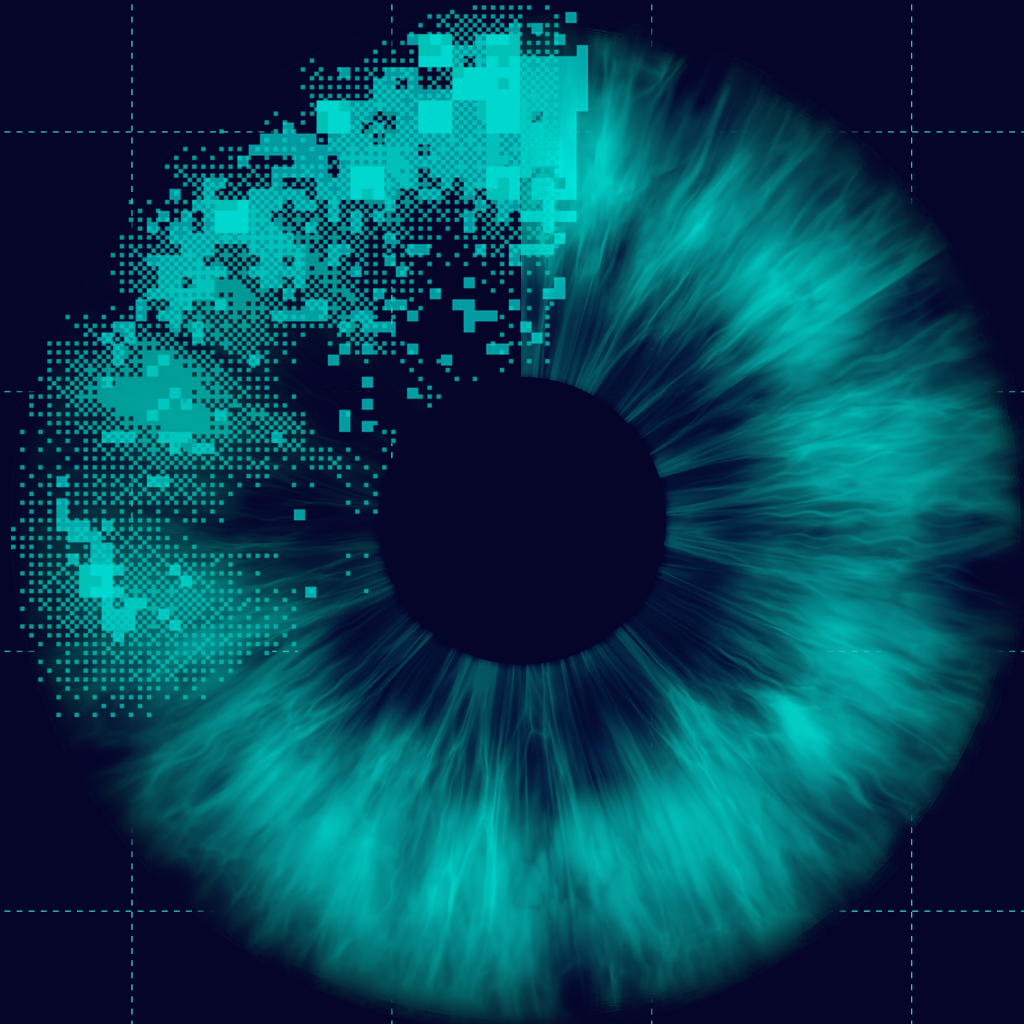


SEON

Scaling Without a Safety Net

How Betting & Gaming's Fraud Losses Are Outpacing Revenue

Insights from SEON's 2026 Fraud & AML Leaders Survey

Table of Contents

Executive Summary & Methodology

Executive Summary

Betting and gaming is the fastest-growing sector in our survey. Yet beneath the surging metrics, a structural problem is quietly compounding: operators are critically underprepared to defend the platforms they are scaling.

More than half of betting and gaming operators report revenue growth exceeding 26% over the past year. They are launching novel products, entering new markets and competing aggressively for players. By every commercial measure, the industry is thriving. But that aggressive expansion has come at a steep cost — 57% of operators now report that their fraud losses are growing faster than their revenue.

To stem the tide, operators are defaulting to a familiar, albeit unscalable, reflex: hiring. Nearly half (47%) are prioritizing headcount over every other budget line in 2026. Unfortunately, the risk professionals they bring in are stepping into a deeply fragmented environment. Disconnected point solutions for KYC, fraud detection and AML keep critical data siloed, actively hindering automation. False positives pile up. Vendor integrations stall. Meanwhile, strategic investment in AI is 23 percentage points below the rate in other industries.

This gap is architectural, not technological. To stop throwing headcount at a structural problem, operators must first fix their data foundation to break the loop.

Methodology

As part of SEON's AI Reality Check: 2026 Fraud & AML Leaders Report, this research draws on responses from 332 betting and gaming leaders. It examines several prevailing issues at the center of the industry's fraud landscape: how growth strategies create fraud faster than defenses can absorb it, why disconnected tools make the growing threat impossible to triage and why the default response of hiring over automating simply cannot scale. The insights are specific to betting and gaming operators worldwide and grounded in current decision-making frameworks.

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 is sourced directly from survey responses unless otherwise noted.

Key Findings

1

Growth Is Feeding the Fraud Problem

Betting and gaming's dominant fraud threats are a direct consequence of the industry's own growth playbook. Account takeover leads all categories at 27%, followed by promotion and bonus abuse (23%) and loyalty program abuse (18%). Together, these three types account for 68% of all fraud losses.

Crucially, every one of them exploits the exact incentive structures operators built to acquire and retain players. Growth and fraud are not separate problems in betting and gaming; they are deeply intertwined. And for 57% of operators, fraud is winning the race against revenue.

2

Disconnected Tools Are Making It Worse

Many operators run separate, siloed systems for KYC, fraud detection and AML compliance. Because each tool only views a narrow slice of the player journey, the platform can never see the whole picture. Consequently, betting and gaming leaders are nearly four times more likely than their peers in other industries to describe creating a unified data view as "extremely challenging" (22% vs. 6%).

As attack volumes rise, these disconnected tools cannot correlate signals across the player lifecycle. Alerts fire on incomplete information, and false positives climb. In response, 28% of operators plan to rip out and replace a vendor in 2026 — nearly double the rate of other industries — as they desperately search for a way out of the complexity they've created.

3

The Default Response Cannot Scale

Betting and gaming is investing in people, not technology, at an unmatched rate. While 47% of operators prioritize headcount increases, only 34% are actively investing in AI and machine learning. Across every other industry we studied, AI investment leads headcount. Betting and gaming is the lone sector where this priority is inverted. This isn't due to AI skepticism; operators actually lead in specific, localized AI applications, such as alert summaries.

The gap is structural. You simply cannot deploy sophisticated machine learning across fragmented, disconnected systems. So, operators pull the only lever they have left: hiring. But people scale linearly, and fraud scales exponentially.

Section 1

The Growth Engine

When Growth Creates Its Own Risk

Betting and gaming systematically expands its own attack surface. With over half of operators reporting revenue growth of 26% or more over the last 12 months, the momentum is undeniable. An overwhelming 99% plan to launch a new product or enter a new market in 2026. Yet, every new region unlocked and every welcome bonus deployed acts simultaneously as a growth lever and a fraud vector.

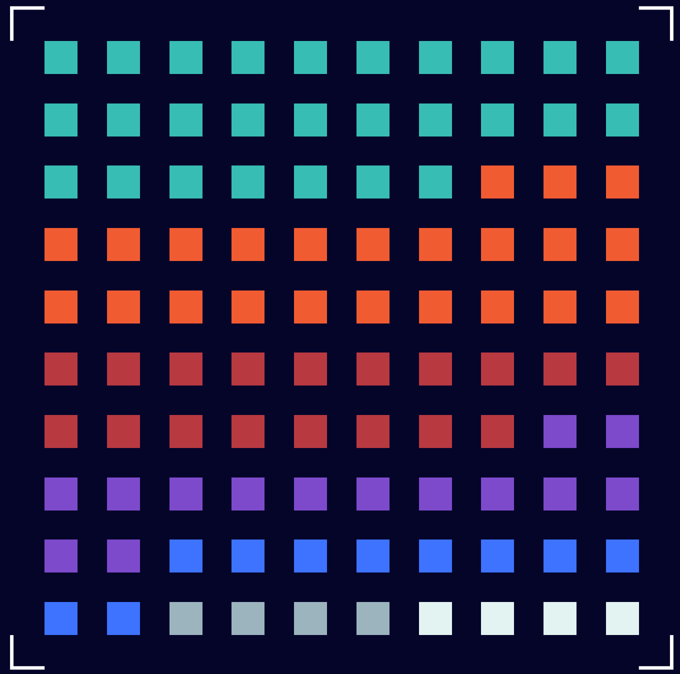
Unlike other industries, where fraud primarily poses an external threat to payment systems, betting and gaming face threats that constitute a form of business abuse. Account takeover and promotion abuse account for the majority of the sector's losses because they deliberately target the incentive structures designed to drive acquisition. The faster operators grow, the more incentives they introduce — and the wider the surface area becomes for organized abuse.

Successful operators understand that sustaining growth requires building capable defenses. By turning risk intelligence into a competitive advantage, they can confidently offer more generous incentives, knowing their controls will absorb the risk without bleeding revenue.

Where Betting & Gaming Fraud Comes From

What is the primary source of online fraud losses at your organization?

- 27% - Account takeovers
- 23% - Promotion / bonus abuse
- 18% - Loyalty / rewards program abuse
- 14% - Chargebacks
- 10% - Return fraud
- 5% - Alternative payments abuse (crypto)
- 4% - First-party / friendly fraud



→ **The top three fraud types account for 68% of all losses. Every one of them is directly tied to betting and gaming's growth and retention strategies.**

Section 2

The Broken Foundation

The Point-Solution Problem

When operators work across disconnected systems, the root cause of their challenges remains purely architectural. Individual point solutions often perform well in isolation, yet they inevitably fail to provide a cohesive view of risk.

Imagine a KYC system flagging a suspicious document during onboarding. If the fraud engine doesn't see that signal, it will miss the pattern when the same player triggers a bonus abuse alert three weeks later. Or consider an AML alert firing on a high-value withdrawal, while the crucial investigation data sits trapped in a separate fraud system. When risk signals stay siloed, the consequences ripple across the entire organization.

The frustration is palpable. Over half (55%) of betting and gaming leaders say achieving data visibility is extremely or very challenging. When asked about integration barriers, 52% cite a lack of skilled personnel, while 49% cite data silos. To correct course, 28% of operators plan to remove a vendor in 2026 — nearly double the rate recorded in other industries. Solving this fragmentation requires deliberate consolidation. Operators must transition to a unified platform that connects KYC, AML and fraud data into a single, comprehensive view.

Difficulty Creating a Unified Data View

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

→ **Betting and gaming operators are nearly 4x more likely than peers to say unified data is "extremely challenging."**

Top Integration Barriers

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

→ **The barriers to fixing fragmentation are internal — people, silos and culture — not external. That means the problem is solvable. It is a question of prioritization, not capability.**

Section 3

The Headcount Trap

Hiring Falls Short of Solving Architectural Problems

When fraud volumes rise, and the tools lag, the immediate instinct is to hire. Across all industries in our full AI Reality Check report, hiring is increasing as automation reshapes the nature of fraud work. But in betting and gaming, the pattern is distinct.

Today, 47% of betting and gaming operators are prioritizing headcount increases in their 2026 budgets, a figure that sits nearly 12 percentage points higher than other industries. Almost all operators plan to add staff, with the largest segment targeting six to ten new full-time risk professionals.

On the surface, leaders are making a rational choice in an irrational situation. Teams are completely overwhelmed, with more than a third of operators experiencing false-positive rates of 26% to 50%. Their disconnected systems lack the underlying architecture to support meaningful automation. Consequently, the industry is trying to scale its defenses with people, while fraud scales aggressively with technology. Every new hire simply inherits the same broken infrastructure.

This dynamic sharpens the AI paradox within the sector. Betting and gaming operators actually lead other industries in practical, localized AI applications — like auto-filling regulatory reports or generating alert summaries. However, when it comes to strategic investment in AI and machine learning capabilities, betting and gaming allocates just 34% of its budget, compared to 57% elsewhere. The constraint is not a lack of willingness; it is a lack of infrastructure. Operators deploy AI eagerly within bounded systems, but without unified data, transformational AI remains out of reach.

Where the Budget Goes

In which areas is your organization allocating increased fraud/AML budget for 2026?

	Betting and Gaming	Other Industries	Delta
Headcount increases	47%	35%	+12%
AI / ML investment	34%	57%	-23%

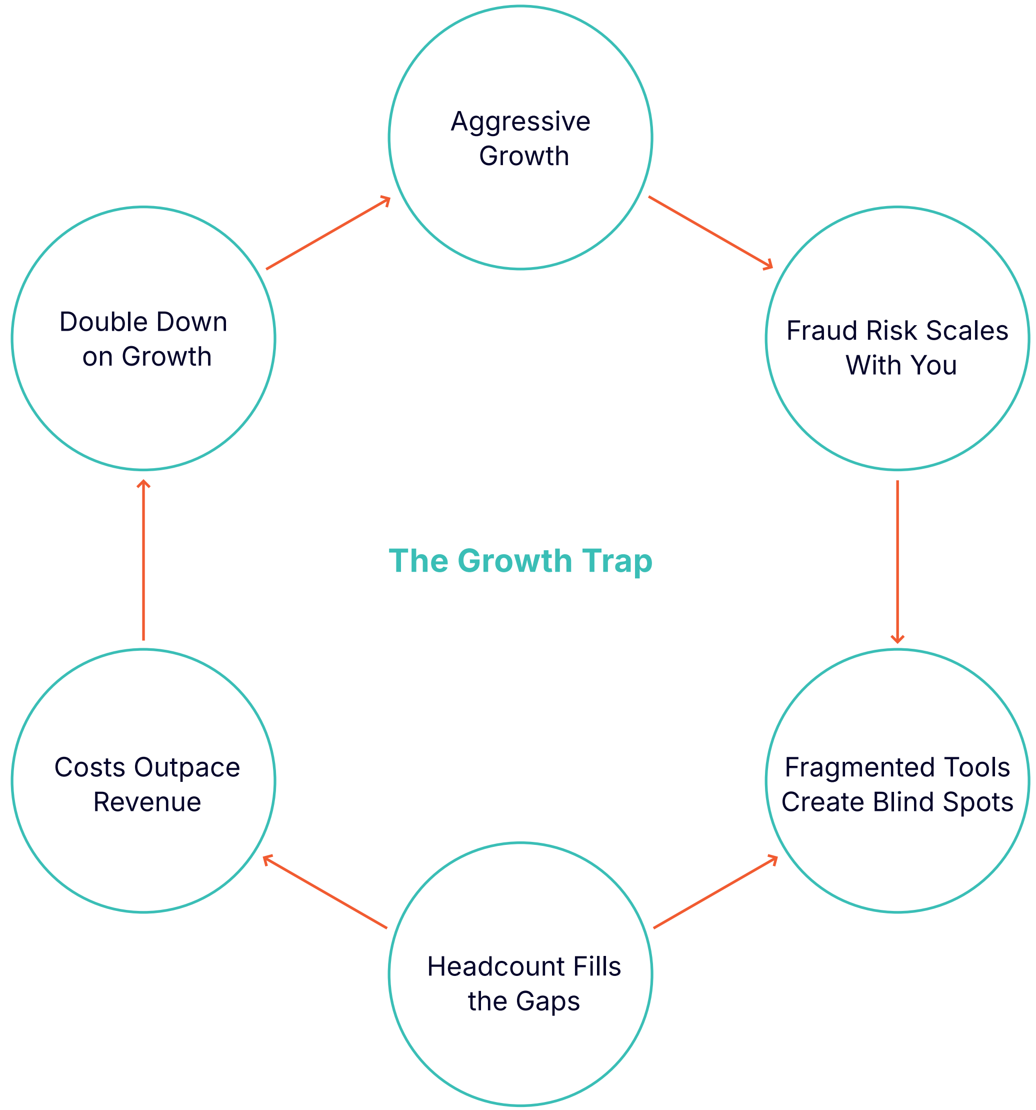
→ **Betting and gaming stands alone as the only industry in our survey where headcount investment leads AI/ML investment. Every other sector reverses this priority. Thirty-six percent of betting and gaming operators report false-positive rates of 26% to 50%. Every one of those false positives requires manual review by the people they just hired.**

Section 4

Breaking the Loop

The data in this report traces a single, self-reinforcing cycle. Aggressive growth creates fraud. Disconnected tools miss the signals. Operators hire more people to compensate for those blind spots. Fraud costs rise faster than revenue, squeezing the economics. To compensate, operators push even harder on growth. The cycle repeats.

Changing the sequence is the only way to break the loop. Operators must fix their foundational data architecture before attempting to automate or scale. Those who take these deliberate steps will not only reduce fraud losses but will transform their defense into a tangible competitive advantage.



Before rushing to scale, every betting and gaming fraud leader should be asking three questions:

→ **Is our data architecture as mature as our growth strategy?**

The gap between growth ambition and data readiness defines betting and gaming's vulnerability today. Unifying the data layer is the strategic prerequisite for everything that follows. A cohesive foundation lowers false positives, accelerates investigations and enables effective AI deployment — allowing teams to scale efficiently alongside the business.

→ **Are we investing in AI as a capability, or just consuming it as a feature?**

Most betting and gaming operators already use AI every day. However, relying on fragmented vendor data severely limits its potential. Strategic AI investment requires unified data; otherwise, siloed systems reduce AI to just another feature, yielding incremental improvements. A unified data pipeline, by contrast, delivers transformational results.

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

The headcount trap is a fully solvable challenge. Operators break the loop by consolidating tools, unifying data and building automation on that secure foundation. Forward-thinking teams don't just hire to survive; they build infrastructure that lets them compete fiercely on player experience and incentive generosity. Solid infrastructure transforms fraud prevention from a cost center into an engine for business expansion.

Get the Full Picture

This report covers the betting and gaming-specific findings from 332 fraud and AML leaders worldwide. For the complete analysis — AI adoption benchmarks, vendor ecosystem trends, investment forecasts and the full dataset from 1,010 respondents across betting and gaming, fintech, payments and retail — download the full report.

⟶ **Download the AI Reality Check: 2026 Fraud & AML Leaders Report**

⟶ **Talk to a SEON Expert**

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.