SEON

GUIDE

The Rising Tide of iGaming Fraud: Prevention, Detection & Competitive Advantage

Leading Global Fraud Prevention

SEON.IO

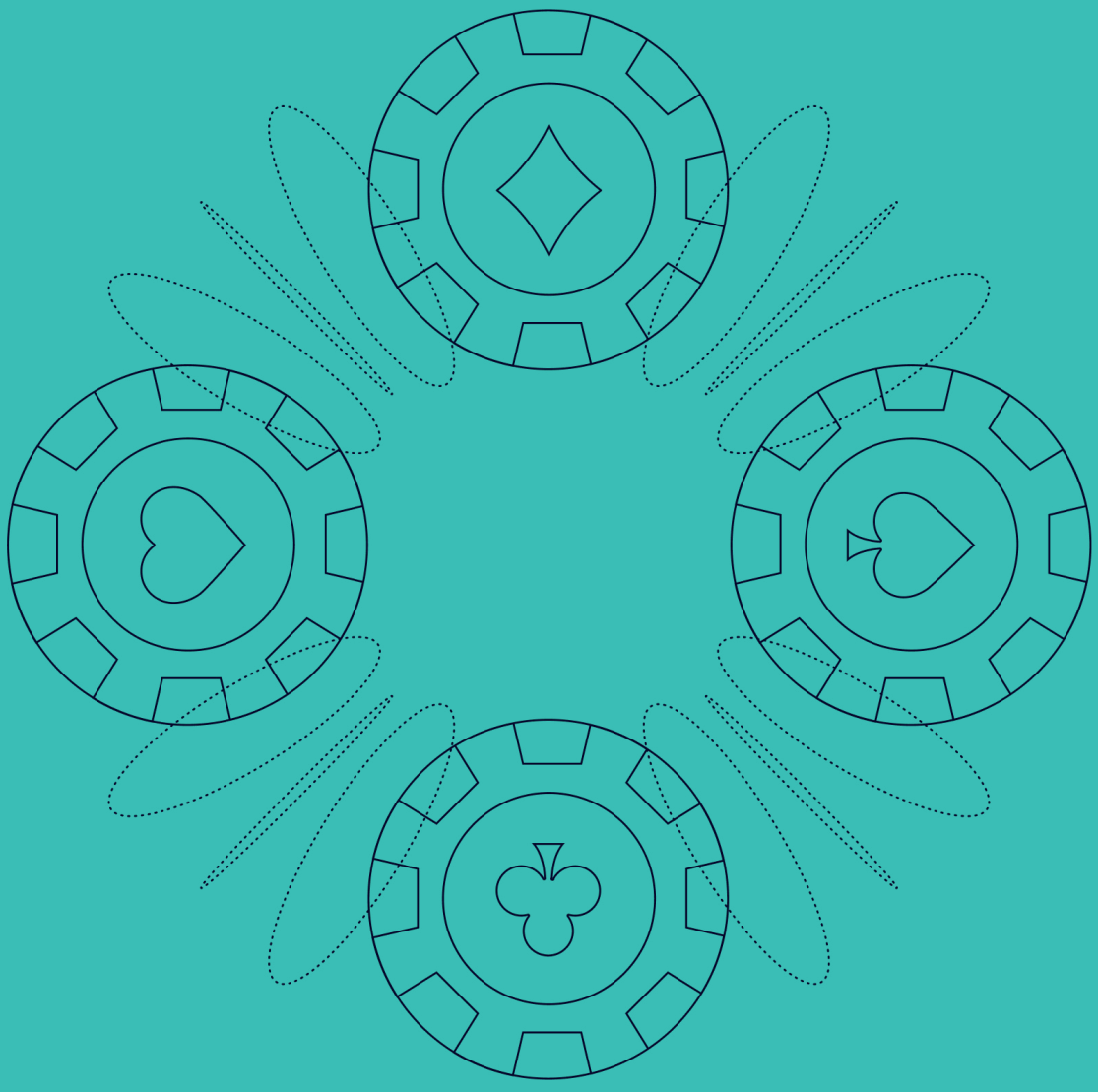
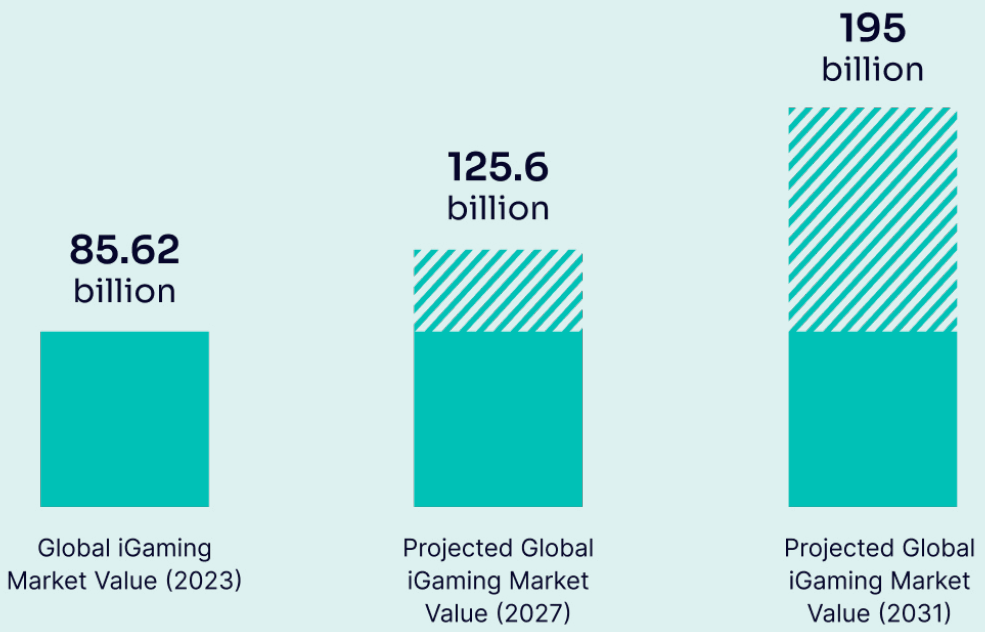


Table of Contents

Introduction

Fraud in the iGaming industry is escalating at an unprecedented rate, threatening operators' profitability, compliance and customer trust. **As the market surges toward a projected $195 billion by 2031[1], fraud incidents have risen 64% year-over-year from 2022 to 2024[2].** The conventional approach — focusing solely on fraud detection — is no longer sufficient in the current landscape. To mitigate risk, operators must embrace a proactive, multi-layered fraud prevention strategy that identifies threats at every stage of the customer journey while maintaining a seamless player experience.

SEON differentiates itself by integrating prevention and detection into a unified fraud-fighting approach. Unlike competitors that focus only on stopping fraud after it has already infiltrated the platform, SEON's real-time monitoring, AI-driven risk scoring and digital footprint analysis stop fraud at the earliest possible stage while continuously adapting to emerging threats. This dual-layered approach ensures operators can combat fraud across the player journey, from onboarding to transaction monitoring.



1 iGaming Industry Growth: Key Statistics and Trends

2 What To Expect From iGaming in 2025?

Multi-Layered Fraud Prevention: Defense at Every Stage

1. Stopping Fraud at Registration: The First Line of Defense

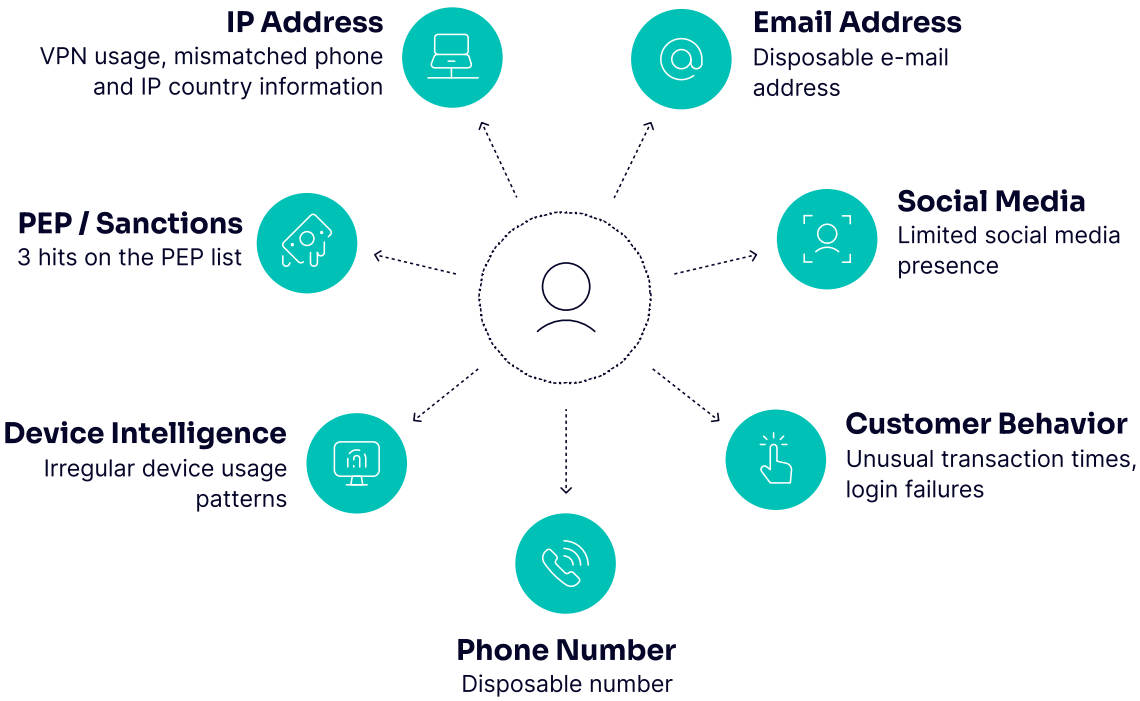
The most effective fraud mitigation strategy is identifying and blocking fraudulent users at the point of entry, minimizing exposure and reducing the risk of chargebacks, bonus abuse and account takeovers. At the registration stage, operators have an opportunity to filter out fraudulent users before they cause any harm — without disrupting the experience of legitimate players.

Digital Footprint Analysis: Spotting Fake Users Before They Gain Access

SEON goes beyond standard email and phone verification by analyzing thousands of digital and social signals to asses user legitimacy. By evaluating a user's broader online presence, SEON can identify disposable emails to discern if an email is legitimate or fake, phone numbers with no digital history and geolocation mismatches, such as mismatched country codes and IP addresses — all common indicators of fraudulent intent. This helps operators detect multi-accounting and synthetic identities, major tactics used to exploit promotions and bonuses. Inconsistencies in user details, such as variations in names and addresses, can also signal bot activity or synthetic identities. A significant advantage of digital footprint analysis is its role in preventing bonus abuse, a common fraud tactic where users create multiple accounts to exploit promotional offers.

Device Intelligence: Unmasking Fraudsters and Detecting Hidden Connections

SEON's device intelligence technology flags users attempting to mask identities through emulators, virtual machines and



device spoofing. By analyzing the hardware and software configurations, SEON detects irregularities that indicate fraudulent activity. Another core element of device intelligence is its ability to identify related accounts through common devices. This not only blocks new fraudulent accounts from being created, but it also flags accounts that are already on a platform and linked to known fraud patterns, allowing for early intervention.

IP analysis further strengthens fraud prevention by pinpointing geolocation mismatches, detecting users hiding behind proxies or VPNs, and flagging IP addresses with a history of fraudulent behavior. Operators leveraging SEON's device and network intelligence have reported massive reductions in multi-accounting attempts.

2. Real-Time Monitoring: A Continuous Layer of Protection

Even with strong entry-point defenses, sophisticated fraudsters may still find ways to bypass initial safeguards. That's where continuous transaction and behavior monitoring becomes a crucial component of a defense-in-depth (DiD) anti-fraud strategy. By implementing real-time monitoring across the entire player journey, operators can ensure that fraudulent activity is identified and intercepted before it escalates into financial or reputational damage.

Detecting Anomalies Before Fraud Happens with Behavioral Analytics

Suspicious behavioral patterns such as irregular betting activity, account takeovers and coordinated fraud rings can be caught using customizable velocity rules set to detect high-frequency actions, such as multiple logins from different locations, helping operators find and stop potential account sharing or ATO attempts. Behavioral analytics plays a critical role in identifying deviations from established user patterns — whether it's frequent withdrawals, erratic login attempts or sudden changes in user behaviors — allowing for the detection of account takeovers and bonus abuse schemes.

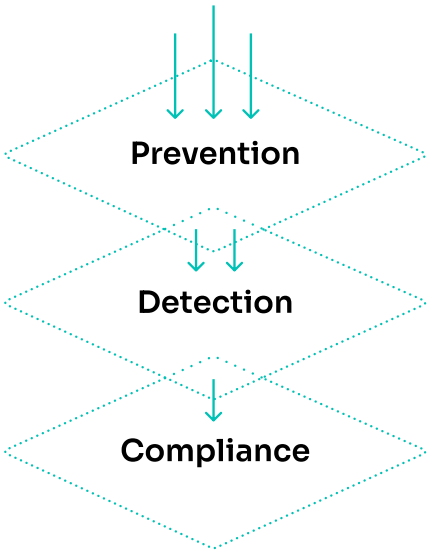
Adaptive AI & Machine Learning to Stay Ahead

Machine learning algorithms analyze billions of transactions in real time, continuously adapting to new fraud patterns and flagging deviations from normal behaviors over time to recognize emerging fraud tactics. When used in tandem with automated fraud detection systems, operators can minimize false positives, ensuring legitimate players enjoy a frictionless experience while staying ahead of fraudsters who constantly evolve their tactics.

3. Compliance & AML Monitoring in iGaming

Regulatory compliance is as critical as fraud prevention in the iGaming industry, ensuring platforms remain secure, lawful and protected from financial crime. Anti-money laundering (AML) regulations require operators to verify customers, monitor transactions and report suspicious activity to avoid legal penalties and protect both their business and players. Non-compliance comes with heavy costs — fines, reputational damage and even license revocation.

Effective AML tools help filter out high-risk users and detect money laundering patterns through transaction monitoring and



1. Digital Footprint Analysis
   Device Intelligence
2. Real-Time Monitoring
   Behavioral Analytics
   Adaptive AI & Machine Learning
3. AML Monitoring

risk scoring, flagging irregular deposit and withdrawal behaviors. A strong customer due diligence process includes screening against PEP and sanctions lists to prevent high-risk individuals from exploiting gaming platforms. The challenge is maintaining compliance without disrupting the player experience. Tools like pre-KYC checks and device intelligence allow seamless onboarding for legitimate users while stopping fraudsters early.

A Unified Approach: Integrating Prevention, Detection & Compliance

Fighting fraud in iGaming isn't just about reactive measures anymore — it's about having a seamless strategy that brings prevention, detection and compliance together. Relying on multiple disconnected solutions can slow teams down, increase manual work and leave gaps for fraudsters to exploit. A unified approach makes fraud management more efficient, accurate and cost-effective while keeping legitimate players' experiences smooth.

By combining digital footprint analysis, device intelligence, behavioral monitoring and AML checks, operators get a full view of user activity, making it easier to spot risks early. Blocking fraud before it happens prevents bonus abuse and multi-accounting from eating into revenue, while automated risk assessments help identify high-risk users, ensuring stronger KYC and AML compliance.

Operators using a unified system have seen an 80% increase in bonus abuse detection and identified 93% more multi-accounting incidents, proving how practical an integrated approach can be.

A smarter fraud prevention strategy improves the player experience by allowing real users to onboard quickly and seamlessly without unnecessary friction. Automation frees up fraud teams, helping them focus on high-value cases instead of manual reviews. With real-time insights and adaptive fraud detection, operators can stay ahead of evolving threats, protect revenue, and scale confidently in a fast-moving industry.

How SEON Empowers Operators in Fraud Prevention

Registration
Filters out bonus abusers

Login
Prevent account takeovers

Deposit
Intercept unusual transactions

Activity
Detect malicious player activity

Withdrawal
Catch suspicious payouts

SEON is the only comprehensive fraud prevention solution using AI-insights to stop fraud before it happens across the entire customer journey.

SEON combines prevention and detection to stop fraud before it enters your platform. By **analyzing over 1,000 digital and device signals** — including digital footprints, IP addresses, device intelligence, email and phone data — SEON assesses risk at the earliest stage. This allows operators to instantly identify fraudulent users and detect fraud rings, bonus abuse, multi-accounting and synthetic identities before any financial harm.

Unlike fragmented solutions that require multiple integrations, SEON's **unified platform** offers a centralized dashboard for complete fraud management, **streamlining AML and KYC compliance** while providing scalable protection against evolving threats.

Speak with an expert


SEON