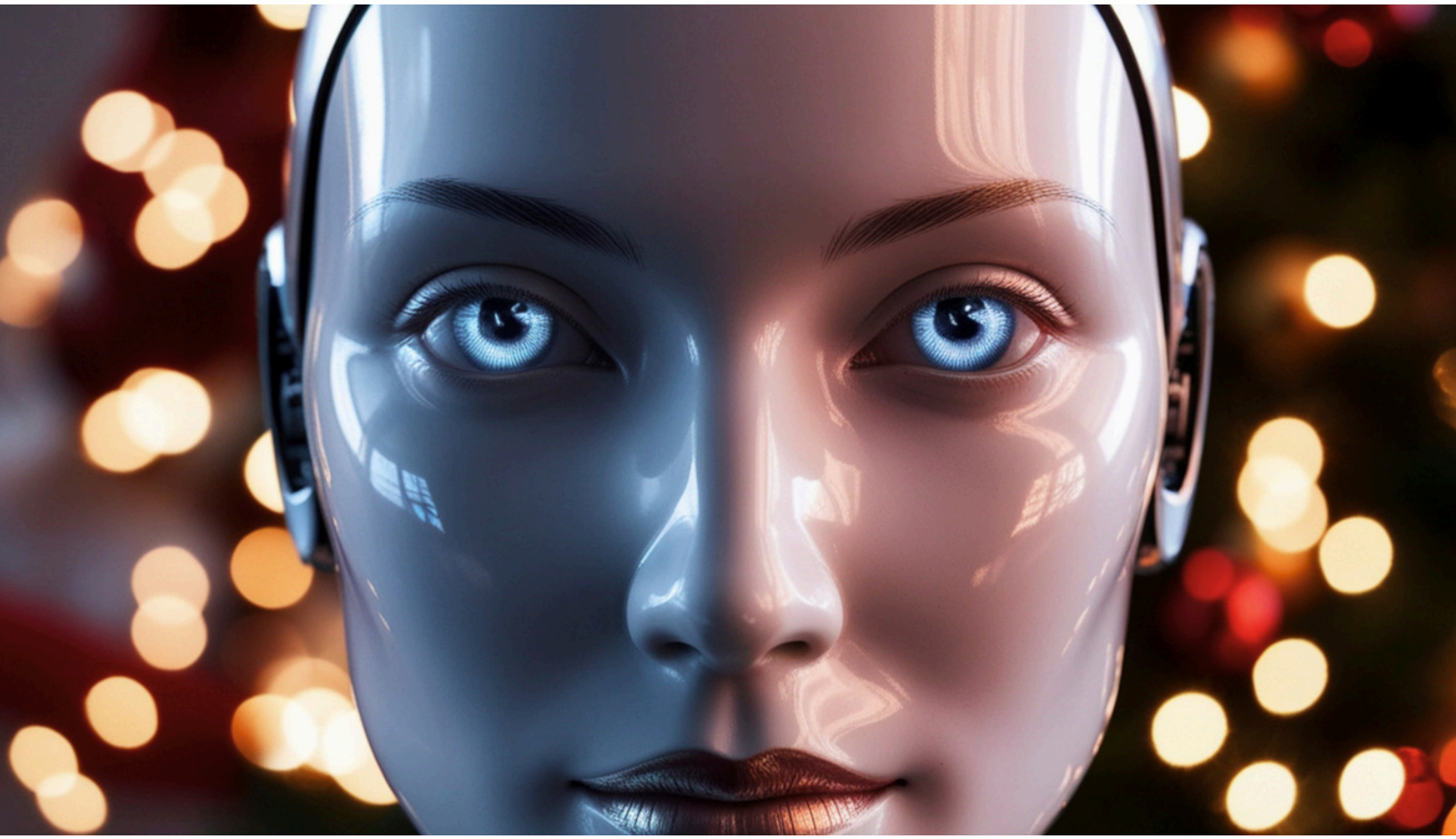
Closing Insight

Resilience is Built in the Everyday



Feature Article

The New Face of Fraud: Harder to Spot, and Easier to Believe



Fraud isn't just increasing — it's evolving.

For years, financial fraud followed familiar patterns: suspicious emails, obvious red flags, and errors that trained teams could learn to catch. But that's no longer the case. Today's fraud is more polished, more targeted, and far more convincing.

Advances in artificial intelligence are accelerating that shift. Fraudsters now have access to tools that can generate highly realistic emails, replicate writing styles, and even mimic voices. Messages that once would have raised immediate concern now appear routine — blending seamlessly into everyday business communication.

The result is a fundamental change in how fraud shows up inside organizations. There are fewer obvious warning signs, and a greater reliance on systems and processes that were built for a different kind of risk.

Where Strong Teams Still Win - and Where They Need Support

People are still one of the most important lines of defense against fraud. (Continued next page)

Experienced teams notice when something feels off. They understand vendor relationships, recognize patterns, and often catch issues before systems do. That human awareness is valuable—and it's not going away.

But the environment around them has changed.

Today's fraud is designed to look legitimate. Requests are well-written, contextually accurate, and timed to feel routine. In many cases, there's nothing obviously "wrong" with what's being asked.

That's where even strong teams can be put in a difficult position. Without clear processes, consistent expectations, and reinforcement from leadership, individuals are left to make judgment calls in moments that may feel urgent or routine. And that's exactly where fraud is most likely to succeed.

The organizations that navigate this well don't rely on instinct alone—**they support their teams with structure.**

They create environments where:

- Verification is standard, not optional
- Slowing down to confirm details is encouraged, not questioned
- Processes are followed consistently, even when things feel familiar

Strong teams are still a critical defense. But in today's environment, their effectiveness depends on the systems and leadership around them.

Where Controls Begin to Break Down

Most organizations don't lack controls. They have policies in place: dual approvals, vendor verification procedures, defined workflows.

But in practice, those controls don't always hold. Under pressure to move quickly, steps get skipped. Verification processes become informal.

Teams rely on familiarity — assuming a request is legitimate because it looks and feels right.
This is where modern fraud succeeds.

It doesn't require a complete breakdown of controls. It only requires a moment of inconsistency — a missed callback, a rushed approval, or a decision based on assumption instead of verification.

The gap between what exists on paper and what happens day to day is where risk lives.
(Continued next page)

"The shift is this: from trying to detect what looks wrong to ***verifying what appears right.***"

- Becky Limoge

A Shift in Mindset
Fraud today is designed to look legitimate. That means the question is no longer, “Does this look suspicious?”

It’s: “Has this been properly verified?”

That shift may seem small, but it’s critical.

Because the biggest risk in today’s environment isn’t just faster payments or more sophisticated tools. It’s the growing gap between what we think we would catch — and what we actually do.

The organizations that navigate this shift successfully won’t be the ones with the most complex systems. They’ll be the ones with clear processes, consistent execution, and leadership that reinforces the right behaviors over time.

Because in the new face of fraud, believability is the advantage — **and discipline is the defense.**

Risk Radar

What’s Changing Right Now

Fraud isn’t just evolving—it’s showing up differently inside organizations. Here are a few patterns emerging across finance teams:

Fewer Obvious Red Flags
Fraudulent requests are increasingly well-written, well-timed, and contextually accurate. The absence of errors is no longer a sign of legitimacy.

More Pressure to Move Quickly
Teams are being asked to process payments faster—whether due to real-time payment capabilities or internal expectations. That urgency is where mistakes happen.

Breakdowns at Routine Moments
Fraud is slipping through during everyday processes—vendor updates, payment changes, and familiar requests—where teams feel comfortable and less likely to pause.

Quick Takeaway:
Fraud isn’t getting easier to detect—**it’s getting easier to overlook.**

Risk Radar

Where Organizations Are Most Exposed

Fraud doesn't typically break through at the most complex points—it shows up in everyday processes where controls are assumed rather than confirmed.

Pay close attention to these areas:

Vendor Payment Changes

Requests to update banking details remain one of the most common entry points for fraud—especially when verification steps are skipped.

User Access and Permissions

Access often expands over time without review. Excess or outdated permissions create opportunities for both internal and external risk.

Approval Workflows Under Pressure

Dual controls can break down when teams are busy or processes feel routine, allowing transactions to move forward without proper oversight.

Fraud doesn't need a system failure. Just a moment where the process isn't followed.

Quick Takeaway: Risk tends to concentrate where processes feel familiar—those are the moments that require the most discipline.

Efficiency Spotlight

From Policy to Practice: Making Controls Actually Work

Most organizations don't need more controls—they need their existing ones to work consistently.

Policies like dual approvals, vendor verification, and user access reviews are often in place. But in day-to-day operations, those controls can break down under pressure, urgency, or routine. Small gaps in execution are where risk enters.

The most effective way to strengthen your defenses isn't by adding complexity—it's by reinforcing how your current processes are used.

Focus on these three areas:

- Standardize verification for vendor changes
- Confirm all payment or banking updates through a **known, independent contact**—not email alone.
- Reinforce dual controls **without exception**
- Ensure approvals are consistently followed, with no shortcuts or **single points of control**
- Review access with fresh eyes
- Regularly validate user permissions and remove access that no longer aligns with current roles.

If money is moving, ***verification isn't optional*** - even when everything looks right.

Efficiency Spotlight

Daily Visibility: Your Simplest Fraud Defense

One of the most effective ways to reduce fraud risk isn't new technology—it's visibility.

When transactions go unreviewed for days or weeks, small issues can quickly become large losses. The longer something goes unnoticed, the harder it is to recover funds and understand what went wrong.

Consistent, frequent review creates a much smaller window for fraud to succeed.

Daily visibility into cash activity allows teams to:

- Catch unusual transactions early
- Identify errors before they compound
- Maintain a clear, real-time understanding of cash flow

This doesn't require a complex process—but it does require consistency. Even a quick daily review of key accounts, exceptions, and alerts can significantly reduce exposure.

Make It Easier to Stay Consistent

Many banks and treasury platforms offer tools that support daily visibility without adding manual work.

Consider:

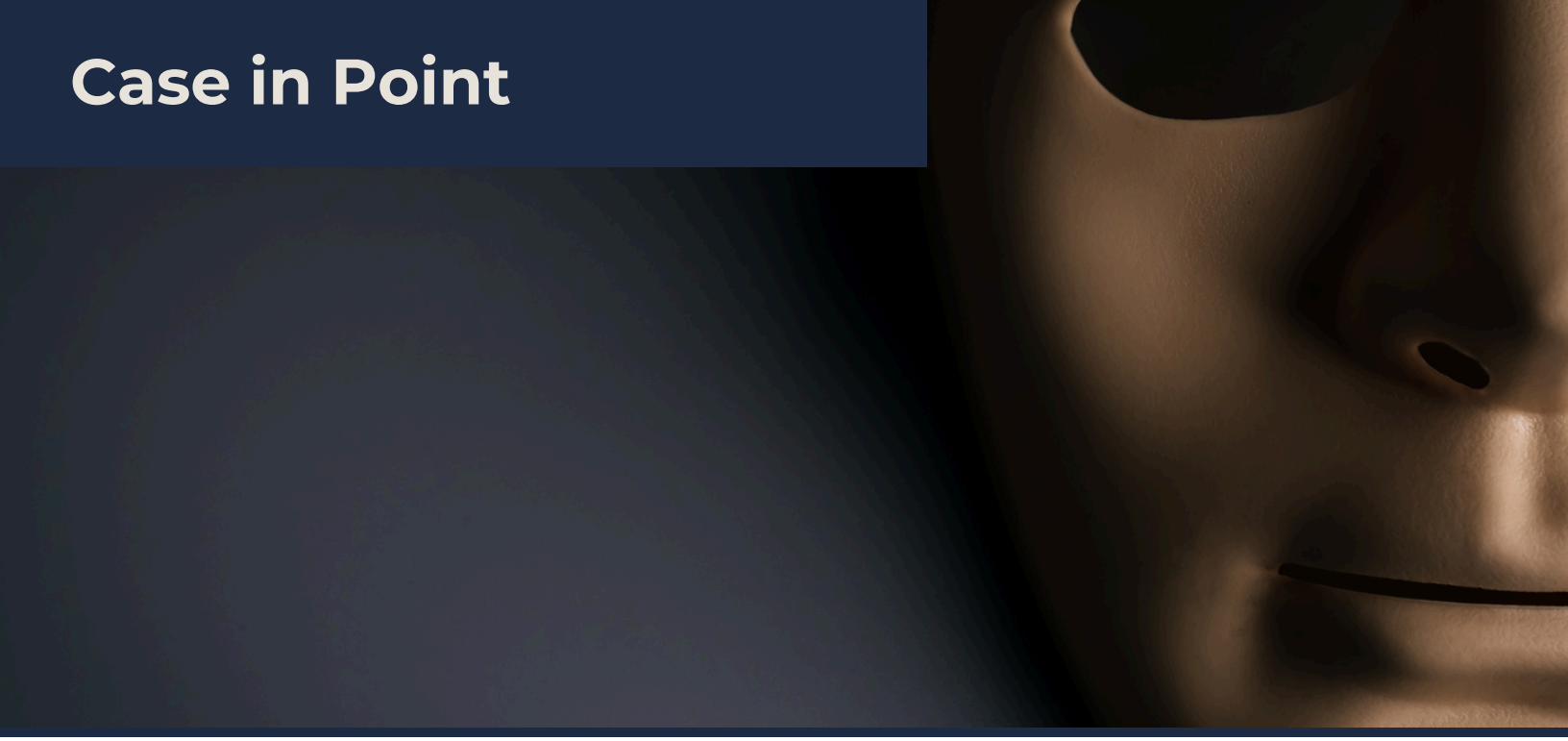
- Automated account alerts for transactions over a set dollar threshold
- Daily balance and activity notifications sent to key team members
- Exception-based reporting to highlight unusual or high-risk items

These tools don't replace review—but they make it easier to focus your attention where it matters most.

Quick Tip:

Review your primary operating account daily - and use alerts to stay ahead between reviews.

Case in Point



Case in Point: When “Routine” Led to a $25 Million Loss

In 2024, a multinational company lost more than $25 million after an employee was deceived by what appeared to be a legitimate internal request.

The employee received a video call from individuals who looked and sounded like senior executives within the organization. The request—to initiate a series of transfers—appeared routine and aligned with ongoing business activity. Trusting the authenticity of the interaction, the employee processed multiple payments before the fraud was discovered.

The call was later identified as a deepfake—using AI-generated video and voice to convincingly impersonate company leadership. By the time the fraud was detected, the funds were largely unrecoverable.

What broke down:

- The request appeared familiar and aligned with normal operations
- The interaction felt legitimate due to realistic video and voice
- Standard verification steps were bypassed in a moment that seemed routine

What changed:

- The organization reinforced independent verification for all payment requests—regardless of source
- Additional controls were implemented around high-value transactions
- Teams were trained to recognize that even highly realistic interactions may require verification

Key takeaway:
Even when a request looks and feels legitimate, it must be independently verified. **No exceptions.**

Case in Point: A Simple Email, a Changed Account, and a Six-Figure Loss

A U.S.-based organization received what appeared to be a routine email from a long-standing vendor requesting an update to their payment information.

The request was well-written, referenced recent invoices, and included updated ACH instructions. Nothing about it seemed unusual. The finance team updated the vendor's banking details and processed several payments over the following weeks.

It wasn't until the real vendor followed up on overdue invoices that the issue surfaced. By then, more than **$400,000 had been sent to a fraudulent account.**

What broke down:

- The request appeared consistent with normal vendor communication
- Banking changes were processed without independent verification
- Multiple payments were sent before the discrepancy was identified

What changed:

- All vendor payment changes now require call-back verification using a known contact
- Dual approvals were added for any updates to vendor banking information
- Teams were trained to treat payment changes as high-risk, even when they appear routine

Key takeaway:
Don't rely on familiarity—always verify vendor payment changes using a known, independent contact before processing.

Tools & Resources

A Simple Check on Your Current Risk Exposure

There's no doubt that fraud is evolving—but the most effective defenses remain practical and within your control. The question isn't whether you have safeguards in place. It's whether they're working consistently.

Use the quick checks below to assess where you may have gaps:

Verification

- Do all vendor payment changes require confirmation through a known, independent contact?
- Are urgent or high-value requests handled differently—or do they follow the same process every time?

Approvals

- Are dual approvals required and consistently enforced for ACH, wire, and vendor changes?
- Are there any situations where one person can initiate and approve a transaction?

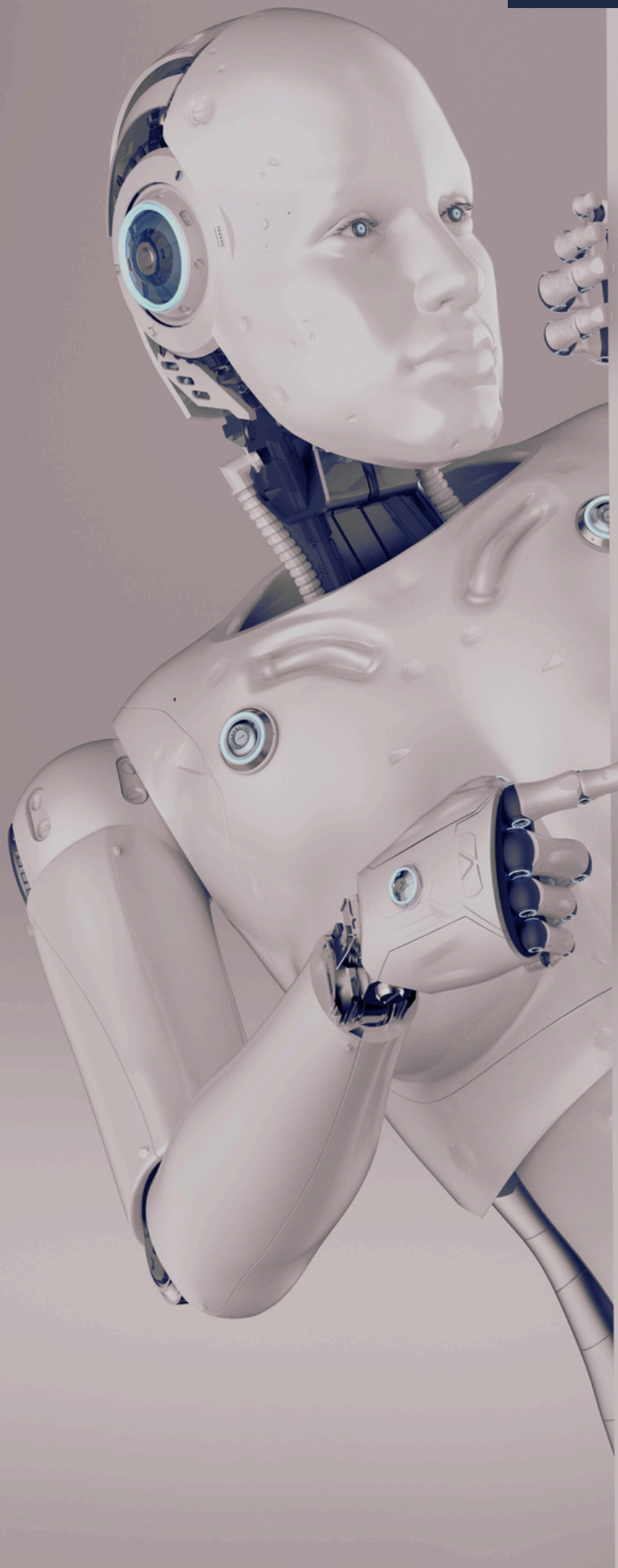
Visibility

- Are key accounts reviewed daily for unusual or unexpected activity?
- Are alerts in place for large or out-of-pattern transactions?

Access

- When was the last time user permissions were reviewed?
- Does access align with current roles and responsibilities?

Quick Start: If you're unsure where to begin, start with one area—verification is often the most immediate opportunity to reduce risk.



Resilience is Built in the Everyday

If there's one theme that carries through this year's report, it's this: fraud isn't just increasing—it's becoming more believable.

But that doesn't mean organizations are at a disadvantage.

Even as technology evolves, the **fundamentals still hold. Strong teams, clear processes, and consistent execution remain the most effective defenses.** In fact, in an environment where fraud is designed to look real, those human strengths matter more—not less.

Strong controls don't fail because they don't exist. **They fail when they aren't followed**—especially in moments that feel routine, familiar, or urgent.

That's where resilience is built.

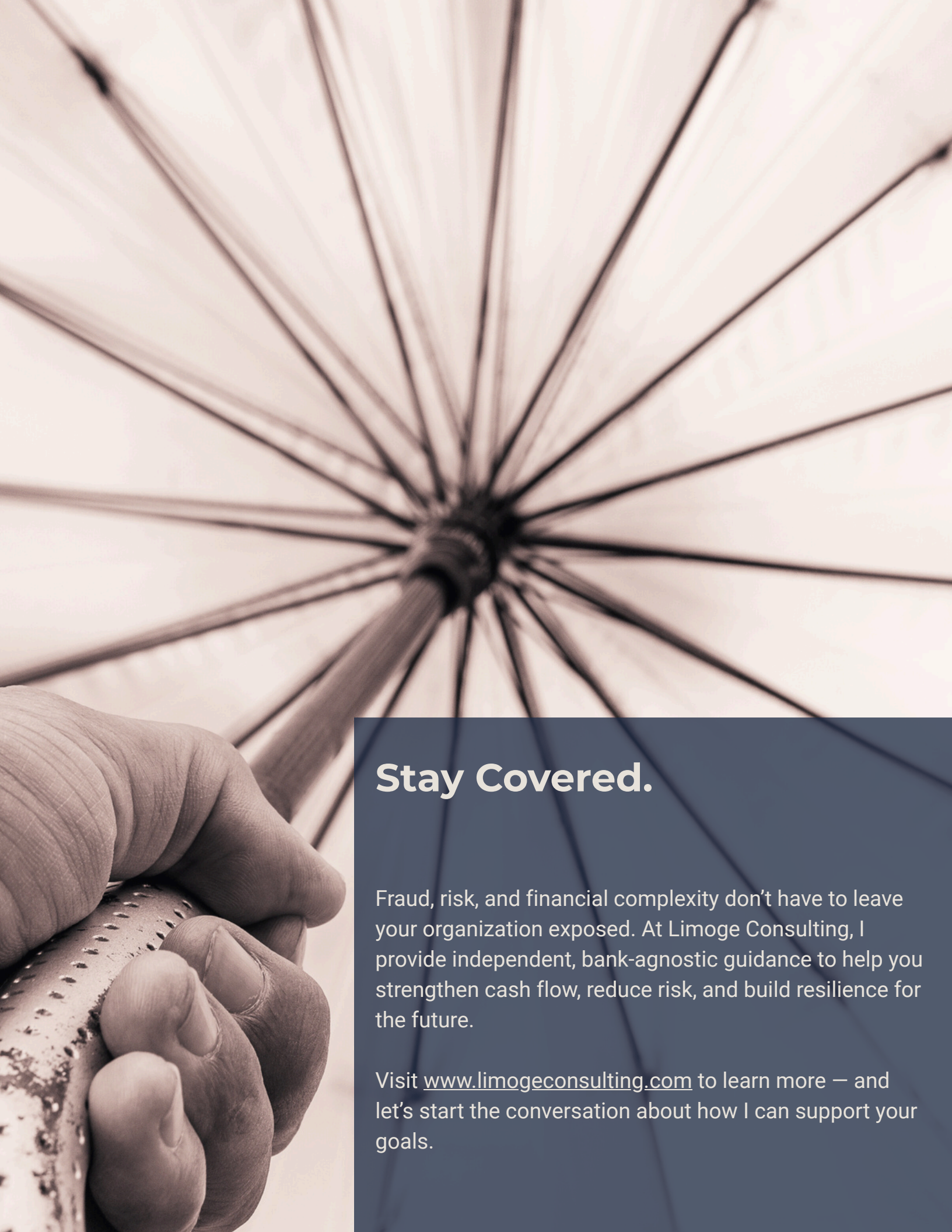
Not in response to a major incident, but in the everyday decisions to verify, to pause when something needs a second look, and to follow processes even when everything appears legitimate.

We don't need to outpace technology—we need to stay grounded in the practices that work.

Because in a world of increasingly intelligent fraud, **discipline, clarity, and well-supported teams remain the strongest line of defense.**

Stay disciplined. Stay consistent.

Becky Limoge
Founder, LIMOGE | Consulting



Stay Covered.

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.