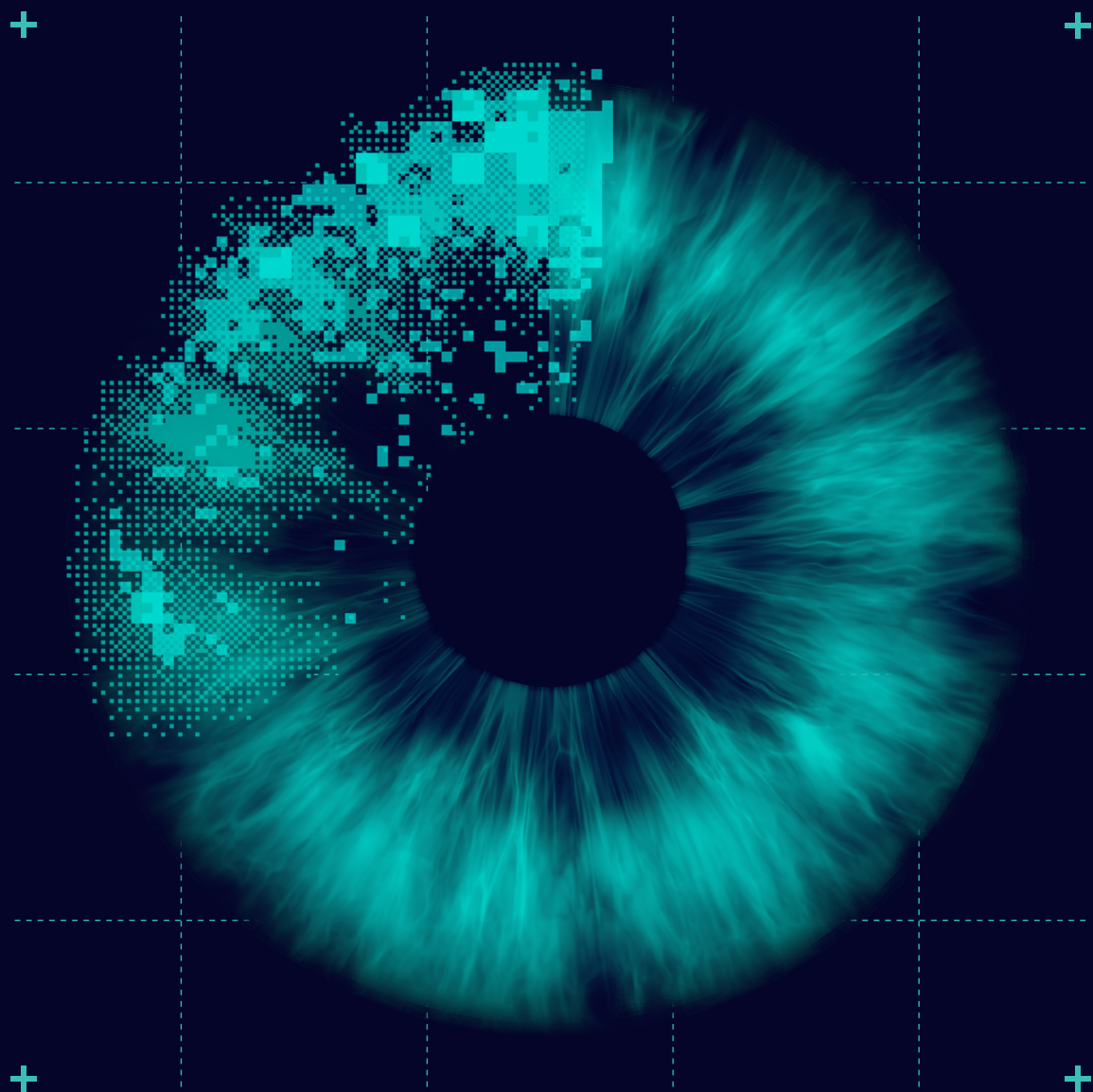




The Specialization Trap

The Hidden Cost of
Fighting Fraud in Isolation

Insights from SEON's 2026 Fraud & AML Leaders Survey



Table of Contents

Executive Summary & Methodology	3
Key Findings	6
Section 1	
The Specialists	7
Section 2	
The Blind Spot	10
Section 3	
The Invisible Cost	14
Section 4	
Fixing the Foundation Before Automating	17
Get the Full Picture	19

Executive Summary & Methodology



Executive Summary

Financial sector companies run some of the most specialized fraud and AML divisions in our survey. Across fintech and payments, risk teams bring intense focus and exceptional funding. AI investment outpaces other industries by 10 to 22 percentage points. Vendor ecosystems keep expanding and confidence remains high.

But that specialization has produced a deep organizational divide. Fewer than 5% of financial sector fraud and AML leaders sit within digital or eCommerce operations, compared to 30% in other industries. Fraud professionals outside financial services work alongside the business teams they serve about six times more often than their financial sector peers. The gap is the largest divergence in SEON's second annual Fraud & AML Leaders Report. Meanwhile, strategic investment in AI is 23 percentage points below the rate in other industries.

The divide matters because fintech and financial services are placing the biggest bet on AI. And AI performs only as well as the data it can access. When fraud and AML teams operate in isolation, the AI inherits that exact blind spot. We call it the specialization trap. Critical signals slip through because no one is positioned to see them. The fix isn't diluting expertise. It's wider, real-time visibility.

Methodology

As part of SEON's AI Reality Check: 2026 Fraud & AML Leaders Report, this research draws on responses from 347 global fraud and AML leaders across fintech (124), payments (26) and financial services (197). It examines a pattern unique to the financial sector: decades of investment in specialized fraud teams created an organizational blind spot, and that divide now limits the return on the sector's most ambitious AI investments. The insights apply across all three verticals and reflect how leaders are making decisions today.

Respondents hold senior decision-making roles, including Head of Fraud, VP of Risk, Chief Compliance Officer and equivalent C-suite titles. All data cited in this report comes from survey responses unless otherwise noted.

Key Findings

1

The Financial Sector Has the Most Specialized Fraud Operations

Fraud management dominates as a function across all three financial verticals. More than half of payments (58%) and financial services (52%) leaders sit in dedicated fraud roles, along with 43% of fintech leaders. Only 33% of leaders in other industries hold equivalent positions. Factoring in risk management, the financial sector shows the highest concentration of dedicated expertise in the survey.

Aggressive technology spending reinforces that specialization. Fintech leads with 67% of budgets allocated to AI and machine learning, followed closely by payments at 65% and financial services at 55%. Other industries sit at 44%. Vendor expansion grows even faster — 88 to 93% of leaders plan to add a new vendor in 2026.

2

Why Critical Fraud Signals Fall Between Teams

The organizational divide wasn't created by any individual fraud leader. It's the predictable outcome of decades spent building dedicated fraud functions separate from AML and digital operations. But the consequences are measurable.

Many of the most important fraud signals — unusual login behavior, suspicious transaction patterns — don't originate within fraud systems alone. They sit at the intersection of fraud data and customer journey data. And that intersection is exactly where no team is looking. If no team is looking, no tool will catch it.

3

The Biggest AI Bet, Deployed From the Narrowest Vantage Point

The financial sector's commitment to AI is strategic, sustained and unmatched. But spending more doesn't mean deploying broadly. Transaction monitoring accounts for 46% of AI usage in payments and 35% in financial services. That's the exact layer where the blind spot runs deepest.

AI can only work with the data it's trained on. Patterns that emerge when fraud and business data combine, such as shifting customer behavior and pre-fraud engagement signals, never reach the model. The financial sector spends more on AI than any other industry, yet most of the investment is concentrated around the point of transaction.

Section 1

The Specialists



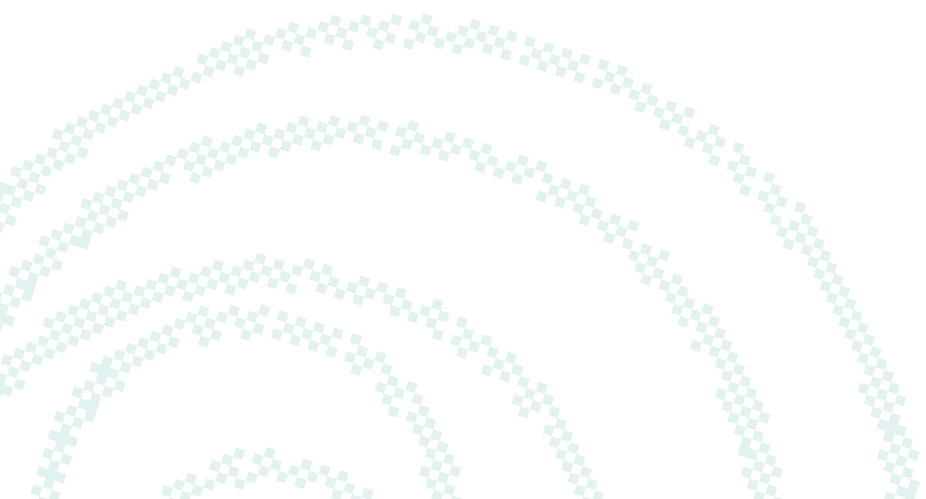
The Best-Funded Fraud Teams

Decades of regulatory pressure, surging transaction volumes and the steep cost of financial crime forced the financial sector to build specialized fraud defenses — a deliberate evolution fueled by sustained investment in dedicated teams and risk infrastructure.

Today, 58% of payments leaders and 52% of financial services leaders hold dedicated fraud management roles, well above the 33% average in other industries. Add risk management into the mix and the financial sector pulls further ahead, outpacing every other group in the survey by double digits. These are organizations built around fraud and risk.

The investment goes well beyond headcount. All three financial verticals allocate AI and machine learning budgets that dwarf other industries. Fintech leads the entire survey at 67%, 23 percentage points above the baseline, with payments close behind at 65%. Even financial services, traditionally the most conservative of the three, invests at 55%.

Vendor expansion follows the same trajectory. Between 88% and 93% of leaders across all three verticals plan to add a fraud or AML vendor in 2026. Fintech is in build mode, with 93% adding and only 7% removing. Payments and financial services curate more actively, planning 15–19% removals alongside their additions. The question is whether those dollars are landing in the right place.





The Financial Sector’s Investment Advantage

Budget allocation and tech stack priorities by vertical



→ Across every investment metric, all three financial verticals outpace the rest of the survey.

Section 2

The Blind Spot

Why Critical Fraud Signals Fall Between Teams

Where a fraud leader sits within an organization tells you how connected their operation is to the broader business. The financial sector built dedicated teams, handed them their own tools and measured them against their own metrics. Fraud operations evolved into a self-contained silo, separated from the digital business they were built to protect.

The isolation looks different across the three verticals, but the result is the same. Payments face the most extreme version: zero fraud leaders sit in digital operations. System complexity ranks as their top integration challenge at 73% (22 percentage points above other industries), compounded by regulatory constraints. Financial services show a subtler divide. Integration levels are lower (40% fully integrated versus 46% elsewhere), and 7% still run entirely separate fraud and AML systems. Fintech comes closest to bridging the gap. 58% report fully integrated workflows, the highest of any vertical, but only 5% of fintech fraud leaders sit in digital operations.

That gap between teams is a blind spot. The fraud team tracks transaction patterns and risk scores. The digital team monitors customer journeys and engagement metrics. Risk signals that fall between those two worlds have no owner. A customer whose behavior shifts after onboarding is exactly the signal that slips through.

The financial sector faces uniquely complex threats that deliberately cross the boundary between fraud and business operations. Chargebacks dominate fintech and payments. Account takeover is the primary threat in financial services. Alternative payments abuse specifically plagues payments. Every vertical faces a different mix, but every threat exploits the same gap.



Integration Barriers by Vertical

What are the biggest challenges in integrating fraud and AML workflows?



→ The financial sector concentrates heavily on fraud management and is nearly absent from digital operations, a gap of 25 to 30 percentage points consistent across all three verticals.



The Organizational Disconnect

How challenging is it to obtain a unified view of data and insights across your fraud and AML systems?



→ The barriers vary by vertical, but they point to the same problem: fraud infrastructure that was never designed to connect to the broader business.

Section 3

The Invisible Cost



You Can't Solve What You Can't See

In 2026 budgets, the financial sector prioritizes AI and machine learning over headcount. That's the exact inverse of industries like betting and gaming, where headcount leads AI by 13 percentage points. Fintech allocates 67% to AI versus 36% to headcount. Payments sit at 65% versus 30%, and financial services at 55% versus 41%.

But investment breadth doesn't equal deployment breadth. Transaction monitoring accounts for 46% of AI usage in payments and 35% in financial services. The sector spending the most on AI is concentrating most of it around the point of transaction.

By traditional metrics, the approach works. Extreme false positive rates appear less often here than in other industries. Data fragmentation runs lower, and workflow integration in fintech tops the survey. The financial sector performs well by every measure it tracks.

When fraud and risk teams operate as standalone functions, they only see what their own data shows. Models trained exclusively on fraud-side data catch known patterns with increasing precision. But customer behavior signals, onboarding anomalies and engagement shifts that sit within digital operations may never reach those models. The real cost hides in signals that never surface, fraud patterns that evolve before transaction monitoring catches up.

Ambition outpaces the infrastructure. Financial services leaders hold the highest expectations for AI, with 46% anticipating it will handle most tasks with human oversight. Yet they also report the lowest workflow integration rate at 40%. In payments, 62% of leaders say they are "very confident" in AI, but system complexity and regulatory hurdles stand in the way. The organizations that close the visibility gap first will see the returns on their AI investments. That means connecting fraud data to business data and embedding intelligence into digital operations.

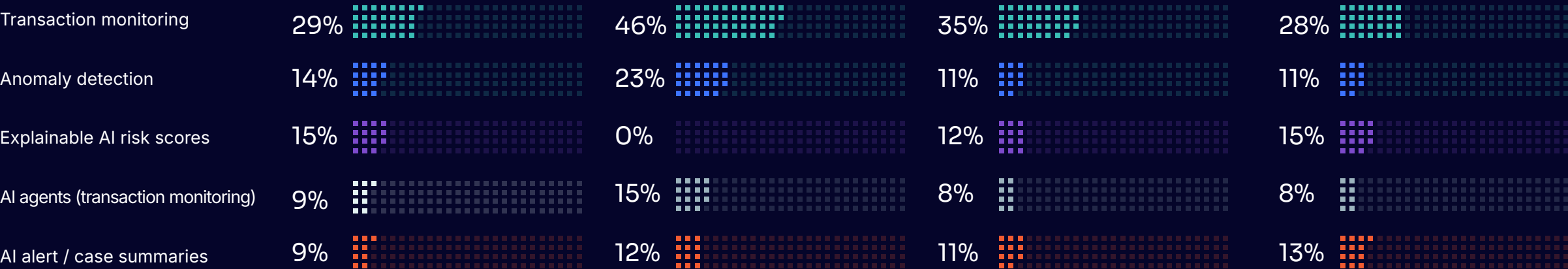


Where the AI Budget Goes and Where It Lands

Budget Allocation: AI/ML vs. Headcount



AI Tool Usage: Where Deployment Is Concentrated



→ The financial sector invests more in AI than any other industry group and concentrates most of it at the transaction layer.

Section 4

Fixing the Foundation Before Automating



The data in this report traces how the financial sector built specialized fraud operations and created an organizational divide between risk teams and business operations in the process. Now, the industry's largest AI investments are being deployed from behind that divide, automating existing constraints and scaling blind spots instead of fixing the foundation.

Closing the gap doesn't mean dismantling what has been built. The expertise and infrastructure of the past are genuine advantages, but they need to be connected. Bridging fraud intelligence with broader business operations gives AI access to the complete picture, allowing organizations to unlock the returns they expect from their automation investments. Those that don't will keep spending more to see less.

Before rushing to scale, every financial sector fraud leader should ask three questions:

→ **Does our fraud team see the business, or just the fraud?**

The 25 percentage point disconnect from digital operations reflects decades of deliberate specialization, not a staffing gap. Fraud teams were built as self-contained functions with their own metrics and tools, but that specialization turned into isolation. Connecting fraud intelligence to business operations like customer journeys and conversion patterns lets the team see beyond the transaction without diluting specialized knowledge.

→ **Is our AI seeing the full picture?**

A model trained exclusively on fraud-side data will only automate fraud-side insights. Anomalies that span the organizational divide stay out of reach when fraud data is disconnected from business data. Until that connection exists, AI will only automate what teams already know.

→ **Can our fraud function scale as fast as our business?**

All three financial verticals are expanding their vendor ecosystems. Every new tool adds another disconnected data source unless the organization consolidates around platforms that connect fraud, compliance and business data. Those that keep adding disjointed point solutions will scale their existing complexity. The technical infrastructure is already there, but the fix is organizational. The organizations that make it first will see the returns on their AI investments.

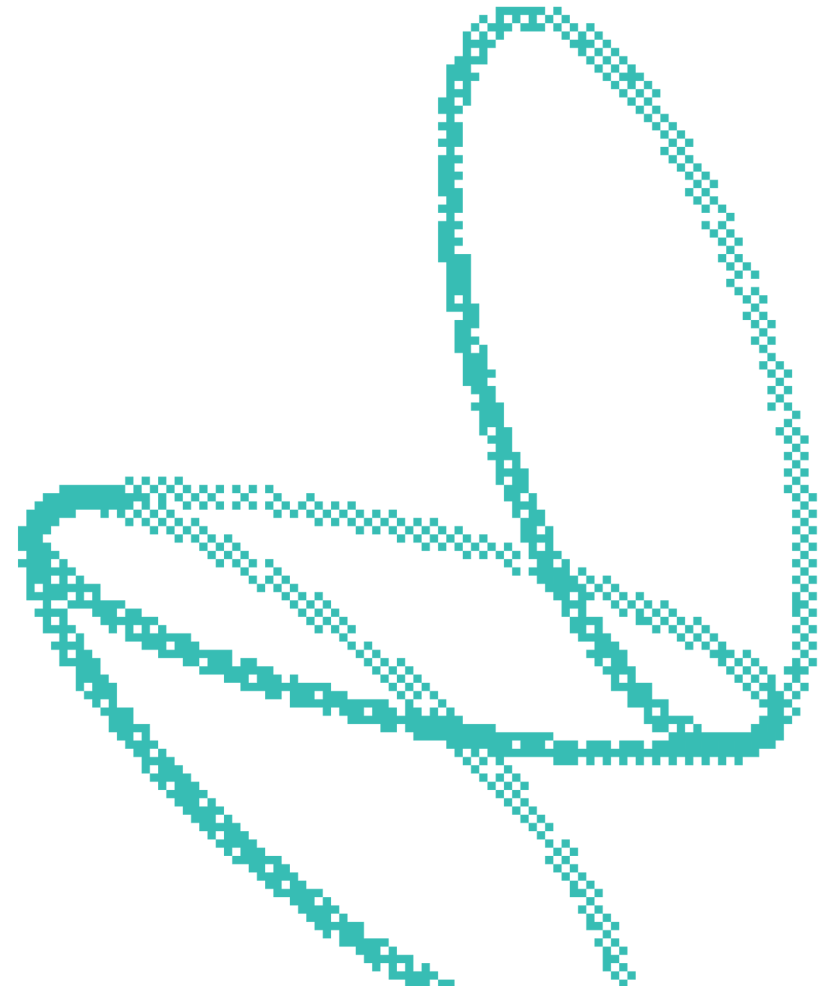
Get the Full Picture

The report covers specific findings from 347 fraud and AML leaders worldwide, spanning fintech, payments and financial services. For the complete analysis, download the full report. It includes AI adoption benchmarks, vendor ecosystem trends and investment forecasts alongside the full dataset from 1,010 respondents across all verticals.

—→ [Download the AI Reality Check: 2026 Fraud & AML Leaders Report](#)

—→ [Talk to a SEON Expert](#)

Based on SEON's 2026 Fraud & AML Leaders Survey. 1,010 respondents across betting and gaming, fintech, payments and retail. Research conducted by Jane Singh & Katy Chrisler.





The Command Center for Fraud Prevention & AML Compliance

This report is based on insights from a survey commissioned by SEON, gathering perspectives from fraud prevention and compliance professionals across industries. Research and analysis were conducted by Jane Singh & Katy Chrisler.

[Read more at seon.io](#)

[The Total Opportunity Cost of Fraud is Bigger Than You Think](#)

[Read Article](#) —>

[Leveraging AI & Innovative Tech to Combat Emerging Complex Fraud Schemes](#)

[Read Article](#) —>

[Traditional Fraud Prevention Measures Aren't Enough](#)

[Read Article](#) —>