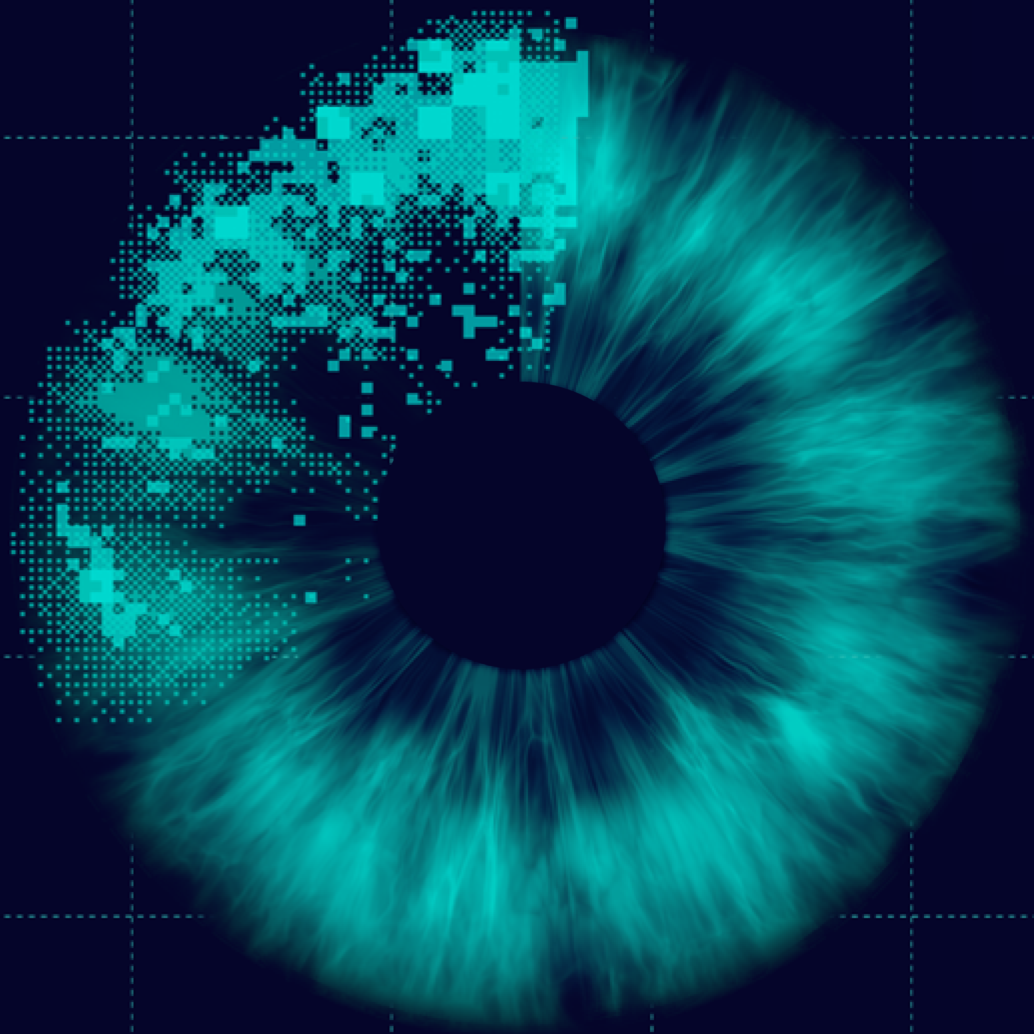


AI Reality Check

2026 Fraud & AML Leaders Report

SEON.IO

Table of Contents

A Note From Our CEO

Fraud and financial crime were supposed to become more manageable as AI matured and automation moved into production. Instead, 2026 is the year many leaders are confronting a more complicated reality: AI is working in production, yet the biggest constraints are increasingly the systems, data and operating model around it.

The industry has moved beyond experimentation. Today, AI is successfully embedded in day-to-day workflows, delivering tangible efficiency gains in well-defined areas. We see this clearly in use cases like AML screening, where AI helps reduce false positives, and in automated SAR narrative generation, which cuts down on hours of manual report writing. These are important, valuable steps forward.

Yet in high-growth, high-risk environments, headcount and budgets are not shrinking in step with automation, and operational pressure continues to rise faster than efficiency gains. This is not a verdict on whether AI works, but a signal that real leverage comes from how quickly teams can integrate signals, operationalize controls and reach defensible decisions.

This is the core tension at the heart of **AI Reality Check: 2026 Fraud & AML Leaders Report**. Now in its second year, this report explores how AI has reshaped fraud and AML operations without reducing the overall workload. AI is no longer a project to adopt — it is an operating environment that reshapes every decision, from onboarding and payments to investigations and reporting. Leaders are asking vendors not just for models, but for transparency, control and auditability that stands up under real operational volume.

Many of these emerging agents, while powerful in their narrow focus, operate without a holistic understanding of the data and the complex relationships between different risk signals. They are being layered on top of the same fragmented systems that created the complexity in the first place, risking becoming just another silo.

What this research makes clear is that the bottleneck is no longer a question of whether AI works, but how it is architected. Most organizations report that their fraud and AML workflows are only partially integrated, and 80% indicate that obtaining a unified view of data and insights remains a significant challenge. Much of this stems from data living in siloed, disconnected systems. Even when a single tool introduces automation, those gains rarely translate into end-to-end process improvements – teams still depend on manual intervention to move information between platforms and reconcile decisions across tools. The most effective teams we see are not just deploying more models. They are building a foundational layer, a common protocol, that allows different AI tools and data sources to speak the same language. For agentic workflows to be truly successful, they cannot operate in a vacuum. They require a standardized, unified view of the risk context to make intelligent decisions.

With that foundation in place, teams can move from being reactive ticket resolvers to proactive risk architects, focusing their expertise on strategic threats, complex investigations and the critical oversight of these new automated systems. Leaders who manage this best unify fraud and AML signals, shorten the distance between a new threat and a new control and invest in the connective tissue between systems — because the value of AI is only as strong as the context it can access.

Our philosophy is straightforward: AI should enhance human effectiveness. Fraudsters are already weaponizing automation, synthetic identities and AI agents. The only sustainable response is a transparent, explainable and adaptive architecture where humans and machines learn together — shifting left toward earlier detection and transforming blackbox scores into decisions that can be explained, audited and defended. It means being precise about where different AI approaches add value: real-time monitoring demands deterministic systems, while modern AI transforms the layers around it, accelerating investigations, optimizing rules and explaining anomalies in language that teams can act on and leaders can defend to regulators.

The leaders who pull ahead will not be the ones with the most tools; they will be the ones with the clearest signals and the strongest alignment between people, process and technology. For fraud and AML leaders, 2026 is not just another cycle of upgrades. It is the moment to decide whether AI becomes another layer of complexity or the foundation of an intelligence-led discipline that keeps pace with growth, regulation and today's quick-moving adversaries.

Tamás Kádár

Tamás Kádár
Chief Executive Officer, SEON

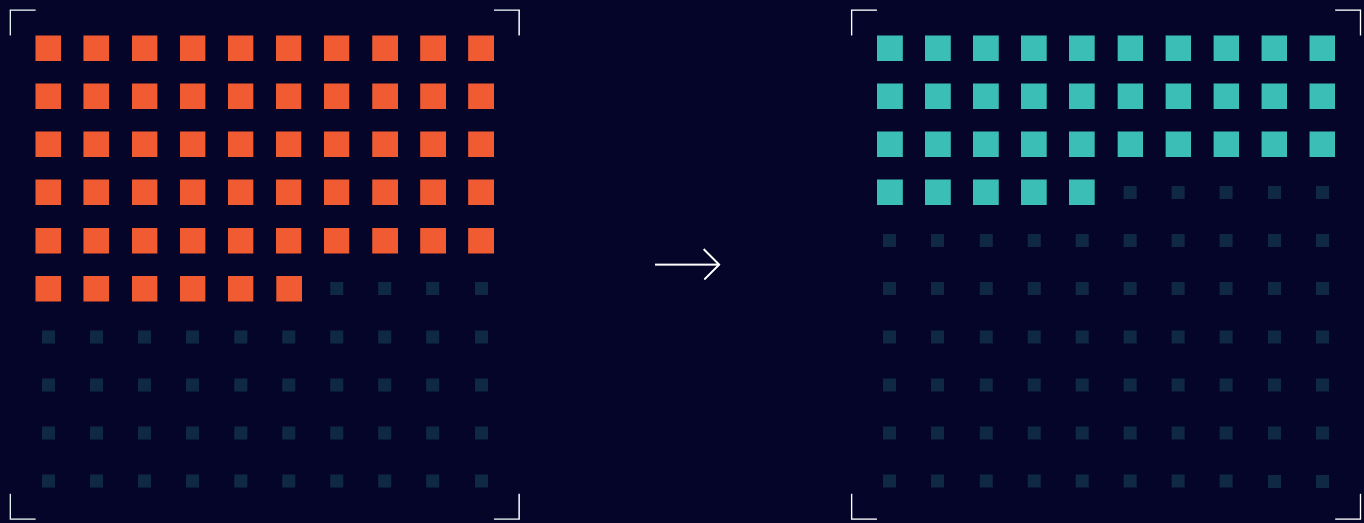
Executive Summary

AI Reality Check: 2026 Fraud & AML Leaders Report reveals an industry that has fully embraced AI and is discovering that the hard work is only just beginning. AI is real, embedded and widely trusted, but it has not materially reduced the scope of fraud and AML operations. In many cases, criminals' use of AI has stretched that scope faster than efficiency gains can keep up.

One signal stands out in the year-on-year data. Last year, 56% of leaders disagreed or strongly disagreed with the statement, "fraud losses are growing faster than our revenue;" this year, that figure has dropped to 35%, a shift that suggests many organizations now feel losses pressing closer to, or even outpacing, growth. As AI becomes a tool for both defenders and attackers, simply keeping up has become a larger, not smaller, task.

Year-on-Year Shift in Fraud Loss Pressure

Do you agree that fraud losses are growing faster than your revenue?



56% of leaders disagreed in 2024

35% of leaders disagreed in 2025

Key Takeaways:

1

AI is everywhere, but simplification isn't

- → AI is now baseline infrastructure, not a pilot. Ninety-eight percent of leaders report that their teams are already integrating AI into day-to-day workflows, with AI/ML for transaction monitoring being the most common and mature use case (30%).
- → Confidence is high, but pressure is higher. Ninety-five percent are confident that AI can reliably detect and prevent fraud, and 52% are very confident — yet most report an increase in volume, structural complexity and regulatory and operational scrutiny, rather than a decrease.

2

Investment keeps rising across budgets, headcount and tools

- → Budgets continue to grow. Eighty-three percent of organizations expect their fraud and AML budgets to increase in 2026, only slightly below last year's 86%, signaling that modernization is a strategic priority.
- → Hiring is accelerating, not shrinking. Ninety-four percent of leaders plan to add at least one full-time fraud/AML hire in 2026, up from 88% the prior year, with one-third planning 3-5 hires, another third planning 6-10 and 17% planning to add more than 10 roles.

3

Automation is redefining teams, not replacing them

- → AI agents are seen as copilots, not substitutes. Over 85% of leaders believe AI agents should support or augment analysts, while only 12% think they should eventually replace them.
- → Human roles are shifting up the value chain. As automation absorbs volume and routine triage, teams are reallocating time toward complex investigations, model oversight, regulatory reporting and cross-functional strategy.

4

Fragmentation is the new bottleneck

- → Integration is widespread on paper, brittle in practice. While 95% of organizations report at least some integration between fraud and AML workflows, only 47% run fully integrated platform workflows; the rest rely on partially connected systems that create friction and blind spots.
- → Unified visibility remains elusive. Eighty percent say it is at least somewhat challenging to obtain a unified view of data and insights across fraud and AML systems, and more than 40% describe it as extremely or very challenging, undermining both AI performance and operational efficiency.

5

Time-to-value compounds every other risk

- Go-lives still take months. Most organizations report that implementing a new fraud or AML solution takes multiple months after vendor selection. Specifically, 38% go live within one to three months, while another 24% require four months or more.
- Delays have real costs. When implementations overrun, leaders most often cite increased operational costs (521 respondents), prolonged exposure to fraud risks (475) and sustained manual workarounds reflected in higher operational load and technical effort as the top consequences, not simply IT inconvenience.

6

High-growth leaders look different

- Growth and integration move together. High-growth organizations (26–50% and 51%+ revenue) are more likely to be very confident in AI and almost twice as likely as slower-growing peers to report lower levels of difficulty achieving unified visibility, likely reflecting earlier and more sustained investment in integration.
- They treat integration as a strategy, not plumbing. Compared to slower growing peers, high-growth organizations are more likely to unify fraud and AML intelligence, and the data suggests they are also more inclined to reduce reliance on fragmented point solutions and prioritize shared data foundations.

7

The next frontier: governance, identity and skills

- Leaders are increasingly focusing on explainability, auditability and human accountability as AI becomes embedded in high-stakes risk decisions.
- Decentralized identity is on the radar. Eighty-five percent of respondents believe decentralized digital identity will become part of the future fraud and AML stack, even as timelines remain uncertain and regulatory clarity continues to evolve.
- Skills are evolving toward AI, data and collaboration. Fraud teams are prioritizing AI, machine learning and advanced data analytics, alongside cross-departmental collaboration and customer experience optimization, as the most critical future capabilities.

Together, these findings suggest that the winners in the next era of fraud and risk prevention will be the organizations that pair explainable automation with better data foundations, truly unified fraud/AML workflows and teams empowered to act as designers of intelligence, not just operators of tools. Leaders already see the cost of getting this wrong: more than half say that limitations in their data sources account for at least a quarter of their false positives, underscoring how gaps in coverage and quality erode both efficiency and customer experience.

Methodology & Respondent Profile

This report presents a global, leadership-level perspective on the evolution of fraud and AML in the era of AI. It focuses on what leaders are actually doing and measuring today so that investment decisions can rest on evidence rather than intuition.

Who We Surveyed

The findings are based on a quantitative third-party survey of 1,010 fraud, risk and compliance leaders working in digital-first organizations. All respondents hold director level or more senior roles, with direct responsibility for fraud prevention, AML compliance, risk management or adjacent decision-making, ensuring the insights reflect how strategy and operations actually meet in practice, not just theoretical opinions.

Respondents come from organizations across various sectors, including:

→ **Betting and gaming**

→ **Payments, fintech, financial services & online lending**

→ **Retail and eCommerce**

Regions, Verticals and Roles

The sample is intentionally global, with substantial representation from North America (NOAM); Europe, the Middle East and Africa (EMEA); Latin America (LATAM) and Asia Pacific (APAC), capturing a mix of both mature and fast-growing fraud environments and highlighting how regional nuances shape threats, regulation and technology choices.

Within each region, the survey targeted digital businesses at scale — organizations with meaningful online transaction volume, cross-border exposure or both. Across verticals, respondents share an everyday reality: they operate in environments where fraud, AML and customer experience are tightly coupled and where AI adoption is no longer optional.

How to Use This Report in Your Strategy

Use this report in three main ways:

→ **Pressure-test your roadmap**
Compare AI adoption, hiring plans, budget trajectory and stack modernization against more than a thousand peers.

→ **Clarify trade-offs**
See how leading teams balance automation with headcount, fraud loss with customer experience and innovation with regulatory scrutiny.

→ **Prioritize bottlenecks**
Identify whether your greatest constraint is data quality, fragmentation, time-to-value or skills and where integration will unlock outsized gains.

Most importantly, treat the findings as a way to reframe internal conversations. Whether you are making the case for a unified fraud/AML command center, accelerating AI adoption or investing in better data, the patterns in this report give you evidence to move beyond anecdotes — and to align executives, product, engineering and risk around a shared, intelligence-led strategy.

Section 1

2026 in Context

Why Fraud & AML Teams Matter Now

The organizations represented here are growth-oriented by design. Nearly 80% report revenue growth above 10% in the past 12 months, with 48% in the 11–25% range, 36% in the 26–50% range and 4% growing at 51%+. In that environment, fraud and AML teams sit directly between growth ambitions and risk exposure.

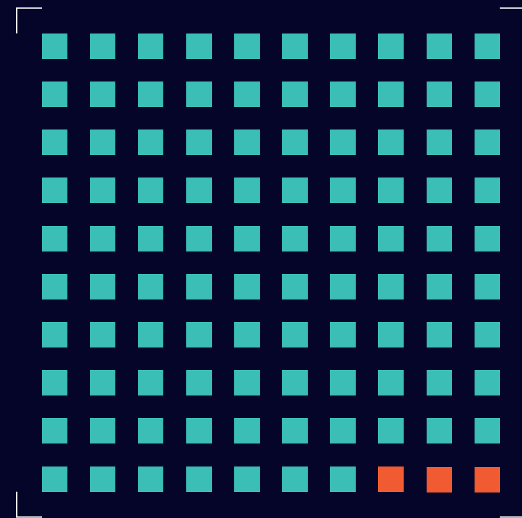
These leaders are also operating in a truly global footprint. The respondents are distributed across North America (263), EMEA (252), LATAM (243) and APAC (252), as well as across payments/fintech/financial services (347), retail/eCommerce (331) and betting and gaming (332). Their work spans revenue protection, customer experience, regulatory compliance and cross-border expansion — making their decisions central to whether growth is sustainable.

2026: A Year Defined by Growth

Expansion is the default setting for 2026

Expansion Plans

In 2026, which of the following does your organization plan to do?



- **97%** of companies plan major growth move
  - 17% plan to expand into a new country or region
  - 25% plan to launch a new product or service
  - 55% plan to do both
- **3%** expect to do neither

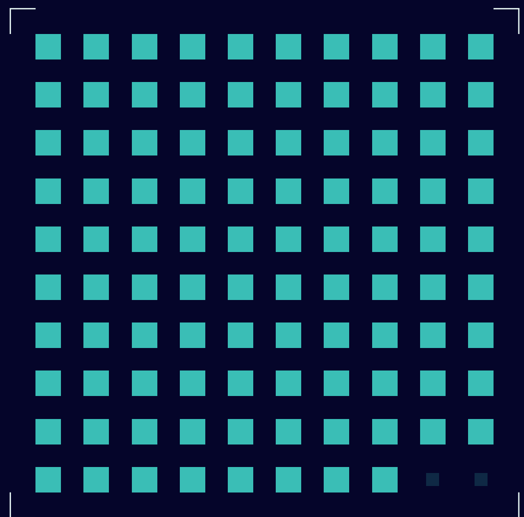
This combination of product and geographic expansion fundamentally reshapes the fraud landscape. It drives higher transaction volumes, introduces new payment methods and behaviors and increases regulatory exposure across multiple jurisdictions, all of which expand the surface area fraud and AML teams must monitor and control.

Top Threat Vectors Reported by Respondents

- **Account takeovers:** 26% — the most commonly cited threat, reflecting rising credential-based attacks
- **Promotion or discount abuse:** 18% — frequent exploitation of marketing offers and incentives
- **Return fraud:** 18% — persistent challenge linked to lenient refund policies
- **Chargebacks:** 16% — often tied to disputed transactions or false claims
- **Loyalty or rewards program abuse:** 13% — targeting stored value and points-based systems
- **Alternative payments abuse (e.g., crypto):** 6% — reflecting the growing risk in emerging payment channels
- **First-party or "friendly" fraud:** 4% — lower in volume but difficult to detect and dispute

AI Adoption in Fraud & AML Workflows

Do your teams already use or plan to integrate AI?



98% of leaders say their teams are already integrating AI into their workflows

The Core Tension

Against this backdrop, AI is a success story on paper. Ninety-eight percent of leaders report that their teams are already integrating AI into fraud and AML workflows, and 95% say they are at least somewhat confident that AI can reliably detect and prevent fraud; more than half (52%) describe themselves as very confident. AI and automation have clearly moved from experimentation into everyday operations.

But resourcing and complexity are moving in the opposite direction as the "AI will simplify everything" narrative." Looking ahead to 2026, 83% of organizations expect their fraud and AML budgets to increase, and 94% plan to add at least one full-time fraud/AML hire. At the same time, only 47% run fully integrated fraud and AML workflows. In comparison, another 47% rely on partial integration, and 80% report that obtaining a unified view of data and insights is at least somewhat challenging.

The core tension is simple: AI adoption and confidence are high, but hiring, budgets and operational investment continue to grow, and many teams still struggle with fragmented systems and incomplete visibility.

Section 2

AI Has Moved From Experimentation to Expectation

Near-Universal AI Adoption in Fraud & AML

With 98% of leaders already integrating AI into their workflows, just 2% are still in the planning phase. This adoption spans regions and verticals, embedding AI into how alerts are triaged, cases are investigated and risk decisions are made.

Where AI Is Embedded Today (and Where It Isn't)

The deepest penetration is in core monitoring and scoring. When asked which AI tools they use today:

- AI & ML for transaction monitoring tops the list at 30%, making it the most common and mature application
- AI risk scores with explainable outcomes are used by 14%, surfacing machine-learned assessments in a form that analysts and auditors can interrogate
- AI-generated summaries for alerts and cases are now live at 12%, reducing manual narrative work and accelerating investigations
- AI & ML for anomaly detection are in place at 11%, flagging subtle behavioural or transactional outliers beyond static rules

Specialized capabilities are emerging at more minor, but meaningful, scales:

- AI regulatory reporting/automatic form fills are used by 13% of organizations
- AI SAR narrative generation and AI agents for sanctions screening each achieve a 5% success rate
- AI agents for transaction monitoring are used by 8%, typically as copilots that recommend actions rather than fully automate them

Almost no one is sitting out entirely, with 2% reporting that they are not currently using AI but plan to implement it, and 0% in the neither use nor intend to use AI for fraud and AML purposes. AI has transitioned from an innovative status to a baseline expectation, even if the depth and sophistication vary by use case.

AI Tools in Use

What AI tools are you currently using?

30% AI & ML for transaction monitoring vs rules-based systems

14% AI risk scores (with explainable outcomes)

14% AI regulatory reporting automatic form fills

12% AI summaries (e.g. for alerts and cases)

11% AI & ML for anomaly detection

8% AI Agents for transaction monitoring

5% AI Agents for sanctions screening

5% AI SAR narrative generation

2% We are not currently using AI, but planning to implement it in the near future

Confidence, Limits & the End of the Pilot Mode

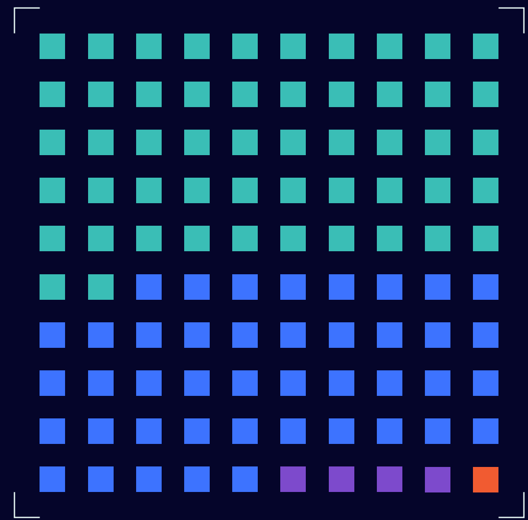
Confidence in AI is high. Ninety-five percent of leaders are somewhat confident that AI solutions can reliably detect and prevent fraud, and more than half (52%) describe themselves as very confident. Just 4% are "not very confident" and 1% "not confident at all."

This confidence rises with growth. Among organizations projecting 0–10% revenue growth, 40% are very confident in AI; this increases to 48% for those expecting 11–25% growth, 59% for the 26–50% group and 68% among those forecasting 51% or more increase. Faster-growing companies are more likely to see AI as a dependable part of their risk stack rather than a test bed.

At the same time, the surrounding data shows clear limits. Even with this degree of adoption and trust, 83% still expect fraud and AML budgets to increase and 94% plan to grow headcount, while many report persistent challenges with integration and visibility. Pilot mode is over; the complex problems now lie in scaling, governing and connecting AI, not in proving that it works.

Perceived Reliability of AI

How confident are you that AI solutions can reliably detect and prevent fraud today?



- 52% - Very confident
- 43% - Somewhat confident
- 4% - Not very confident
- 1% - Not confident at all

Confidence in AI

Percent that responded "very confident" that AI solutions can reliably detect and prevent fraud

40% — Respondents that project 0–10% growth in 2026

48% — Respondents that project 11–25% growth in 2026

59% — Respondents that project 26–50% growth in 2026

68% — Respondents that project 51%+ growth in 2026

Section 3

Investment Keeps Climbing

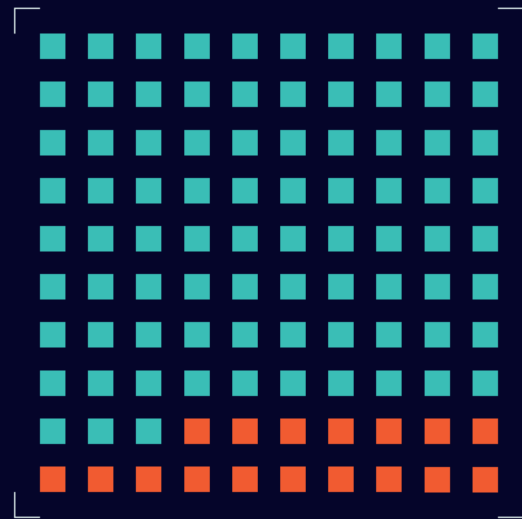
Fraud & AML Budgets in 2026

Budgets are trending upward. Looking into 2026, 83% percent of organizations expect their fraud and AML compliance budget to increase, while only 17% expect it to remain flat or decrease ("not increase").

This follows a period in which 86% said their fraud budget would increase, indicating that elevated spend is becoming the norm rather than a temporary spike.

Expectations for Change

Looking ahead to 2026, how do you expect your fraud and AML compliance budget to change?



83% - Increase

17% - Not Increase

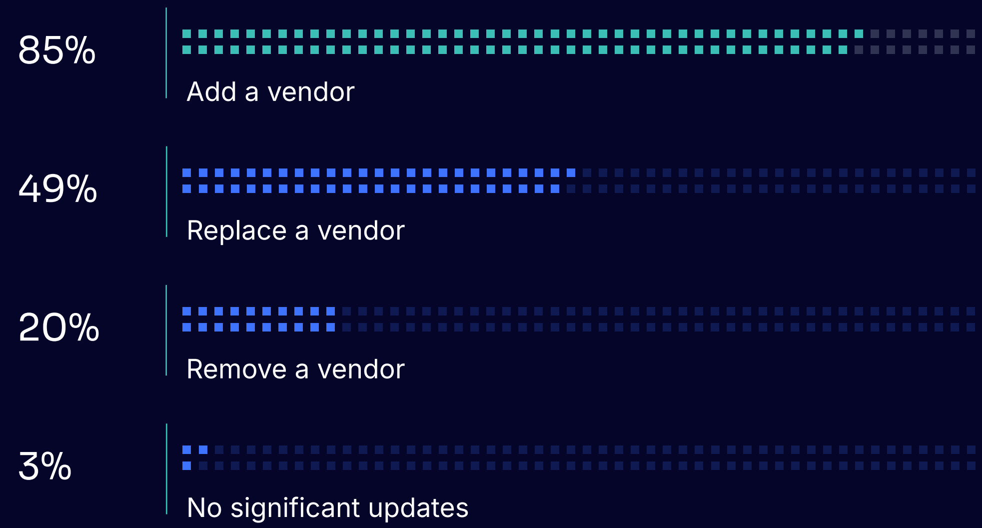
Where Leaders Are Placing Their Bets

On the people side, investment is reflected in concrete hiring plans. The share of organizations planning to add at least one full-time fraud or AML hire has risen from 88% in 2025 to 94% in 2026. Within that 94%:

- → 11% plan to add 1–2 full-time hires (112 organizations)
- → 33% plan 3–5 hires (336 organizations)
- → Another 33% plan 6–10 hires (332 organizations)
- → 17% plan to add more than 10 full-time roles (167 organizations)
- → 3% plan to add contractors (31 organizations)
- → Only 3% report no plans to increase headcount (32 organizations)

On the technology side, almost everyone expects to touch their stack. When leaders are asked what updates they plan to make to their fraud and/or AML technology in 2026:

Plan to change fraud / AML technology stack



This means that well over 85% of organizations will make at least one structural change to their fraud or AML stack, whether by adding new capabilities, replacing existing tools or both.

Vendor Sprawl, Consolidation & Modernization

These choices reveal how leaders are thinking about their tooling. The fact that more than 85% intend to grow their tech stack by adding a vendor and 49% intend to replace at least one vendor in 2026 signals that few teams are satisfied with their current configuration; most are actively moving toward more modern, AI-enabled or better-integrated solutions. At the same time, the 20% who plan to remove a vendor indicate a selective push against unchecked sprawl rather than a pure "more tools" strategy.

The mix of "add," "replace" and "remove" suggests a blended approach. Many organizations are simultaneously introducing new capabilities and replacing underperforming providers rather than simply adding tools on top of legacy platforms. The tiny minority reporting no significant updates (3%) underscores how rare it is for a fraud or AML stack to stay static from one year to the next.

When viewed alongside rising headcount and budget plans, these data points indicate that investment is not about chasing individual features; it is about building an architecture that can handle increased volume, structural complexity and regulatory and operational scrutiny. Leaders are funding people and platforms together, aiming to create environments where AI, first-party data and human expertise can work in tandem rather than in silos.

Section 4

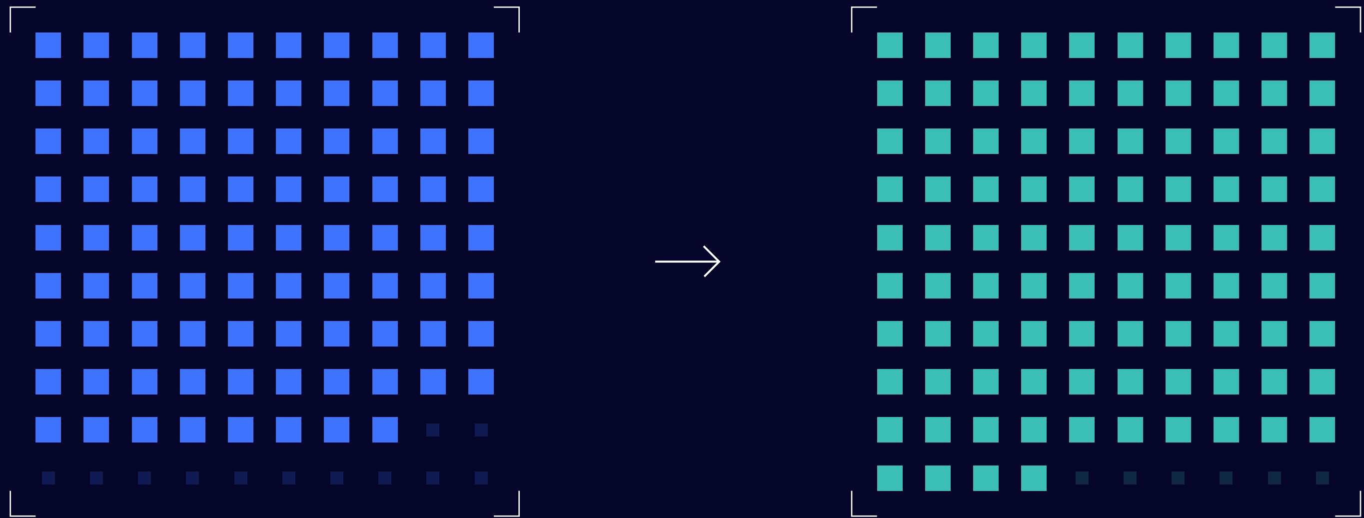
Automation Is Not Reducing Headcount — It's Redefining It

Why Teams Are Growing in the Age of AI

Automation has not led to leaner fraud and AML teams; it has coincided with more hiring. For the 2025 planning cycle, 88% of leaders expected to increase headcount. For 2026, that share has risen to 94%, confirming that staffing continues to increase, not decrease.

Percent of Respondents That Planned to Add at Least One Full Time Hire For the Following Year

Do you plan to add at least one full-time hire next year?



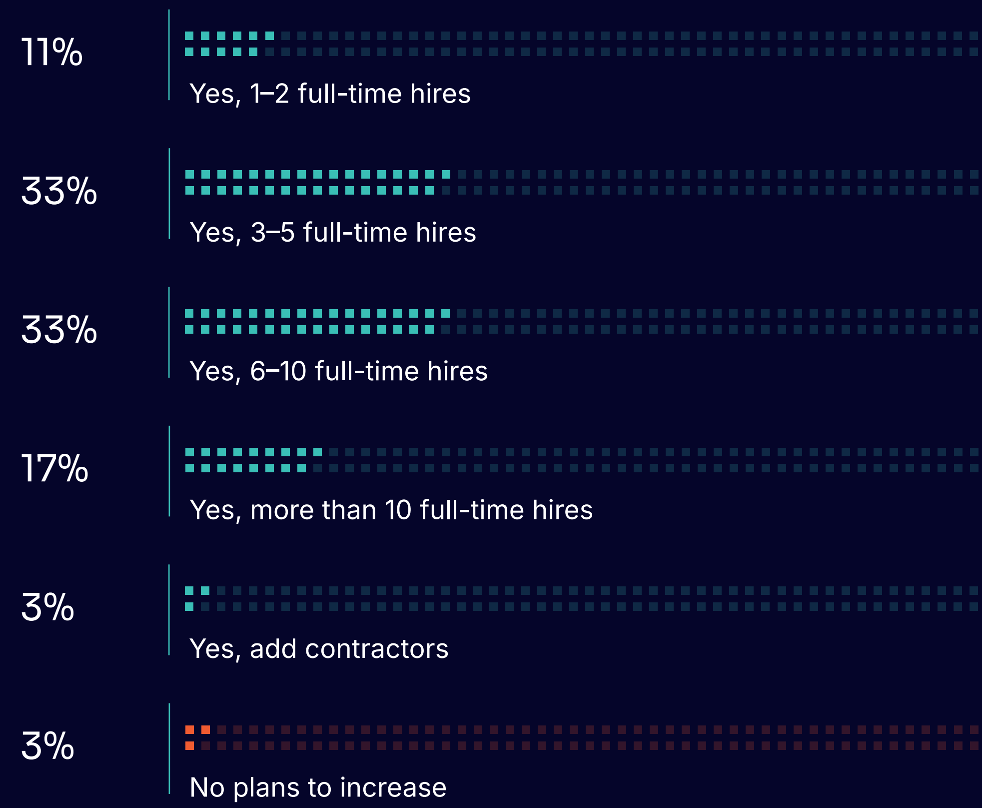
88% of leaders plan to grow their team in 2025

94% of leaders plan to grow their team in 2026

What is changing is the nature of the work. Rather than simply adding more analysts to do the same tasks, leaders are orienting roles toward higher-judgment activities that cannot be fully automated. In effect, AI and automation have created additional work that humans must do, requiring human discernment, regulatory knowledge and cross-functional influence.

Breakdown of Hiring Plans for 2026

Do you plan to increase headcount for your fraud and/or AML team in 2026?



The New Fraud & AML Org Chart

The emerging fraud and AML organization looks less like a small back-office team and more like a distributed intelligence function. As AI and machine learning scale, leaders report increased demand for roles focused on model monitoring, validation, exception handling, complex investigations and regulatory reporting — functions that cannot be fully automated without undermining oversight.

At the same time, the integration data reveals why coordination roles are growing. While 95% of organizations report some level of integration between fraud and AML workflows, only 47% operate a fully integrated platform or workflow, with another 47% relying on partial integration and 6% operating with little or no integration at all. This “in-between” state creates demand for individuals who can bridge systems, reconcile signals and align teams across fraud, AML, product, engineering and compliance.

AI Agents as Support, Not Substitutes

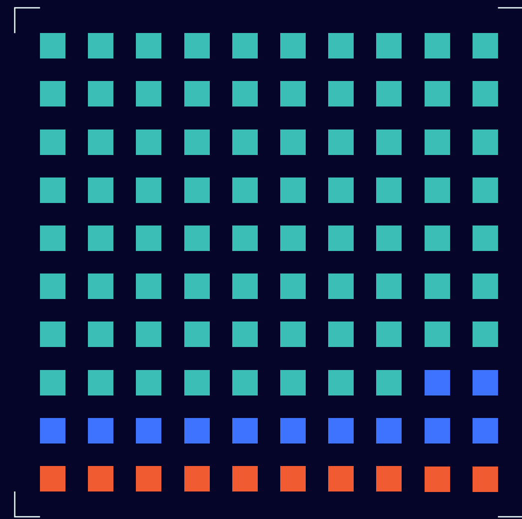
Views on AI agents crystallize the new division of labor. When asked how they see AI agents in fraud and AML operations:

- Only 12% say agents should eventually replace analyst tasks
- 40% believe agents should support analysts with recommendations and summarization based on standard operating procedures
- 38% say agents should augment investigators, providing a starting point for deeper investigations, but not replacing them
- 7% see agents as promising but not yet mature
- 3% prefer human-driven decisions with minimal AI involvement
- 1% say it is too early to tell

In total, over 80% of leaders place AI agents in a supporting or augmenting role, rather than a replacement role. Automation handles volume and repetitive analysis, while humans move into roles that design, supervise and explain these systems — an organizational chart that is larger, more skilled and accountable.

Where AI Agents Fit Today

What best describes your current perspective on AI agents in fraud and AML operations?



- 78% - AI agents should support or augment analysts
- 12% - AI agents should replace analysts
- 10% - Skeptical / prefer minimal AI / unsure

Section 5

What the Data Is Really Telling Us

Why Automation & Hiring Are Rising Together

At first glance, the numbers appear contradictory: AI usage is almost universal and confidence is high, yet budgets and headcount continue to rise.

Ninety-eight percent of organizations already use AI in fraud and AML, and 95% are somewhat or very confident in its ability to detect and prevent fraud. At the same time, 83% expect fraud and AML budgets to increase and 94% plan to grow their teams.

The integration and visibility data help explain this coexistence. While almost all organizations claim that their fraud and AML workflows are at least partially connected, only 47% operate a truly unified platform workflow; another 47% rely on partial integration, 5% on separate systems with little coordination and 1% have no integration at all. Additionally, 80% of leaders report that it is at least somewhat challenging to obtain a unified view of data and insights across fraud and AML systems, with more than 40% describing this as extremely or very difficult.

In other words, AI has improved detection at the workflow level, but scale, fragmentation and oversight requirements have expanded the overall workload faster than efficiency gains can offset it.

Three Structural Forces Reshaping Fraud & AML

Three forces emerge from the data as the main drivers of simultaneous automation and hiring:

1

Volume is scaling faster than efficiency gains

The growth figures indicate that around 80% of companies have increased their revenues by more than 10% in the past year, with a significant share exceeding 25%. That translates into more users, sessions and transactions across more products and geographies. Automation improves how each event is handled, but the total number of events continues to grow, so teams absorb more throughput and complexity rather than less.

2

Oversight and governance requirements are rising

As AI becomes embedded in risk decisioning, regulators emphasize explainability, auditability and human accountability. Leaders must be able to show how decisions were made, which models and rules were used and how outcomes are monitored and corrected. his raises demand for skilled humans in roles such as model monitoring, validation, exception handling and regulatory reporting — functions that expand as AI usage grows, not shrink.

3

Fraud threats are adapting alongside defenses

The increased use of AI and automation has not slowed adversaries; it has pushed them to become more adaptive, cross-channel and sophisticated. New fraud patterns emerge more quickly, edge cases proliferate and static controls become increasingly ineffective. Human judgment remains essential for assessing novel behaviors, investigating unknown patterns and refining controls as threats change, even as automation accelerates detection and response.

Together, these forces mean that AI enables fraud and AML teams to operate at greater scale, but scale itself is expanding even faster.

From Workload Illusion to True Demand

For years, the assumption was that automation would simplify fraud and AML operations enough to reduce team size. The 2026 data suggests that this assumption was always incomplete.

The combination of near-universal AI adoption, rising budgets, aggressive hiring and persistent integration challenges indicates that earlier “workload” estimates were artificially low because so much risk, data reconciliation and oversight work was previously invisible.

AI and automation have not merely made existing work more efficient; they have revealed the actual demand: the real volume of events that need evaluation, the complexity of cross-system integration and the depth of governance required for explainable, defensible decisions. As a result, teams are not doing the same job with fewer people; they are doing a larger, more complex job with systems that can finally keep up.

Section 6

Fragmentation Becomes the Bottleneck at Scale

Partial Integration vs. True Unification

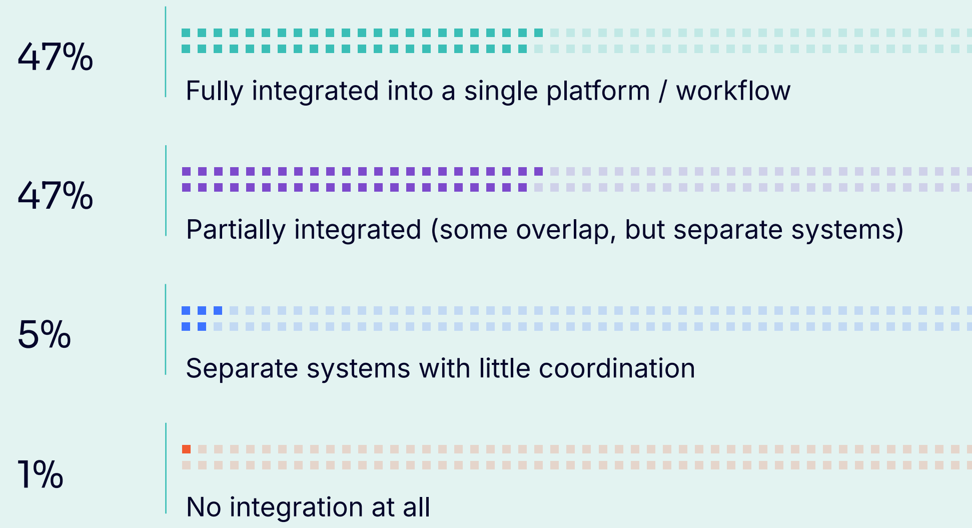
On paper, most organizations claim that fraud and AML are connected, but in practice, they are often stitched together. Ninety-five percent report at least some integration between fraud prevention and AML workflows, yet only 47% operate a fully integrated platform or workflow.

Another 47% rely on partial integration — some shared data, but separate systems — and 6% run separate or non-existent integrations (5% with little coordination, 1% with none).

This “almost integrated” state becomes fragile at scale. As transaction volumes, products and markets grow, seams between systems become more visible and more costly, especially when decisions must be made in real time across both fraud and AML contexts.

The State of Fraud–AML Integration

How integrated are your organization’s fraud prevention and AML workflows?

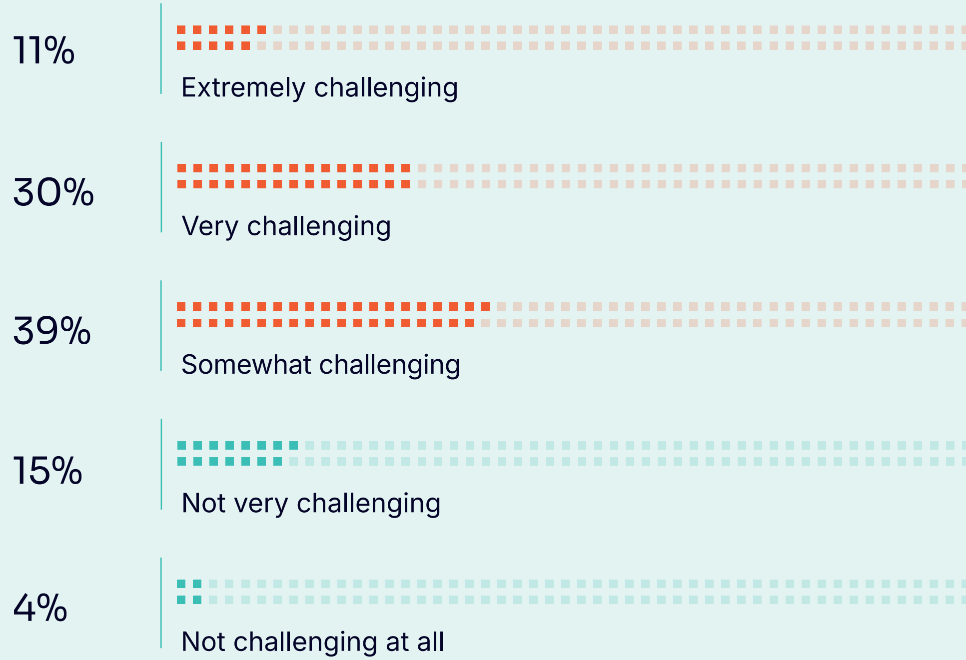


The Cost of Data Silos & Blind Spots

The visibility numbers highlight how integration gaps become apparent on a day-to-day basis.

Difficulty in Achieving a Unified Fraud & AML Data View

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



In total, 80% of leaders experience at least some difficulty achieving a single view, and more than 40% are at the “extremely” or “very” challenging end of the spectrum. These data silos create operational tax: slower investigations, more false positives, duplicated effort and greater reliance on manual reconciliation between fraud and AML teams.

How High-Growth Companies Think About Integration

Growth brings sharper consequences for fragmentation. When looking at those who say unified visibility is not very challenging or not challenging at all, only 19% of all respondents fall into that group — but the share rises with revenue growth:

- Among companies with 0–10% revenue growth, 23% said unified visibility is not very challenging or not challenging at all
- Among those with 11–25% growth, 16% said the same
- For 26–50% growth, 20% said the same
- For the 51%+ growth group, 39% said unified visibility is not very challenging or not challenging at all

This information suggests that high-growth companies are more likely to treat integration and shared data backbones as strategic infrastructure: reducing reliance on disconnected point solutions and designing workflows where fraud and AML intelligence truly converge, rather than merely connect.

The flip side is that mid-growth companies often feel the sharpest pain. In the 11–25% and 26–50% revenue-growth bands, more than 40% of organizations say achieving unified visibility is extremely or very challenging — higher than in the slowest and fastest-growing groups combined. These are businesses that have outgrown ad hoc integrations but have not yet fully invested in unified architectures, leaving fraud and AML teams to absorb complexity without the benefit of a single, comprehensive view.

Section 7

Time-to-Value Remains a Sluggish

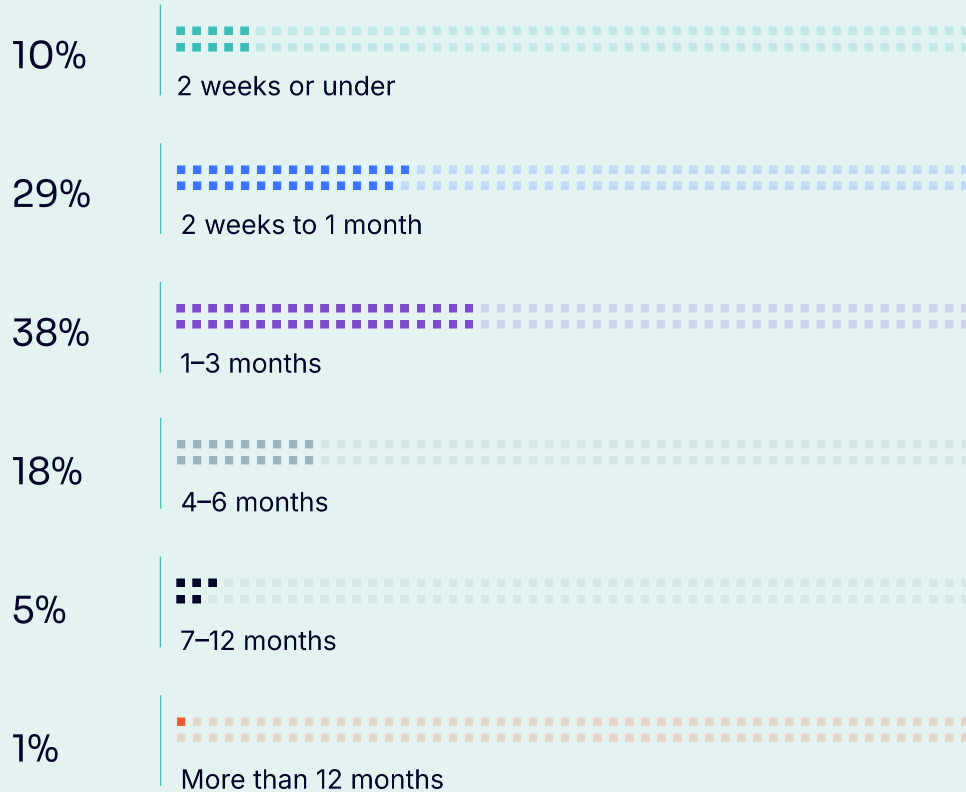
How Long Does It Really Take to Go Live

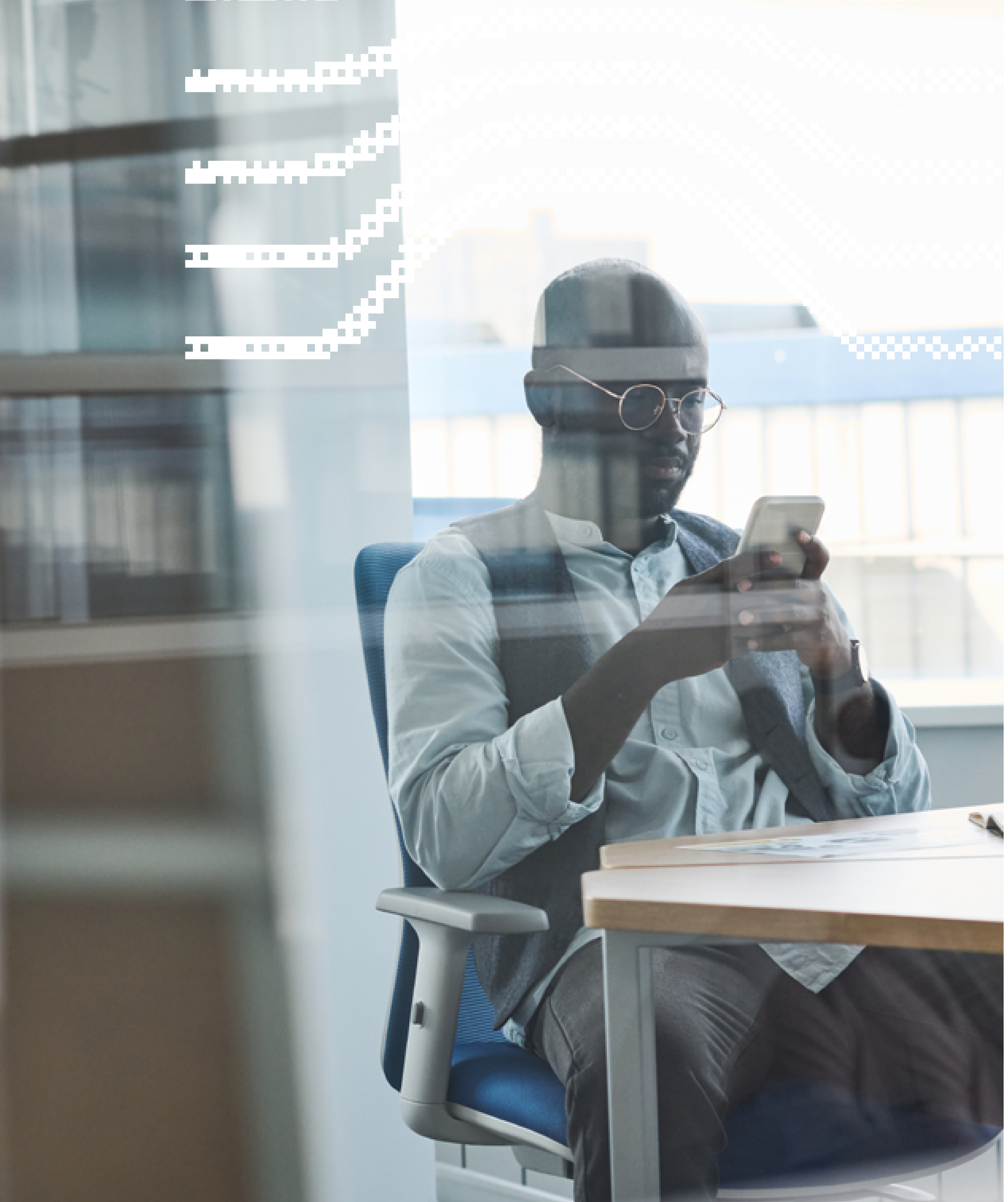
Even as cloud and AI tools mature, the implementation speed has not kept pace with business urgency. After selecting their most recent fraud or AML vendor:

The majority, therefore, spend at least one to three months, and a significant minority spend four months or more, between vendor selection and go-live. In fast-moving fraud environments, those months represent periods where exposure remains higher than leaders would like.

Reported Implementation Timelines for Fraud & AML Platforms

After selecting your most recent fraud or AML vendor, how long did it take to go live with the new solution?





The Hidden Cost of Slow Implementations

When timelines slip, the impact is tangible. Among respondents whose go-live took longer than initially planned, the most common adverse effects were:

- → Increased operational costs (reported by 52% of respondents)
- → Prolonged exposure to fraud risks (47% of respondents)
- → Delayed realization of ROI (26% of respondents)
- → Required excessive technical resources (36% of respondents)
- → Negative impact on team productivity (32% of respondents)
- → Frustration among stakeholders (27% of respondents)
- → Diverted focus from other business opportunities (25% of respondents)

Only 14% said the impact was "minimal," and 7% indicated their go-live did not take longer than planned. Slow implementations do not just delay benefits; they keep teams in hybrid states where legacy systems, manual workarounds and new tools all coexist, stretching capacity and clouding accountability.

Reported Consequences of Extended Go-Live Timelines

If your go-live timeline took longer than originally planned, what negative impacts resulted from that delay?

52% Increased operational costs

47% Prolonged exposure to fraud risks

36% Required excessive technical resources

32% Negative impact on team productivity

27% Frustration among stakeholders

26% Delayed realization of ROI

25% Diverted focus from other business opportunities

14% Minimal impact

7% My go-live timeline did not take longer than originally planned

When Delay Becomes a Risk Vector

As organizations process more real-time payments and onboard customers faster across more markets, time-to-value becomes a direct risk vector. Every extra month between vendor selection and full deployment extends the window during which outdated models and rules remain in production, manual processes and legacy tools carry a greater load than they should and new fraud patterns may emerge before updated defenses are fully operational.

In this environment, speed plays a crucial role in the control environment. Leaders who can reliably move from selection to impact in weeks rather than quarters reduce both their fraud exposure and the organizational fatigue that comes with long, complex implementations.

Section 8

What Leaders Are Watching Next

From "Does AI Work?" to "Can We Trust & Govern It?"

The conversation around AI is shifting. With 98% of organizations already using AI in fraud and AML, and 95% expressing at least some confidence in its reliability, the focus is shifting from basic effectiveness to governance, explainability and control.

Leaders are increasingly concerned with demonstrating how AI-driven decisions are made, monitoring and adjusting models as patterns change and ensuring human accountability and regulatory compliance in AI-supported workflows.

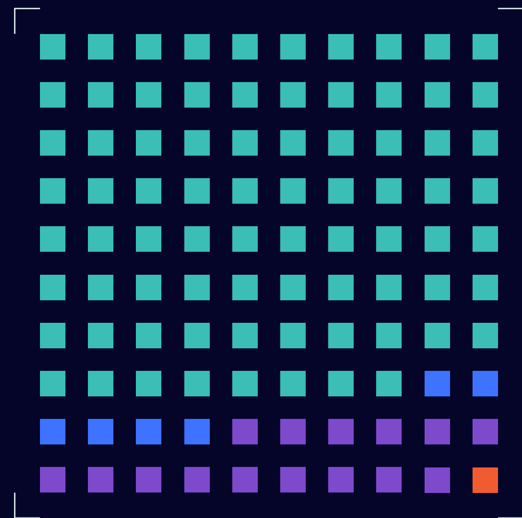
The integration and visibility challenges — where 80% find unified views at least somewhat difficult — reinforce why this governance lens matters: trust in AI must extend beyond individual scores to the entire decision pipeline.

Decentralized Digital Identity and Other Long-Term Signals

Beyond AI, leaders are watching shifts in identity and regulation. When asked whether decentralized digital identity (e.g., Web3 verifiable credentials) will become a significant part of fraud and AML prevention:

Industry Readiness for Decentralized Identity

Do you believe decentralized digital identity will become a major part of fraud and AML prevention in the future?



- 78% say yes — it will be central to the future
- 6% say no — it will not play a major role
- 15% say it is too soon to tell
- Fewer than 1% say they don't know enough to answer

On the broader regulatory and threat landscape, leaders see multiple external forces shaping AML compliance over the next two years:

These responses suggest that leaders expect the next phase of fraud and AML to be defined by identity innovation, AI-enabled adversaries and tighter, more complex regulatory frameworks.

Combined, these pressures underscore why explainability and governance recur throughout this report. When one in three leaders identifies data-privacy enforcement as the dominant external force, and one in four highlights the advancing use of AI by criminals, opaque models and resold third-party data become strategic liabilities. Transparent, first-party signal architectures are the only sustainable way to satisfy regulators while keeping pace with AI-driven attackers.

Top External Pressures Affecting Fraud & AML Programs

Which single external factor do you expect to have the biggest impact on AML compliance in the next two years?

33%	Data privacy regulations (e.g., GDPR, CCPA)
25%	Criminals' advancing use of AI and obfuscation techniques
11%	Growth of crypto/decentralized finance adoption
10%	Expanding sanctions regimes
9%	Political/regulatory uncertainty
9%	Increasing cross-border transactions
5%	Shortages in skilled AML compliance talent

The Future Skill Set of Fraud & AML Teams

As these trends converge, the profile of the fraud and AML professional is changing. Leaders are increasingly prioritizing skills in:

- AI, machine learning and advanced data analytics, to understand, challenge and improve automated decision-making
- System architecture and technology integration, to navigate multi-vendor stacks and unify data flows
- Regulatory and compliance knowledge, to interpret evolving requirements around AI, privacy and cross-border activity
- Cross-departmental collaboration and communication, to work effectively with product, engineering, compliance and customer experience teams

Together with the strong preference for AI agents as support rather than replacement, these priorities point toward teams that act as designers and governors of intelligence — shaping how AI, data and workflows come together, rather than simply operating tools.

Final Reflections: Where Leaders Go From Here

The numbers here mark a clear inflection point. AI now runs through almost every fraud and AML program, yet leaders still add personnel, increase budgets and struggle with fragmented systems. The old assumption — that automation would simplify operations — no longer holds.

1

From tools to architecture

Most organizations already own enough point solutions. The real advantage lies in connectivity: whether fraud and AML share a data backbone, whether signals travel across products and regions and whether decision logic stays explainable end-to-end. The gap between the 47% with integrated workflows and the 80% who can't view everything in one place speaks volumes.

2

From projects to muscle memory

Time-to-value is now a structural property of the organization, not a project milestone. Leaders who deploy new vendors and controls in weeks rather than quarters narrow their exposure window every time they move. Long implementations quietly keep legacy controls alive, even as threats accelerate.

3

From operators to system designers

As AI takes on pattern-matching and triage, fraud and AML roles shift toward pattern-setting. Teams that thrive treat rules, models, integrations and KPIs as design choices to iterate on — not fixed constraints. That shows how they use AI (copilot, not a blackbox), how they staff (toward analytics and governance) and how they engage product, engineering and compliance.

The organizations that treat fraud and AML as an intelligence discipline — where explainable automation, first-party signals, unified workflows and empowered teams reinforce each other — are the ones that will set the pace, balancing AI and human judgment and keeping humans firmly in the loop to question models, interpret edge cases and own the decisions that matter most.

SEON

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 ⟶