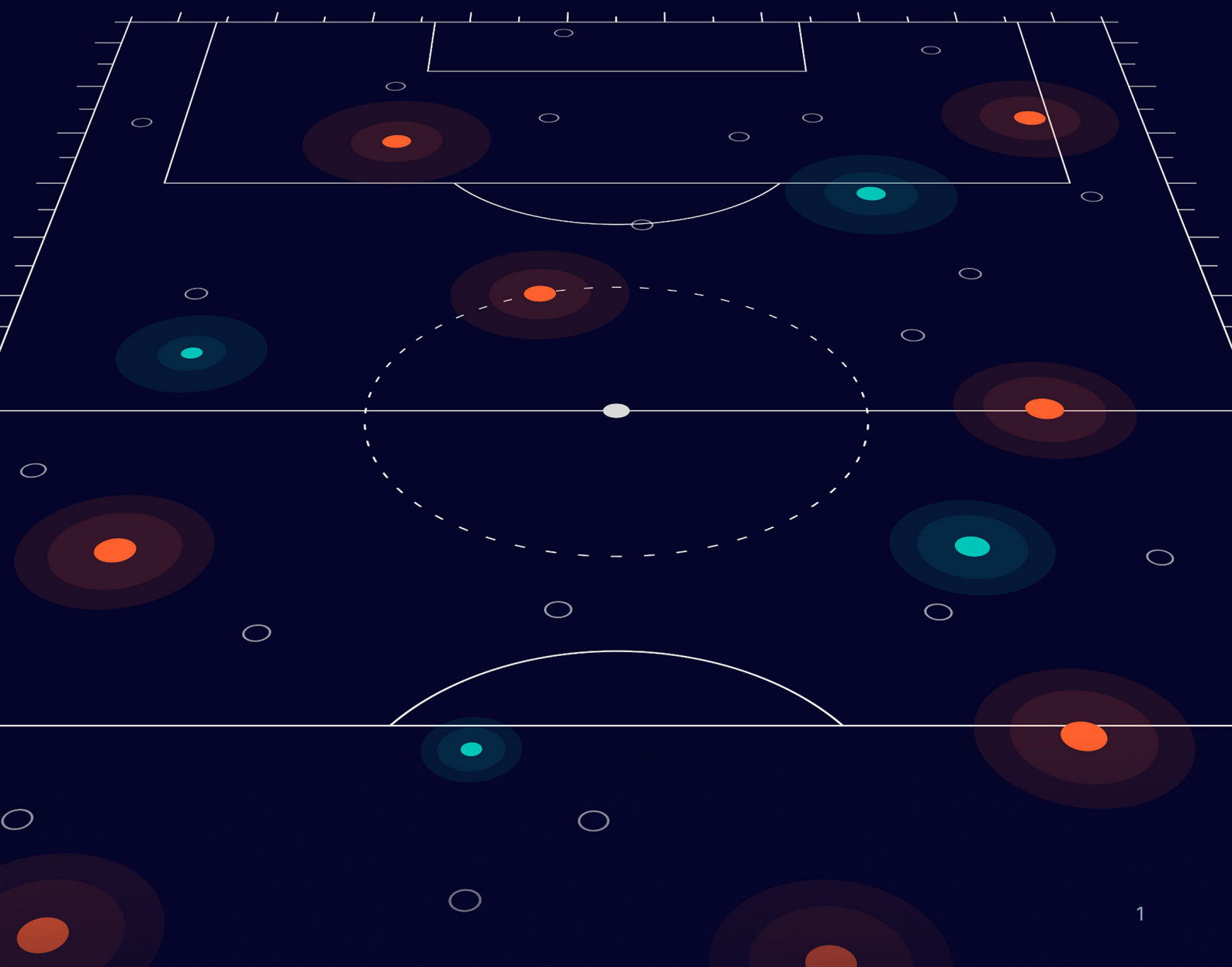
SEON

2026 World Cup Benchmarking Report

SEON INTELLIGENCE REPORT

SEON.IO



Multi-stage fraud exploited verified accounts, operators who saw the full picture made the save.

Operators eased registration controls to compete for players, and pressure concentrated at the exit. It moved through dormant accounts, past compliance controls and out through the cash-out.

This report benchmarks fraud pressure across six stages of the player journey, four regions and 19 risk metrics. Proprietary data from SEON reveals how the world's largest Betting & Gaming brands actually performed during the World Cup.

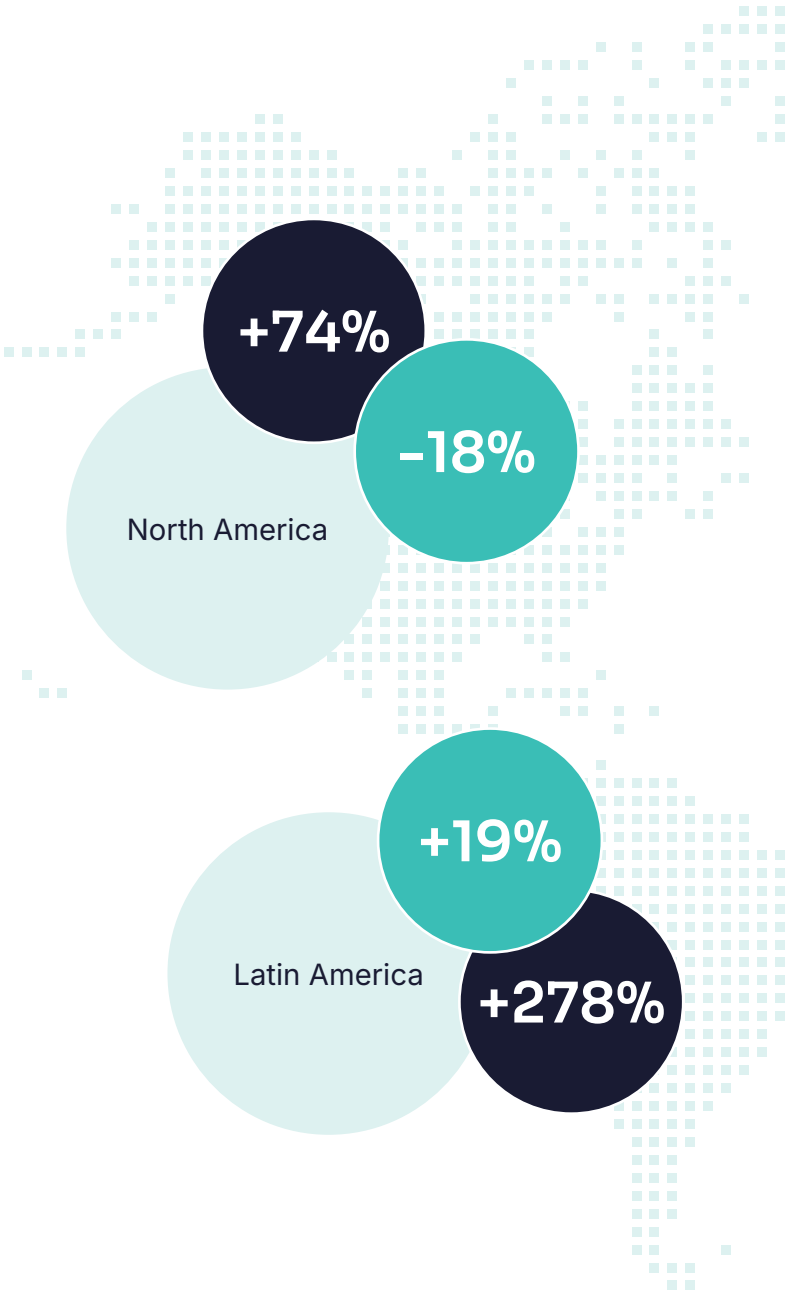
Table of Contents

Reading the Pitch

How fraud repositioned during the biggest event of the year. Every signal below was identified because a single platform connected the entire player lifecycle in real time. What disconnected tools miss entirely, operators on SEON's network caught and blocked.

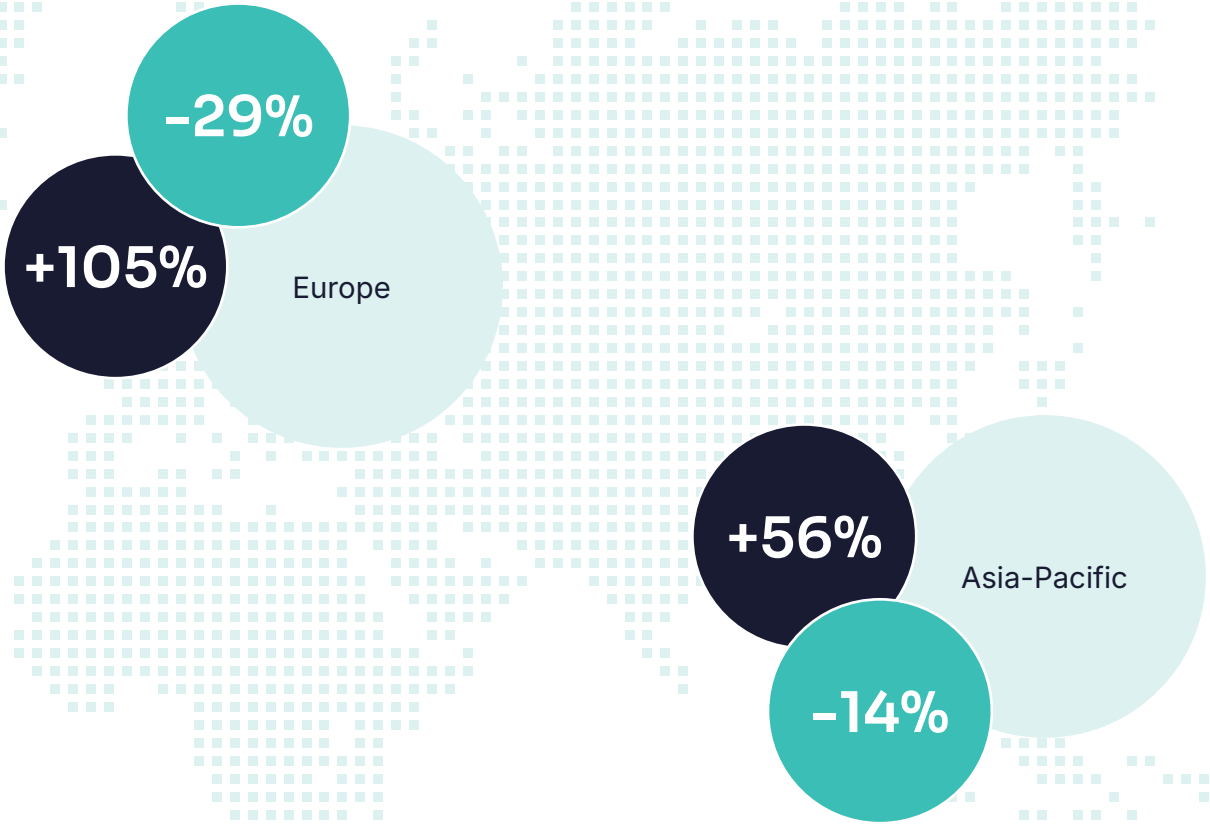
Registration Defenses Eased as Volume Surged

Registration volume more than doubled year over year (+121% globally), with Latin America nearly quadrupling (+278%). But block rates moved in the opposite direction. Operators in Europe (-29%) and North America (-18%) deliberately relaxed checks to avoid turning away players during the marquee event. Consequence played out downstream as losses mounted in stages that no registration metrics could track. Latin America was the exception: blocks rose 19% alongside that surging volume, confirming the region remained the primary target for industrial-scale identity fabrication.



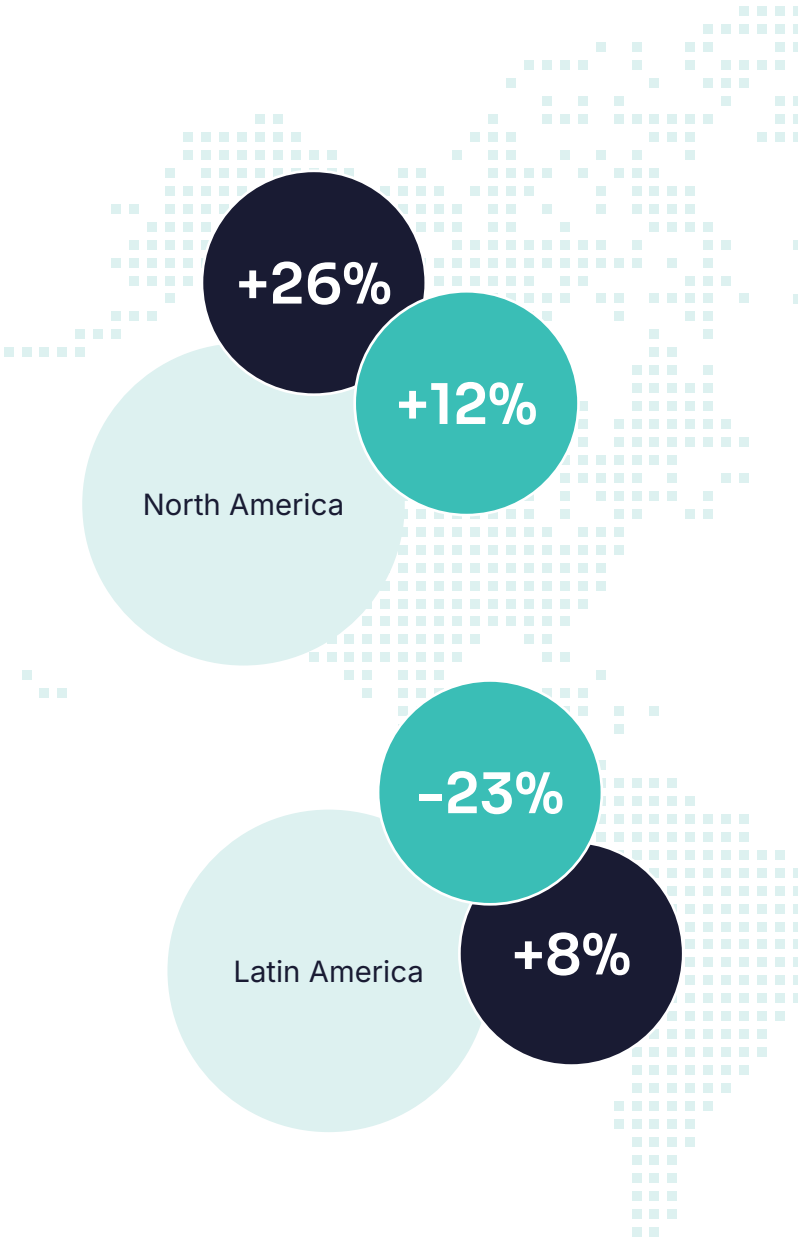
Registration Volume Change by Region (YoY)
Change vs 2025 same period | total registrations

Registration Block Rate Change by Region
Change vs pre-tournament baseline | per 1,000 registrations



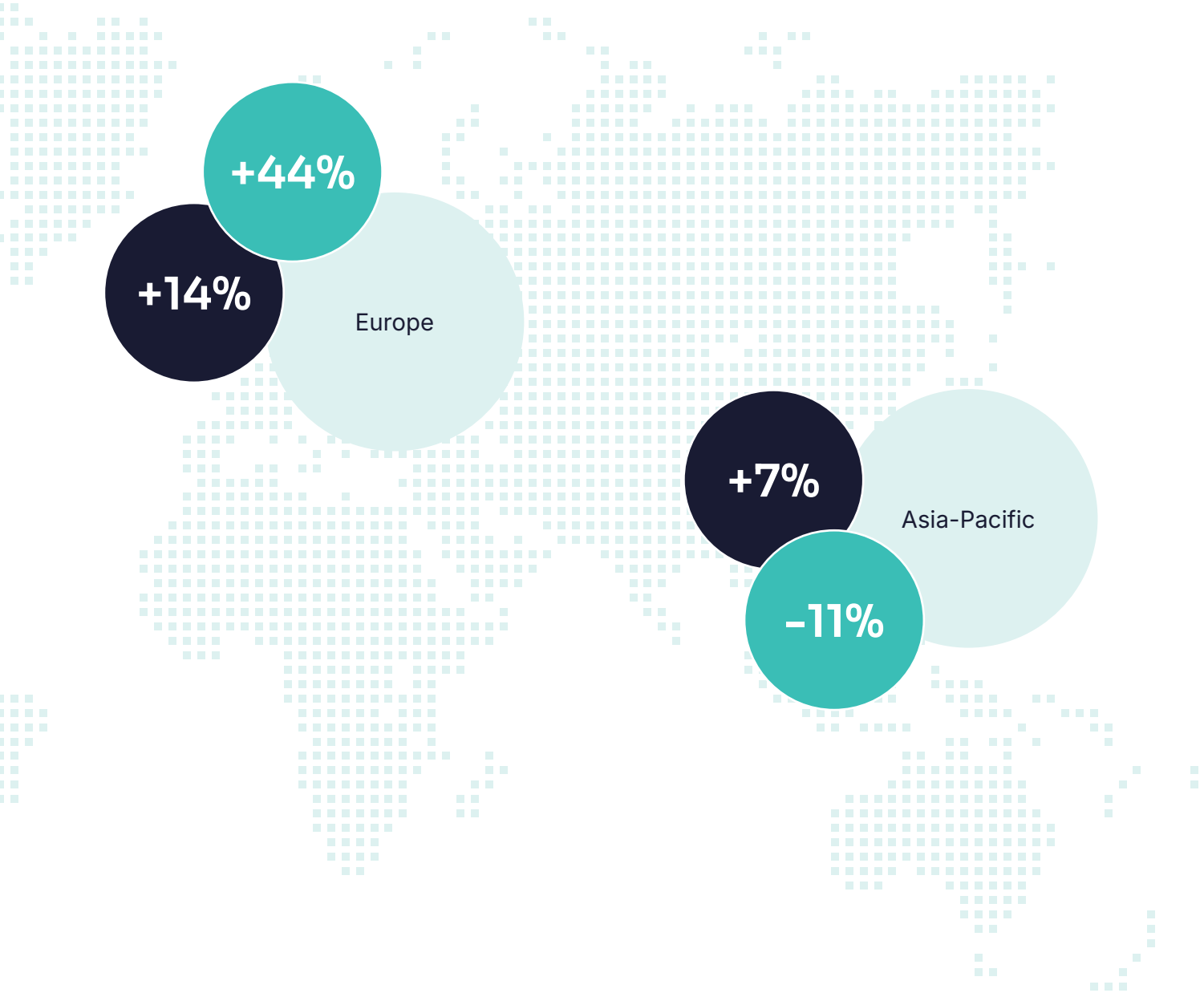
Dormant Accounts Became the Entry Point

While registration quieted, the real movement happened deeper in the player journey. Identity-mismatch signals rose 12% globally, and dormant accounts (inactive 90+ days) drove 83% more of the mismatch signal than during the baseline. These accounts were stolen through credential-stuffing, purchased on dark web marketplaces, or created months earlier and deliberately aged. Once activated, they present the same way: a previously verified account resurfacing on a new device in a new country, still carrying trust scores that no longer reflect reality. Every downstream action inherits that trust unchallenged.



Trusted Account Mismatches

Dormant Accounts Reactivated

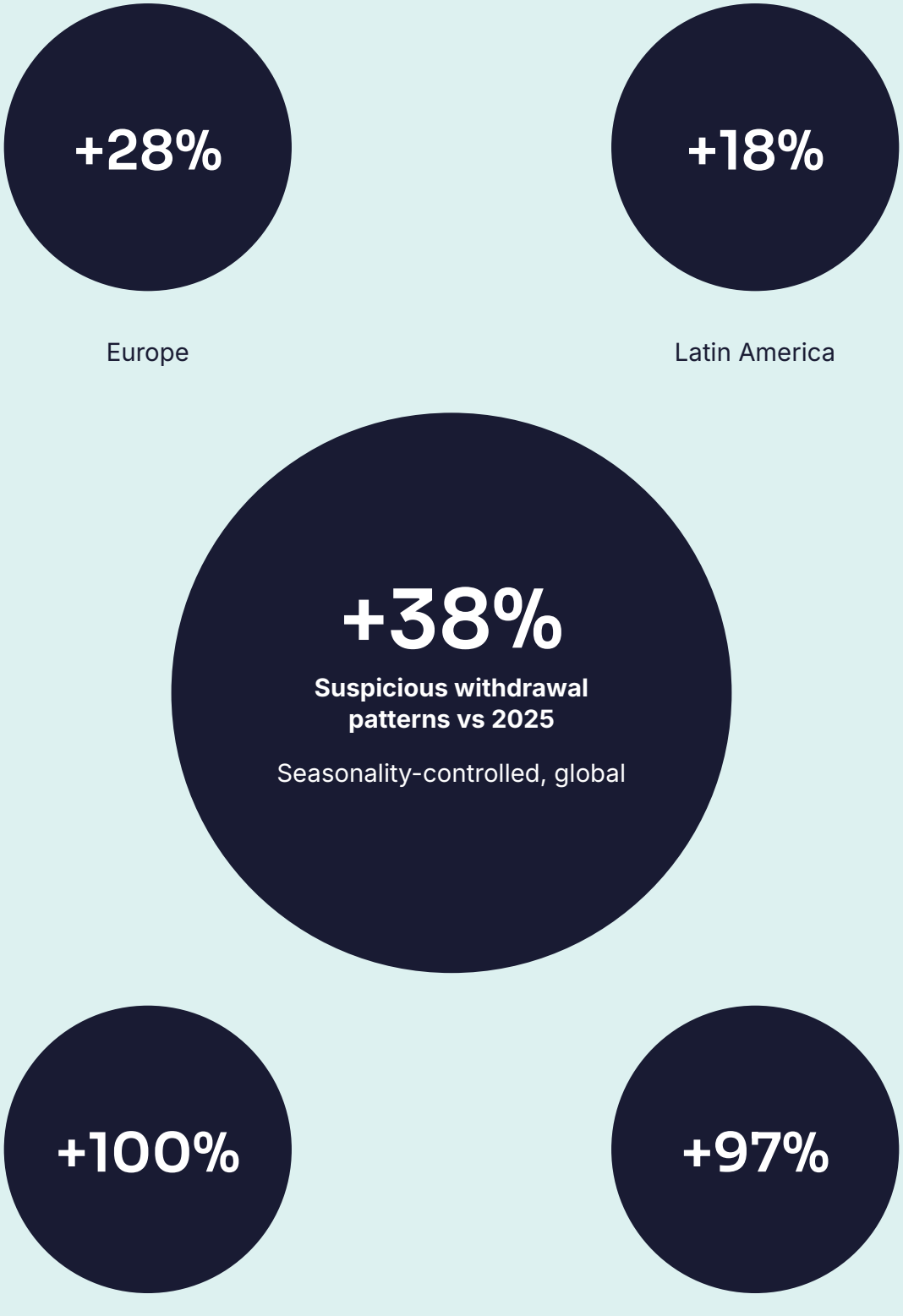


Every Region Converged at the Cash-Out

Suspicious withdrawal patterns rose in all four regions. The seasonality-controlled figure (+38% vs 2025) confirms this is a tournament effect, not a baseline artifact.

This is the most consistent finding in the data.

But the nature of the attempts changed — systems tuned for small withdrawals may not flag a single large withdrawal that looks like a normal high roller cashing out. There is no speed pattern to trigger. The dashboard reports improvement while actual losses climb.


+28%
Europe
+18%
Latin America
+38%
Suspicious withdrawal patterns vs 2025
Seasonality-controlled, global
+100%
North America
+97%
Asia-Pacific

Fewer Attempts, Higher Stakes

Fraudsters abandoned the old playbook of numerous small withdrawals spread out across time.

During the World Cup, they concentrated on single high-value attempts, betting that one big hit could clear before being noticed.

Avg blocked value doubled

$202 ↗ $436

-44%

fewer attempts per day
during the tournament

+21%

total value blocked rose
despite fewer attempts

No Single Stage Sees the Full Attack

Each signal below appeared at a different lifecycle stage and was monitored by a different team. None triggered an escalation on its own.

Europe: The Dormant Account Pipeline

Dormant accounts reactivated
An account that passed KYC two years ago wakes up on a new device in a new country. It looks like a returning player.

Trusted account mismatches
It clears the login because it has a history. It triggers an identity mismatch that gets lost in the noise of legitimate returning traffic.

Suspicious withdrawal patterns
Money moves at cash-out. One path, three stages, one operation.

Latin America: The Synthetic Pipeline

Synthetic-identity blocks
A fabricated identity passes registration. Your fraud team sees one more block in a tripled-volume queue. The ones that get through move within minutes.

Welcome-bonus abuse
Claimed the welcome bonus within minutes of account creation. Met minimum wagering with low-risk bets. The clock is already running.

Suspicious withdrawal patterns
The payments team saw +3%. No alert fired. The pipeline succeeded because the exit looked normal.

Both pipelines end at the cash-out. Three teams. Three queues. Three dashboards, each showing nothing worth escalating. The attack is invisible, not because your rules failed, but because no single team's view is wide enough to see a three-stage operation.

Regional Breakdown

How the global pressure shift is expressed differently across four regions.

Europe

Credential pressure and dormant exploitation

Europe saw the sharpest credential-layer pressure in the panel: brute-force attempts more than doubled (+115%), and dormant reactivations surged (+44%). Operators lowered the registration barrier to acquire players, and credential-stuffing campaigns exploited the same window. The timing was deliberate: peak tournament traffic is the moment security teams are most stretched. A valid credential paired with a clean device history is indistinguishable from a legitimate login. Every successful stuffing attempt becomes a downstream identity mismatch, a bonus claim, or a cash-out that the login layer already approved.

Brute force rate

Dormant accounts reactivated

Registration blocks

Trusted account mismatches

Latin America

Volume surge with targeted synthetic campaigns

Latin America was the only region where registration pressure rose. A 278% year-over-year volume surge brought targeted synthetic-identity campaigns (+34%) with it: synthetic ID at registration, welcome bonus claimed (+65%), cash-out attempt shortly after. Operators who cannot connect signals across the pipeline unknowingly fund fraud. Deposit controls held steady despite the volume surge, with rules scaling to match traffic.

Registration volume

Synthetic identity rate

Welcome bonus abuse

Deposits blocked

North America

Concentrated high-value extraction

North America saw login blocks double (+101%) and cash-out velocity triple (+202%). Declined withdrawal value rose 75%, meaning defenses caught the surge, and the average value per blocked attempt rose 73%. Velocity rules designed for rapid-fire patterns do not trigger on a single deliberate withdrawal from a compromised account with a clean history. The region's larger account balances and higher transaction limits amplify the impact of each successful attack. Deposit blocking rose 35%, showing end-to-end tightening.

Logins blocked

Suspicious withdrawal patterns

Blocked withdrawal value

Deposits blocked

Asia-Pacific

Rising bonus and cash-out pressure

Asia-Pacific is the fastest-growing region in the panel (+56% registration volume year over year). With that growth came rising bonus abuse (+68%) and cash-out pressure (+17% suspicious withdrawal patterns, +19% blocked withdrawal value), directionally consistent with the global pattern.

Registration volume (YoY)

Welcome bonus abuse

Blocked withdrawal value

Suspicious withdrawal patterns

Operator Variance

How do your controls compare to the panel?

Registration

(Europe)

METRIC

Registration Block Rate

Percentage of registration attempts blocked by fraud rules

The sharpest decline in the panel. Operators loosened registration deliberately. With aged credentials in hand, attackers had no need to create new accounts.

Synthetic Identity Rate

Percentage of registrations flagged as synthetic or fabricated identities

Fell sharply while Latin America surged +34%. Synthetic campaigns concentrated where document-verification requirements are less established.

False Positive Rate

Percentage of blocked registrations later confirmed as legitimate

Doubled from a low base. Tightened rules caught edge cases under pressure, not systemic over-blocking. Precision held for most operators.

BEST DEFENDED 25th pctl	TYPICAL 50th pctl	HIGHEST RISK 75th pctl	CHANGE
0.7%	1.0%	2.4%	-29% vs baseline
0.5%	0.66%	1.8%	-35% vs baseline
0.02%	0.07%	0.34%	+106% vs baseline

Login & Activity

(Europe)

METRIC

Login Block Rate

Percentage of login attempts blocked

Moderate rise, but the real story is brute force (+115%).
Successful credential-stuffing passes through without triggering a block.

Brute Force Rate

Percentage of users targeted by credential-stuffing or brute force attempts

More than doubled. Credential-stuffing campaigns timed to peak tournament traffic when security teams are stretched thinnest.

Dormant Accounts Reactivated

Percentage of active users who were dormant (90+ days inactive) and reactivated

The highest reactivation rate in any region. The +44% reactivation surge directly correlates with the +69% rise in dormant account mismatches, confirming the connection.

BEST DEFENDED 25th pctl	TYPICAL 50th pctl	HIGHEST RISK 75th pctl	CHANGE
0.52%	0.92%	2.56%	+12% vs baseline
1.2%	2.56%	3.2%	+115% vs baseline
7.8%	11.22%	14.1%	+44% vs baseline

Account Integrity

(Europe)

METRIC

Trusted Account Mismatches

Percentage of trusted logins showing device, location, or behavioral mismatches

The same accounts that reactivated are generating mismatches. Without re-verification, they look like returning players.

Mismatches From Dormant Accounts

Percentage of identity mismatches attributable to previously dormant accounts

Dormant accounts drive a growing share of mismatches. Without re-verification at reactivation, risk inherited from years-old checks compounds.

Shared-Identity Overlap

How many other accounts the average player is linked to through shared device, email, or phone signals

Europe’s lower baseline (0.5-0.9) compared to shared-device markets means any rise here is more likely to signal deliberate multi-accounting than organic device sharing.

BEST DEFENDED 25th pctl	TYPICAL 50th pctl	HIGHEST RISK 75th pctl	CHANGE
60.3%	69.0%	78.2%	+14% vs baseline
0.04%	0.10%	0.56%	+69% vs baseline
0.5	0.7	0.9	+28% vs baseline

Bonus Abuse

(Europe)

METRIC

Welcome Bonus Abuse

Percentage of bonus-eligible transactions flagged as welcome-bonus abuse

Narrow spread. EMEA's established velocity controls kept the ceiling low. The +6% rise is modest because effective controls were already in place.

Retention Bonus Abuse

Percentage of bonus-eligible transactions flagged as retention-bonus abuse

The -7.3% decline means attackers focused on welcome bonuses, not retention rewards. The spread reflects program generosity, not control quality.

Total Bonus Abuse

Percentage of all bonus-eligible transactions flagged for abuse (welcome + retention combined)

EMEA's existing controls held (-5.6%). The spread reflects program generosity more than control quality.

BEST DEFENDED 25th pctl	TYPICAL 50th pctl	HIGHEST RISK 75th pctl	CHANGE
0.8%	2.77%	5.2%	+6% vs baseline
12.1%	16.81%	55.1%	-7.3% vs baseline
14.2%	19.58%	56.6%	-5.6% vs baseline

Cash-Out

(Europe)

METRIC

Suspicious Withdrawal Patterns

Percentage of active users triggering withdrawal-velocity anomaly rules

Second-highest velocity pressure after NOAM. Confirms downstream extraction followed the credential and account-integrity pressure upstream.

Average Blocked Withdrawal Value

Average USD value per declined withdrawal attempt

Average per attempt fell as operators blocked more aggressively, catching smaller attempts alongside larger ones. The spread ($172 to $725) reflects wealth differences across European markets.

Withdrawal Block Rate

Percentage of all withdrawal attempts that are declined

Block rate declined despite rising velocity anomalies (+59%). Stricter jurisdictions maintain enforcement at the exit even under tournament pressure.

BEST DEFENDED 25th pctl	TYPICAL 50th pctl	HIGHEST RISK 75th pctl	CHANGE
2.4%	5.43%	7.1%	+59% vs baseline
$172	$316	$725	-9% vs baseline
0.4%	1.0%	2.5%	-33% vs baseline

Compliance & AML

(Europe)

METRIC

Deposits Blocked

Percentage of depositing users whose deposits were actively declined by the operator

Deposit controls held steady in EMEA despite rising velocity pressure downstream. The spread (2.1% to 7.8%) reflects jurisdictional differences in regulatory enforcement.

Politically Exposed Person Matches

Percentage of active users matching Politically Exposed Person screening lists

EMEA carries the highest absolute PEP match volume in the panel. The slight decline reflects stable screening against growing user counts.

BEST DEFENDED 25th pctl	TYPICAL 50th pctl	HIGHEST RISK 75th pctl	CHANGE
2.1%	5.18%	7.8%	-1% vs baseline
0.010%	0.015%	0.020%	-3% vs baseline

Practitioner Perspectives

In early 2026, we surveyed 332 Betting & Gaming fraud and compliance leaders about what they expected this year. They told us pressure was rising and their tools weren't keeping up. Then the World Cup happened, and the data confirmed they were right.

57%

of operators report fraud losses growing faster than revenue

These leaders reported this before the tournament started. The World Cup proved them right. Attack value doubled while volume dropped, designed to look normal at any single stage. Without an architecture that connects the full player journey, each successful attempt costs more while the dashboard reports fewer threats. That is how losses outpace revenue.

55%

say achieving data visibility across fraud and AML systems is extremely or very challenging

The attack path we observed during the World Cup crossed every stage of the player journey, from dormant reactivation to identity mismatch to cash-out. Operators using point solutions see each stage in isolation, a fragmented view where no single signal looks worth escalating. The operators who connected their data across the full journey saw one coordinated operation unfolding in real time.

34%

invest in AI/ML, compared to 57% in every other industry surveyed

Attack campaigns spiked and completed within hours, matching the rhythm of the match schedule. Operators with real-time automated decisioning caught them as they happened. Operators relying on manual review queues that take 24 hours to clear had no chance against campaigns that finished in four. The 23-point AI investment gap between Betting & Gaming and every other industry is not a strategic choice. It is the reason some operators are structurally unable to respond at the speed fraud now moves.

Source: 2026 Betting & Gaming Fraud and AML Survey: “Scaling Without a Safety Net” (n=332). Self-reported sentiment data from compliance, fraud operations and risk management leaders across EMEA, LATAM, NOAM and APAC. Presented separately from observed operator data.

What the Tournament Made Visible

These five patterns existed before the World Cup. The tournament just compressed them into 46 days, where they could no longer be ignored.

01 Measurement moved in the wrong direction.

Registration metrics improved. Cash-out blocked values doubled. If KPIs only cover the front of the player journey, teams report safety while pressure builds downstream. The operators that caught the shift were measuring value per block, not volume of blocks.

02 Dormant inventory is compounding risk.

83% more identity mismatches came from accounts that were inactive for 90+ days. These accounts carry the highest trust scores and the cleanest behavioral records. Every month, they sit unverified; their value to an attacker appreciates. Re-verification at reactivation is the minimum defensible position.

03 Fewer blocks does not mean fewer attacks.

Declined count fell 44%. Average blocked value rose from $202 to $436. Attackers shifted from volume to precision: fewer attempts, each one worth more. The operators measuring value per block caught the shift. The operators measuring volume of blocks did not.

04 Credential campaigns are timed to peak traffic.

Europe brute force surged +115% during peak tournament traffic. Attackers time credential lists to the moment player activity is highest and security teams are most stretched. Session-level device signals are the only control that scales with traffic without adding friction.

05 No single team sees the full sequence.

The dormant account that reactivates, the identity mismatch that follows and the withdrawal anomaly at cash-out are steps in the same path. Each team in the chain sees one step. The attack is only visible when data flows across stages in real time.

This is what SEON is built for.

The operators in this data who made the save weren't better staffed. They saw the full picture. The dormant reactivation, the identity mismatch and the velocity anomaly weren't three incidents. They were one attack path moving across three teams, each of which saw nothing worth escalating on its own.

SEON scores risk across every stage of the player journey in real time, on a single platform. When fraud repositions, the picture moves with it. Three blind queues become one connected attack path you can act on before extraction completes.

That visibility changes the economics of growth. When operators trust their defenses across the full journey, they can compete harder on player experience: more generous bonuses, faster withdrawals, stronger retention. Fraud control stops being the tax on growth and becomes what makes aggressive growth safe.

See where your own player journey is exposed.

Unlock the complete World Cup fraud dataset.
Scan to get the global report.

Speak with an expert

Appendix: Methodology and Limitations

About the Data

This report draws on two distinct data sources. Operator data captures observed fraud signals across SEON's network during the 2026 FIFA World Cup period. Survey data captures self-reported practitioner sentiment from the 2026 Betting & Gaming Fraud and AML Survey. These sources are presented separately throughout the report and are never blended.

PARAMETER	DETAIL
Panel	Curated network of Tier 1-3 Betting & Gaming operators across four regions (not an industry census)
Pre-event baseline	28 days immediately preceding tournament kickoff
Tournament window	46 days (full World Cup duration)
2025 control period	36 days, same calendar dates in 2025 (seasonality control)
Primary comparison	World Cup vs baseline (isolates tournament effect)
Secondary comparison	World Cup vs 2025 same period (controls for seasonality)
Units	All comparisons use rates per 1,000 of the relevant denominator unless stated otherwise
Currency	USD as reported, no FX conversion applied
Region	EMEA, LATAM, NOAM, APAC. For APAC, the pre-event baseline is the primary comparison; 2025 control data has limited coverage in this region.

Sampling Approach

The panel is a curated network of SEON-integrated operators, not a random sample of the industry. Results reflect the behavior of this specific cohort and should not be generalized to all Betting & Gaming operators without qualification. Panel composition skews toward mid-market and scaling operators in regulated jurisdictions.

All percentage changes reported in this study exceed the interquartile range of cross-sectional operator variance and are directionally consistent across at least three of the four measured regions.

Confidence and Precision

Percentages are rounded to whole numbers except where the sample genuinely supports decimal precision (e.g., rates per 1,000 with large denominators). PEP match rates are reported to additional decimal places because the absolute numbers are small and rounding would obscure meaningful movement.

Known Limitations

- NOAM figures reflect a market with fewer, larger operators and higher average account values. Regional benchmarks should be read with this market structure in mind.
- For APAC, the pre-event baseline is the primary comparison; 2025 control data has limited coverage in this region.
- 2025 login data captures IP signals only. Device-level comparisons are not available for the YoY control period, so login YoY figures are directional.
- LATAM YoY bonus comparisons are confounded by a program rollout between 2025 and 2026. Use baseline only.
- A device or location mismatch is a change in access pattern, not a proven compromise. “Identity mismatch” is used throughout; “account takeover” is not claimed.
- Some global averages reflect composition effects from LATAM’s growing panel share. Where a global figure diverges from regional trends, the regional figures are the more accurate read.
- Sanctions matches (5 to 9 globally) are too sparse for rate-based analysis. Reported as absolute counts only.

Rate Normalization

All cross-window comparisons use rates (per active user or per 1,000 of the relevant denominator) to normalize for volume differences between operators and regions. Where baseline and seasonality-controlled figures diverge, both are presented. The seasonality-controlled comparison (+38% vs 2025) isolates tournament-driven effects from normal seasonal variation.

Survey Methodology

The 2026 Betting & Gaming Fraud and AML Survey was conducted among 332 practitioners across compliance, fraud operations and risk management roles. Respondents represent operators across EMEA, LATAM, NOAM and APAC. The survey was fielded in Q1 2026. Results are self-reported and may reflect perception bias.

The AI Command Center for Fraud Prevention & AML Compliance

SEON.IO