SEON

Global iGaming Risk & Fraud Report

Leading Global Fraud Prevention and Compliance

SEON.IO

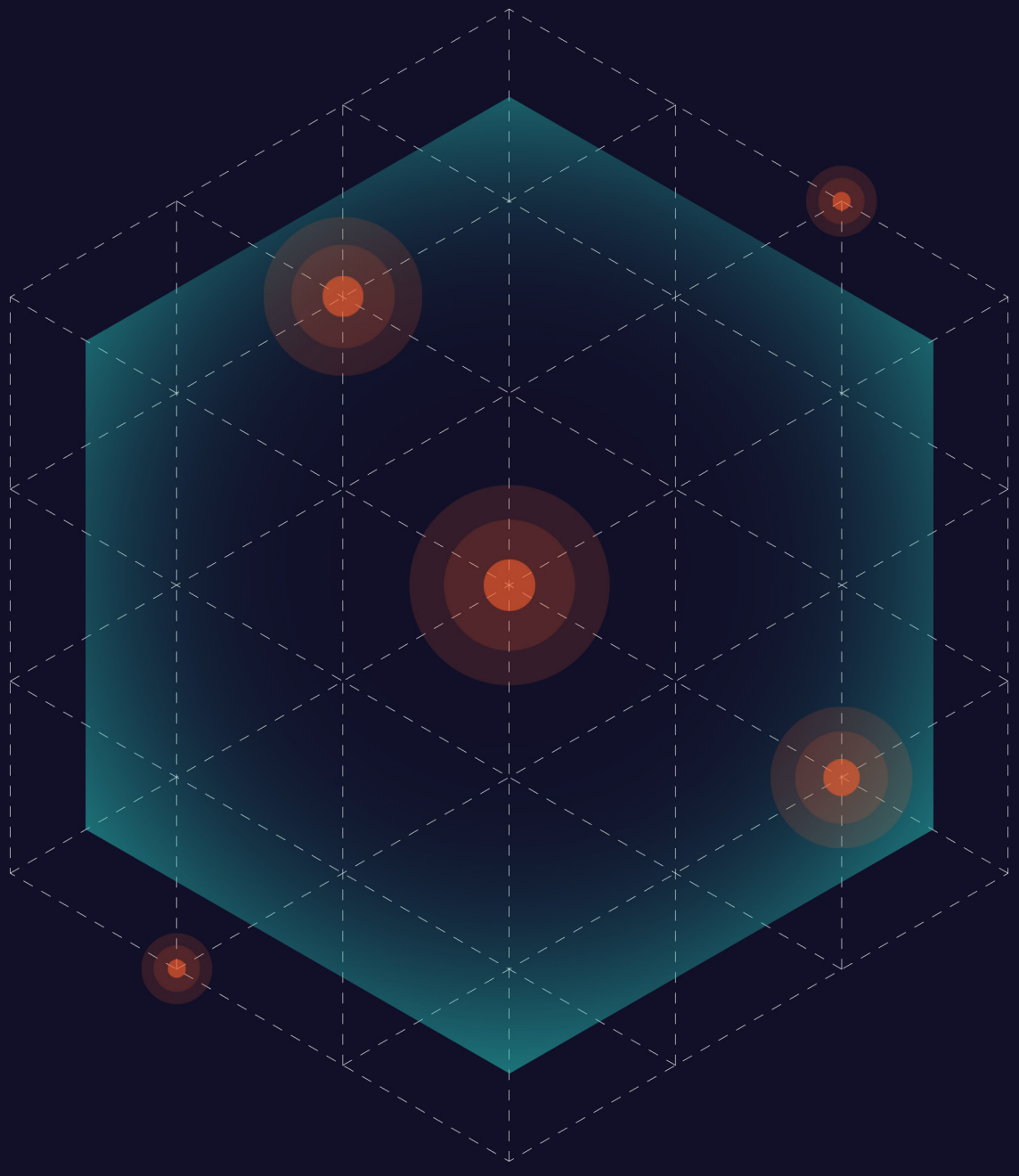


Table of Contents

The Evolution of Modern iGaming Fraud

As the leading solution for fraud, risk and compliance in the iGaming industry, SEON protects the world's most successful operators. This report is based on exclusive data from our global network, revealing the real-world fraud patterns and attacks we have observed over the past year. By examining data from top operators, we can illustrate exactly how fraud evolved — moving away from simple bot attacks toward more sophisticated and organized deception.

This report serves as your guide to the 2026 risk landscape. We explain how the world's leading brands have updated their security to stop these new threats while continuing to grow. These insights will help you understand the current market and ensure your business is prepared for the sophisticated fraud challenges coming in the year ahead.

Who You're Up Against

Fraudster Threat Profiles

The Career Professional

Threat: High

They treat iGaming platforms as recurring revenue sources, focusing on systematic bonus abuse. Their goal is to maximize the lifetime value of their account clusters.

Synthetic Scalability

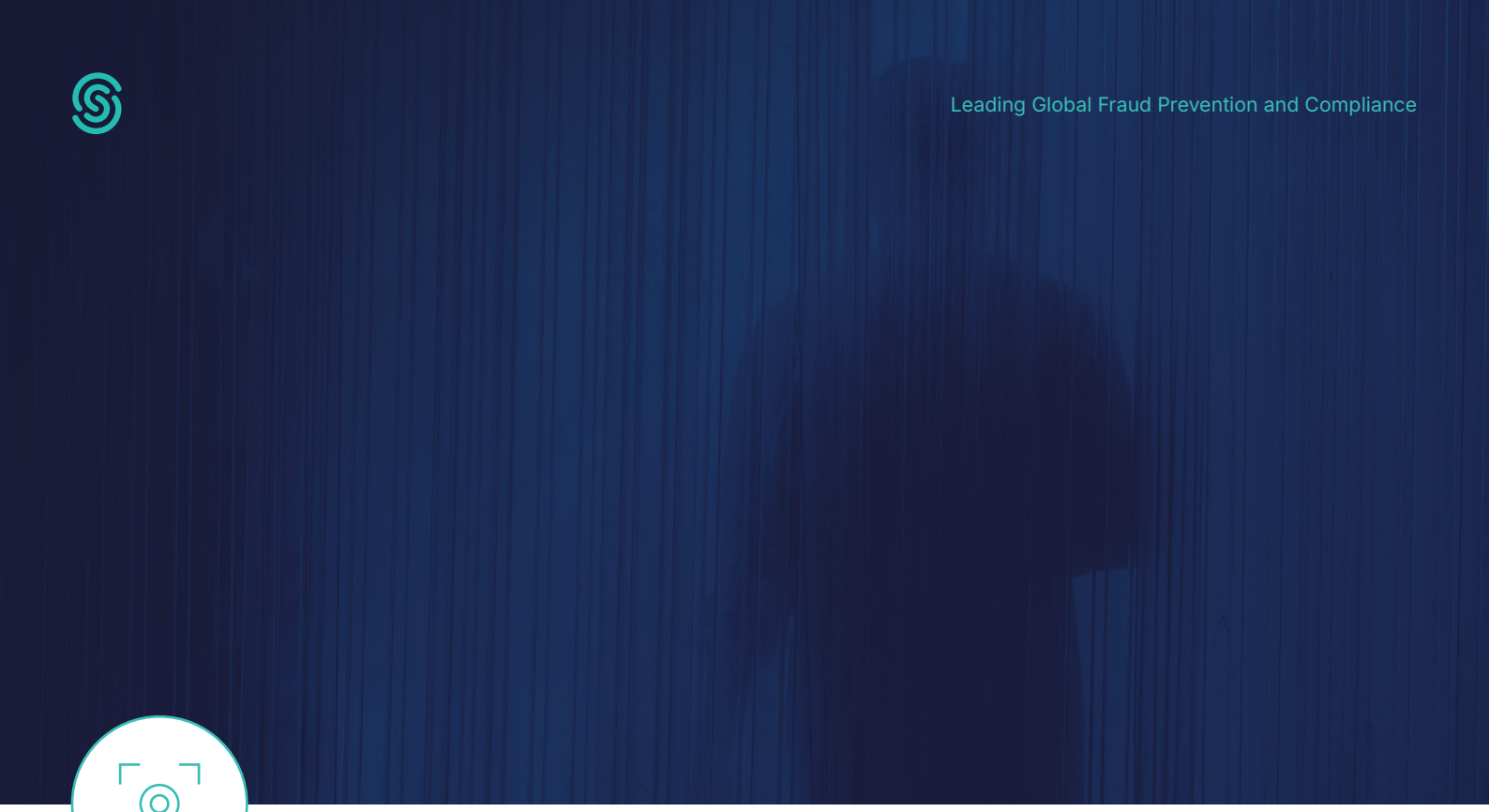
Manages massive account clusters using virtual machines and emulators; neutralized by identifying missing hardware data and reused device IDs

Automated Consistency

Utilizes automated scripts to maintain scale; behavioral monitoring exposed the inhuman consistency of their password entry patterns

Identity Gaps

Leverages synthetic identities that were blocked for lacking the credible, multi-year history found in legitimate player profiles



The Sophisticated Fraudster

Threat: Medium

Highly technical attackers using expensive tools to execute high-quality deception. This is the fastest-growing threat category, focusing on bypassing biometric security and taking over high-value accounts. They invest in unique hardware and residential proxies to evade standard detection.

Hardware Spoofing

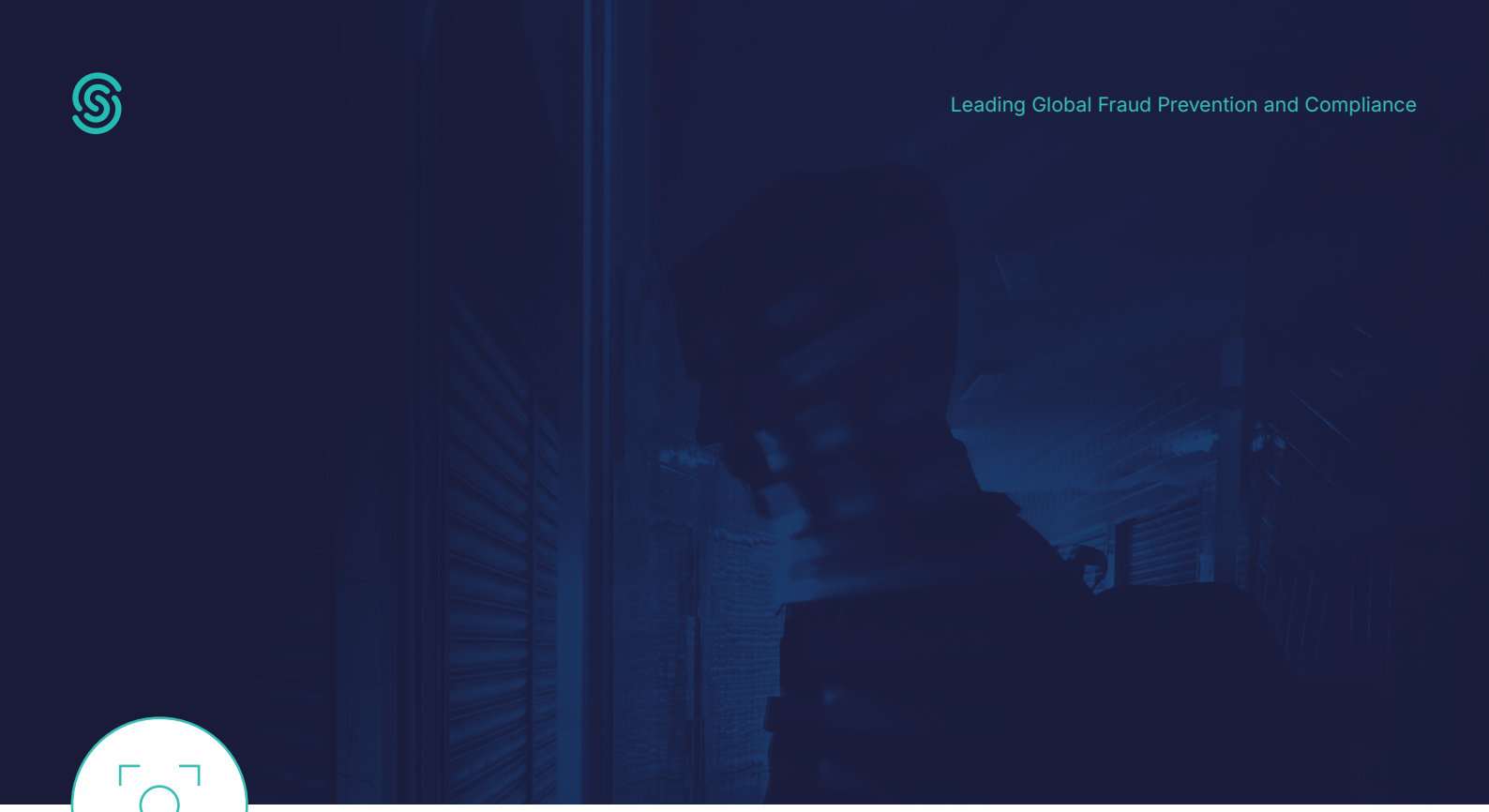
Uses fresh mobile devices to simulate new users; flagged by integrity checks for lacking the organic usage noise of a real device

Footprint Failures

High-cost concealment attempts fail because the identities lacked verified digital footprints on external platforms

AI Manipulation

Deploys Generative AI to create deepfakes, attempting to bypass liveness verification and selfie-based onboarding gates



The Opportunistic Amateur

Threat: Low

Individuals following “easy money” guides to exploit welcome offers. Lacking strategy, they use their own valid credentials for a one-time cash grab. Since the identity is real, they bypass fraud filters, extracting value and churning immediately.

Clean Digital History

Leverages primary personal accounts with legitimate history to bypass standard risk triggers

Residential Visibility

Connects via unmasked residential networks that appear identical to legitimate local traffic

Negative Revenue Churn

Extracts the maximum bonus value and immediately abandons the account without generating revenue

Trends Across Leading Operators

The Professionalization of North & Latin American Fraud

Fraud in the Americas has shifted from high-volume automation to high-fidelity deception. As syndicates adapt technical profiles to bypass legacy controls, effective defense now requires multi-signal alignment across the entire player journey.

North America

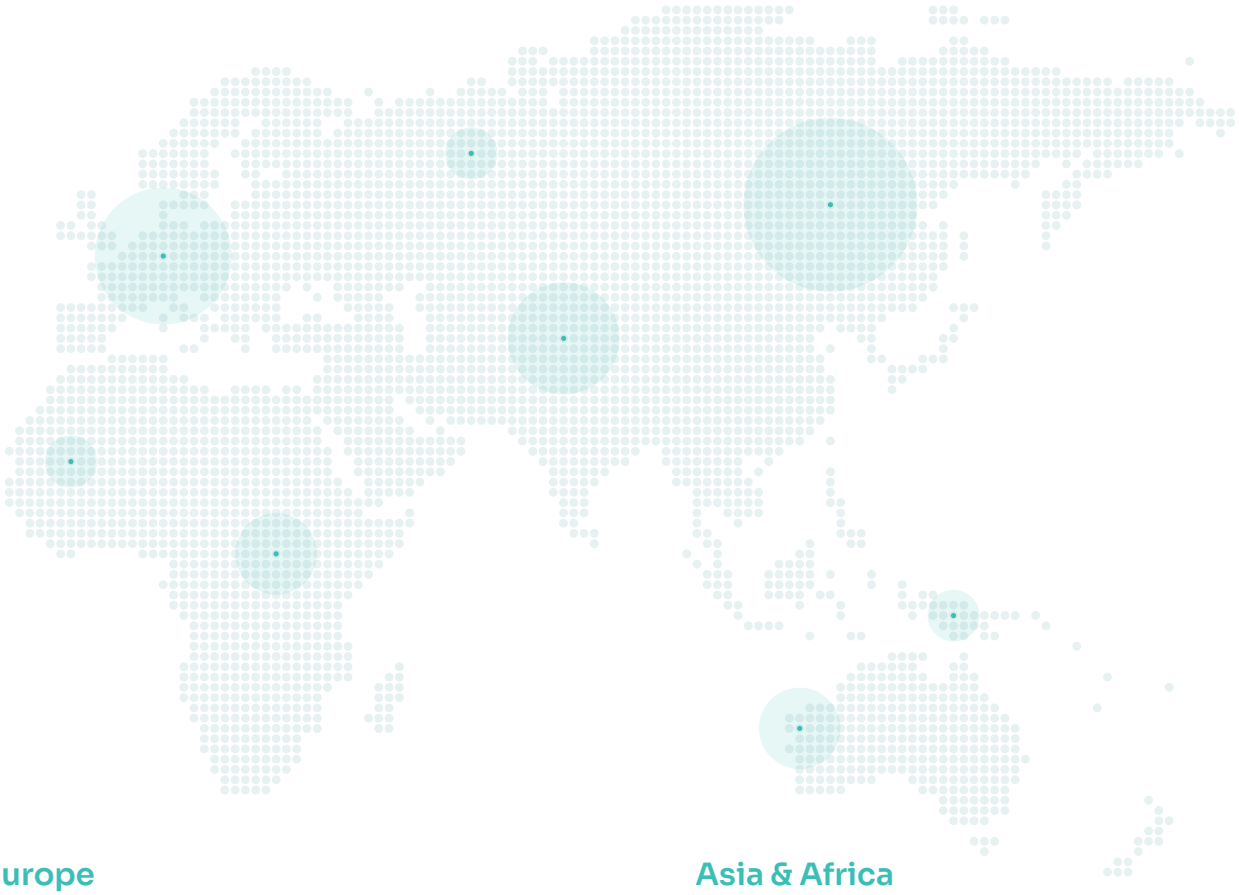
- Effective defense required multi-signal alignment, verifying the device, IP address, phone number and email together at all touchpoints
- Fraudsters linked single social media profiles to fake accounts to build a digital history and camouflage trust signals
- ATO tactics shifted from simple cookie-stuffing to more sophisticated techniques

Latin America

- Fraudsters attempted to bypass new account security filters and KYC gates by linking social footprints to their registration email
- Attackers in Brazil failed to hide their devices and were caught reusing the same device IDs across different platforms
- Fraud traffic migrated from static datacenters to residential proxy networks and mobile botnets for an attempt at better anonymity

Advanced Exploitation Across EMEA and APAC

The shift toward high-ROI, surgical attacks in EMEA and APAC prioritizes the hijacking of aged, verified profiles over new account creation. By leveraging residential connections and domain aliasing, syndicates attempt to bypass legacy filters. Neutralizing these threats requires enforcing 1:1 data alignment to break the economic viability of professional brute-force operations.



UK & Europe

- Fraudsters surgically targeted premium accounts with brute-force attacks to exploit high-value verified users
- Operators stopped botnets by enforcing 1:1 data alignment across device, location and contact info
- Instantly blocking repeated failed login attempts made attacks too expensive for fraud rings to sustain at scale

Asia & Africa

- Bot traffic moved to residential home internet connections to bypass standard geographical blocking tools
- Fraudsters used automated scripts to mass-register high-trust email domains, utilizing aliases to bypass reputation checks
- Sophisticated attackers prioritized hijacking existing verified accounts because it required less effort than creating new fake identities

The Targeted Theft of Trusted Accounts

As synthetic identities become increasingly difficult to generate, fraud rings have shifted their focus to stealing high-value accounts. This forces a change in defense: operators must move beyond checking "Who are you?" at signup to continuously asking "Are you still the same person?"

Dormant Account Abuse

The most sophisticated attack vectors utilized sleeper cell tactics to exploit the trust granted to inactive accounts. Fraudsters acquired aged, verified profiles and intentionally maintained dormancy to bypass standard risk observation windows. Once off the radar, they claimed high-value retention bonuses, bypassing the security checks reserved for new players.

Authentication Anomalies

Previously verified accounts were suddenly accessed through unrecognized devices or foreign IP addresses, signaling a clear credential compromise.

Velocity Anomalies

Historically dormant accounts abruptly shifted into aggressive, high-frequency transaction patterns after months of inactivity.

Systemic Vulnerability

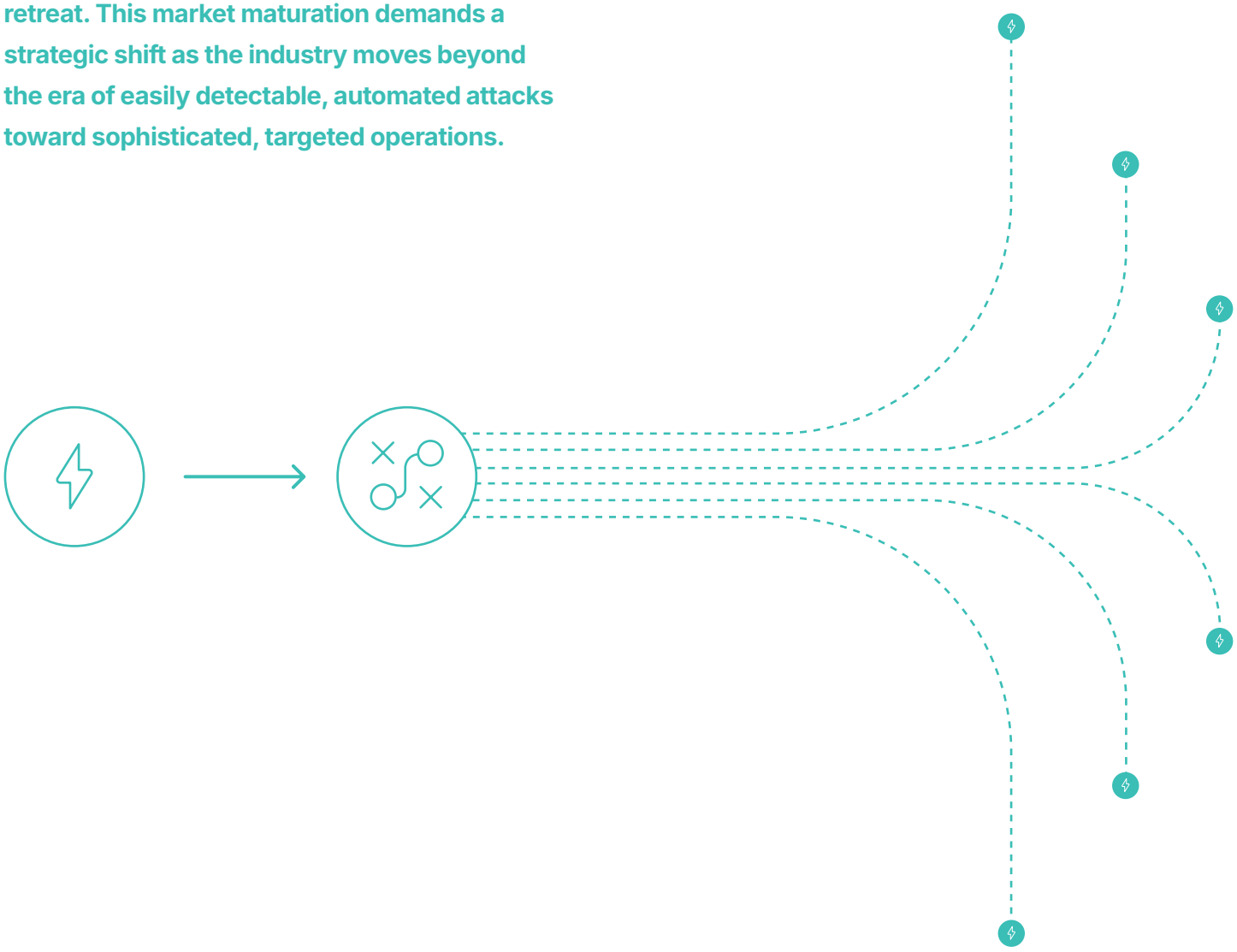
Attackers focused on exploiting established trust rather than attacking the signup gate. This rendered traditional identity checks ineffective because the account was already "verified."

Trust as the Trojan Horse

The hijacking of aged accounts has surged because it is more efficient to steal established trust than to build and "age" synthetic identities. This shift is driven by the high ROI of retention bonuses, which are often more lucrative than welcome offers. Legacy defenses fail because they do not monitor the abrupt behavioral pivot from dormancy to high-velocity engagement. To neutralize this, leading operators have implemented dynamic rules targeting unrecognized devices and IP shifts during the bonus-claim stage. This ensures that "trusted" status is not used as a mask for abuse, protecting both operator margins and player trust.

Fraudsters Aren't Getting Lucky, They're Getting Smarter

Year-over-year analysis confirms a decisive trend: low-effort fraud methodologies are in retreat. This market maturation demands a strategic shift as the industry moves beyond the era of easily detectable, automated attacks toward sophisticated, targeted operations.



The Decline Of The Naive Attacker

A consistent reduction in legacy fraud triggers at registration and login signals a more critical threat: sophisticated, intentional fraud targeting high-value abuse vectors. The retreat of the amateur is confirmed by the sustained decline in these key indicators:

Basic Multi- Accounting

Significant drops in the reuse of cookie hashes, email addresses and usernames at login. Amateur fraudsters abandoned platforms when basic techniques failed.

Basic Session Indicators

Fewer accounts presented multiple unique IP addresses within a 24-hour window. Multi-session attacks became economically non-viable.

Identity Signal Omissions

Reduced registration attempts characterized by missing device details or identity signals. Incomplete profiles are now immediately flagged and blocked.

The Easy Money is Gone

The retreat of low-effort fraud confirms that legacy triggers — such as cookie and IP anomalies — are no longer the primary battleground. As the market matures, the absence of amateur “noise” signifies that remaining threats are exclusively high-value, professional syndicates. Operators must now pivot from high-volume filtering to high-fidelity intelligence that targets intentional hardware and identity deception. By reallocating resources toward these sophisticated vectors, operators can neutralize professional-grade fraud before it impacts the bottom line.

Exponential Rise in Connected Abuse

High-impact threats are now defined by their ability to camouflage across the entire player lifecycle. Professional fraud rings maximize their ROI by exploiting data silos between disconnected point solutions. By unifying intelligence from registration to withdrawal, leading operators have moved beyond basic filtering to neutralize these sophisticated, cross-channel attacks.

Advanced Network & Proxy Mitigation

Traditional IP blocking is insufficient against modern residential proxy networks. By pairing true device IDs with connection metadata, operators expose hidden hardware patterns and pinpoint masked locations that standard network analysis misses.

Multi-Signal Footprint Analysis

The combination of device intelligence with email and phone analysis has proven to be the most effective defense against fraud rings. By cross-referencing these signals with social and digital indicators, operators achieve invisible validation—instantly distinguishing real individuals from synthetic profiles.

Behavioral Identity Mapping

Attackers deliberately cloak identities during high-value withdrawal attempts. By pairing device intelligence with behavioral monitoring, operators can link related accounts and identify clusters of abuse before financial value is extracted.

Bonus abuse has evolved into a high-tech arms race

The rise in linked account clusters proves that professional attackers are no longer targeting a single stage, but are camouflaging their activity across the entire player journey. To win this race, operators must move toward a unified platform that deploys device intelligence and digital footprint analysis from the initial sign-up through the withdrawal stage. This proactive, connected approach closes the technical gaps used by syndicates and removes the incentive for abuse. By securing the player journey, operators gain the confidence to offer more generous promotional offers, directly converting blocked fraud into increased total player value.

The Command Center for iGaming Fraud & Compliance

In the high-stakes world of betting and gaming, your growth is only as strong as your data. Most operators are unknowingly fighting modern fraud with recycled, resold and stale signals that legacy vendors simply repackage. Stop relying on dated information and start leading with precision. SEON provides the industry's most powerful command center for fraud prevention and AML compliance, built on the 900+ proprietary, first-party risk signals.

900+ Proprietary Data Points

Collecting and enriching first-party signals in real time gives you a critical edge in accuracy, revealing intent, detecting patterns, and surfacing anomalies.

Transparent Risk Decisioning

Full visibility into risk scoring with explainable AI signals. Combine AI insights with unlimited custom rules to match your exact risk appetite.

14-day Implementation

Go live in 14 days with one API and 240+ prebuilt rules. Start delivering results from day one and adapt quickly to new markets and regulations.

Deep iGaming Expertise

Fraud-focused experts who live and breathe iGaming threats work alongside you to optimize detection, tackle emerging attack patterns, and scale defenses as your business grows.

Trusted by the World's Most Ambitious iGaming Brands

→

32x ROI:

Lottoland

Lottoland leveraged SEON to safeguard marketing spend and eliminate bonus abuse at scale to unlock ROI.

→

40% Reduction in Manual Queries:

soft2bet

Soft2Bet automated risk reviews, enabling their team to focus on high-value players instead of chasing false positives.

→

20% Efficiency Gain:

BETFLAG
THE TOP OF GAMES WELCOME!

Betflag used SEON's real-time signals to fight bonus abuse while keeping the player journey frictionless.

Stop Fraud. Not Growth.
Ready to take command?

Scan to see why the world's leading iGaming brands choose SEON.