SEON

NO DICE: A 2025 OUTLOOK ON GLOBAL IGAMING FRAUD TRENDS

YOUR FIRST LINE OF DEFENSE AGAINST ONLINE FRAUD

INFO@SEON.IO

WWW.SEON.IO

SEON delivers a **competitive edge in fraud prevention and risk mitigation through advanced digital footprint analysis, device intelligence and real-time AI-driven insights** that empower you to stop and prevent fraud, including multi-accounting, bonus abuse and affiliate fraud – without impacting the player experience.

80%

Prevent Up to 80% More Bonus Abuse
Our advanced data analytics, including the industry's most extensive digital and social footprint analysis, utilize cutting-edge device intelligence to pinpoint and curb bonus abuse and multi-accounting. This precision allows you to proactively identify and mitigate these fraudulent activities effectively.

20%

Accelerate Manual Review Processes by 20%
Our machine learning engine is tailored to enhance fraud prevention efficiencies. You can swiftly analyze patterns in player account activities by automating manual reviews and integrating custom rules alongside velocity checks. This system speeds up the review process and bolsters your anti-fraud measures with targeted insights and faster resolutions.

40%

Cut Manual Queries by 40%
Our system's continuous learning capabilities and transparent risk decision explanations substantially reduce the need for manual interventions. Our platform enhances your fraud detection processes by autonomously refining and applying new rules based on ongoing observations. This allows your analysts to redirect their focus toward more complex cases that demand detailed attention.

United States

- Second highest geographic risk area
- Total bonus abuse in a single state can net more than US $18,000 per user

Latin America

- Surge in operator expansion
- Lower player acquisition costs contribute to higher rates of welcome bonus abuse
- Higher risk tolerances across top-tier operators
- 70% higher approval rates for players

United Kingdom & Europe

- Mature gambling market with experienced operators and sophisticated fraud tactics
- 36% of players found to be high risk upon registration
- 10% of players require manual investigation before approval or decline

Asia

- Highest geographic risk area
- Largest concentration of crypto-related betting
- 40% of all new users are declined for being considered high risk
- Lower player acquisition costs contribute to a larger influx of players; higher rates of welcome bonus abuse

Asia Pacific Economic Cooperation

- Emerging market with less experienced operators
- Moderately sophisticated and increasingly sophisticated fraud attacks

Africa

- Third highest geographic risk area

FRAUD'S REGIONAL RISK PROFILES

We Track and Monitor iGaming Fraud Globally in Real-Time

We've built an anti-fraud detection system that can flexibly adapt to different geographical fraudulent behaviors and needs. Our multi-layered and frictionless fraud prevention platform helps you to stop fraudulent users – irrespective of their location.

32x

ROI ACHIEVED BY LOTTOLAND THROUGH UNIFIED ANTI-FRAUD MEASURES

COMBATING MULTI-ACCOUNTING: A CASE STUDY WITH LOTTOLAND

Background

Lottoland, founded in 2013, has grown from a startup with seven employees into a leading online iGaming operator active across four continents and servicing over 19 million customers. Known for its extensive range of products including lotteries, casino games and sports betting, Lottoland is committed to delivering a seamless customer experience and continuously enhancing fraud prevention strategies.

Before SEON

Lottoland faced significant challenges with fraudulent activities such as account takeovers, bonus abuse and chargeback fraud. Their onboarding processes were particularly vulnerable, allowing fraudulent players to exploit promotional offers. Their reliance on manual reviews for detecting and blocking fraudulent accounts yielded significant inefficiencies, compromised user experiences and disrupted player journeys.

With SEON

Lottoland's implementation of SEON transformed its approach to fraud prevention. By integrating real-time monitoring of player registrations and utilizing machine learning for pattern detection, Lottoland minimized disruptions for genuine players and blocked suspicious activities at the onboarding stage. This shift automated and streamlined their processes and significantly improved operational efficiencies.

Impact

SEON's comprehensive and adaptive fraud prevention tools enabled Lottoland to tackle persistent fraud issues effectively, reducing manual reviews and enhancing data insights. This strategic overhaul delivered a 32x return on investment, reinforcing Lottoland's commitment to secure, responsible gambling and maintaining its reputation as a trusted iGaming leader.

TACKLE BONUS ABUSE WITHOUT SACRIFICING ON PLAYER EXPERIENCE

Our platform is expertly crafted to uncover connections indicative of multi-accounting, utilizing insights from your users' digital footprints combined with behavioral patterns and device intelligence that let you spot and stop suspicious accounts.

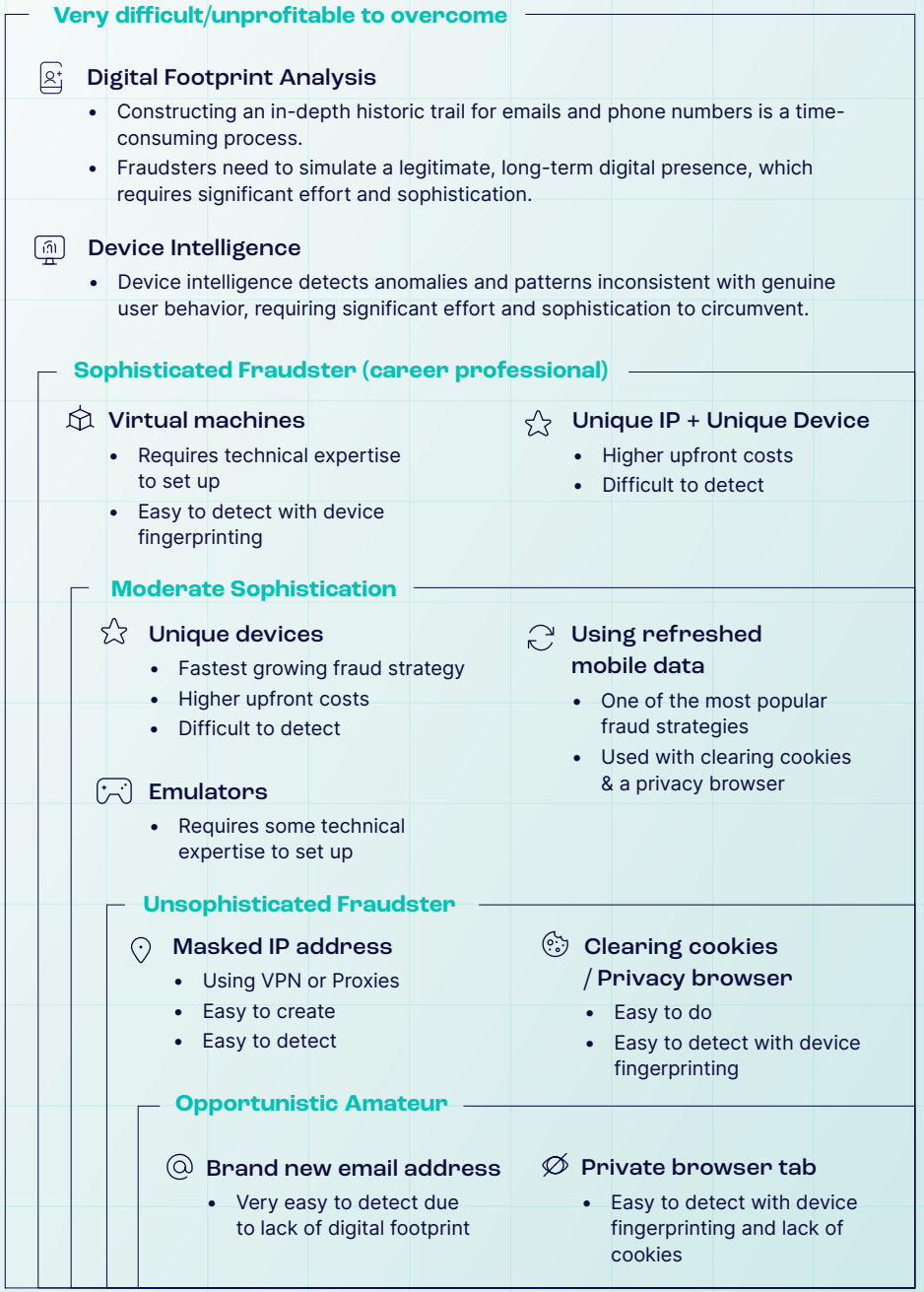
Whether stemming from opportunistic customers or sophisticated fraud rings, SEON runs device fingerprinting, IP, email and phone lookups, and taps other signals to extract as much metadata as possible about the person signing up for your bonus.

All gathered data undergoes rigorous analysis and is fed through a customizable risk-scoring engine designed to give you actionable insights to keep you ahead of the game.

Rooting Out Bad Actors

SEON references hundreds of proprietary real-time data points to reveal bad actors and stop fraud in its tracks.

- Device hashes can show the connection between a large volume of players
- Using device hashes plus additional IP information can detect moderately sophisticated bonus abusers
- Combining device hashes with IP and password hash data can trace advanced bonus abusers across numerous accounts.



CUSTOM RULES ENGINE

Did You Know?

Data breaches play a paradoxical role in discerning the authenticity of emails by inadvertently revealing patterns that distinguish genuine accounts from fraudulent ones. Authentic emails, with established histories, are more likely to appear in data breaches as opposed to throwaway or temporary emails. This disparity offers valuable account insight into the legitimacy of account data.

A Custom Rules Engine at Your Fingertips

As a comprehensive fraud prevention platform that employs advanced digital footprint analysis, a fully customizable rules engine and machine learning, SEON empowers you to maintain control over your risk decisioning and exposure. The inclusion of velocity rules enhances this capability by allowing you to set specific thresholds for the frequency of actions within a defined time period – crucial for detecting and responding to suspicious activities that could indicate bonus abuse or account takeovers.

Expert Guidance on Fraud Prevention

Our team of fraud experts offers guidance on optimal rules for your business needs, providing essential information on fraudster habits and patterns indicative of bonus abuse. This expert advice includes the strategic use of velocity rules to monitor and analyze quick successions of transactions or account activities, further bolstering your defenses against sophisticated fraud tactics.

of bonus abusers **have never been involved in a data breach**

of bonus abusers **use a free email provider**

of bonus abusers **do not have any social media presence** attached to their email address

of bonus abusers **use a proxy to access operator websites**

A BETTER WAY TO CATCH AFFILIATE FRAUD

Affiliate programs are a vital source of traffic and revenue for iGaming operators. Unfortunately, they can also be magnets for fraud due to the nature of affiliate marketing. While the affiliates themselves aren't orchestrating fraud, as they function as promoters of offers, fraudsters keenly observe and exploit the promotions, making affiliates unwitting targets for fraudulent activities.

4 Ways SEON Stops Affiliate Fraud

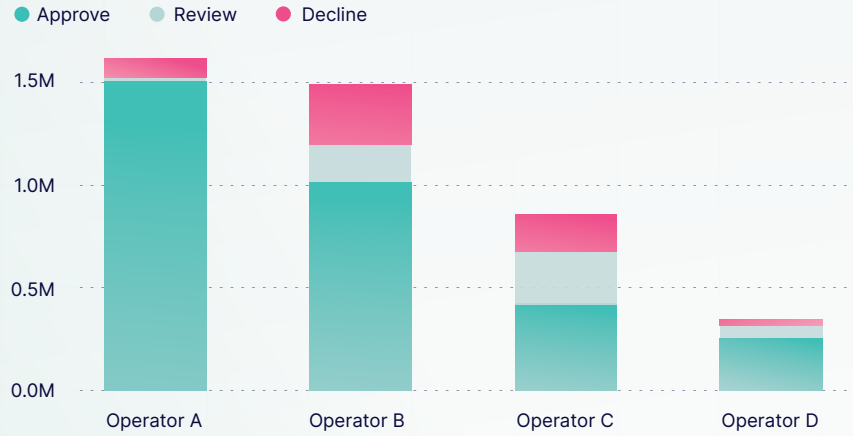
1. Monitors Your Traffic
Gain a comprehensive overview of approved and declined onboarded users per affiliate, providing a clear perspective on the quality of your partnerships and enabling the detection of affiliate fraud.

2. Identify and Track Suspicious Users
Effortlessly uncover fraudulent activities with extensive device, IP, and software analysis coupled with robust digital footprinting – leveraging 90+ unique digital and social signals – to build a complete profile of each of your players, identify and track suspicious users and create a multi-layered defense against affiliate fraud.

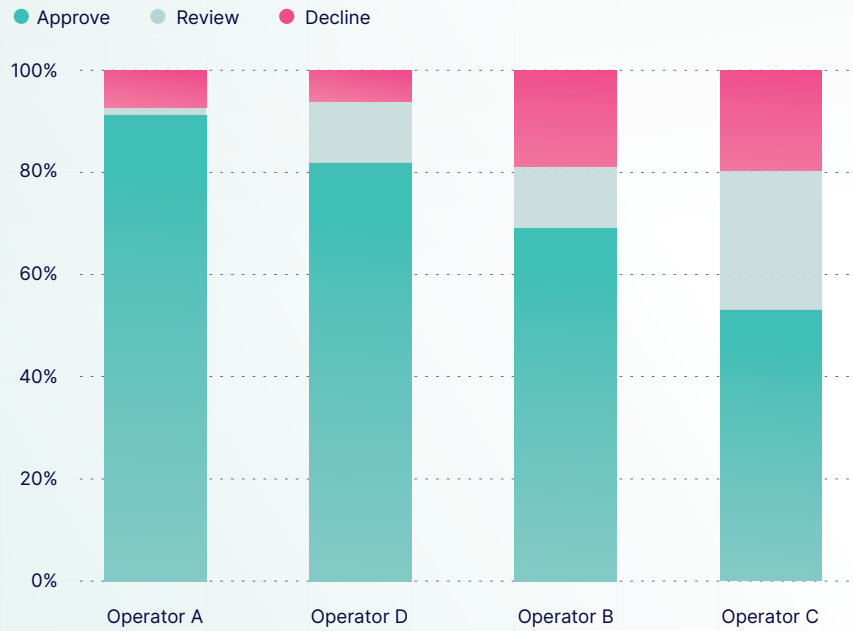
3. Analyze User Behavior
Understanding your users is crucial, and assessing their actions – particularly within a velocity framework – is vital for identifying suspicious behavior. We monitor connection attempts per minute and evaluate the speed of form field completion allowing you to know your customers better.

4. Control the Withdrawal
Prevent undesired users from bypassing controls. Take charge of the withdrawal process and apply advanced risk rules to block users attempting to cash out virtual chips.

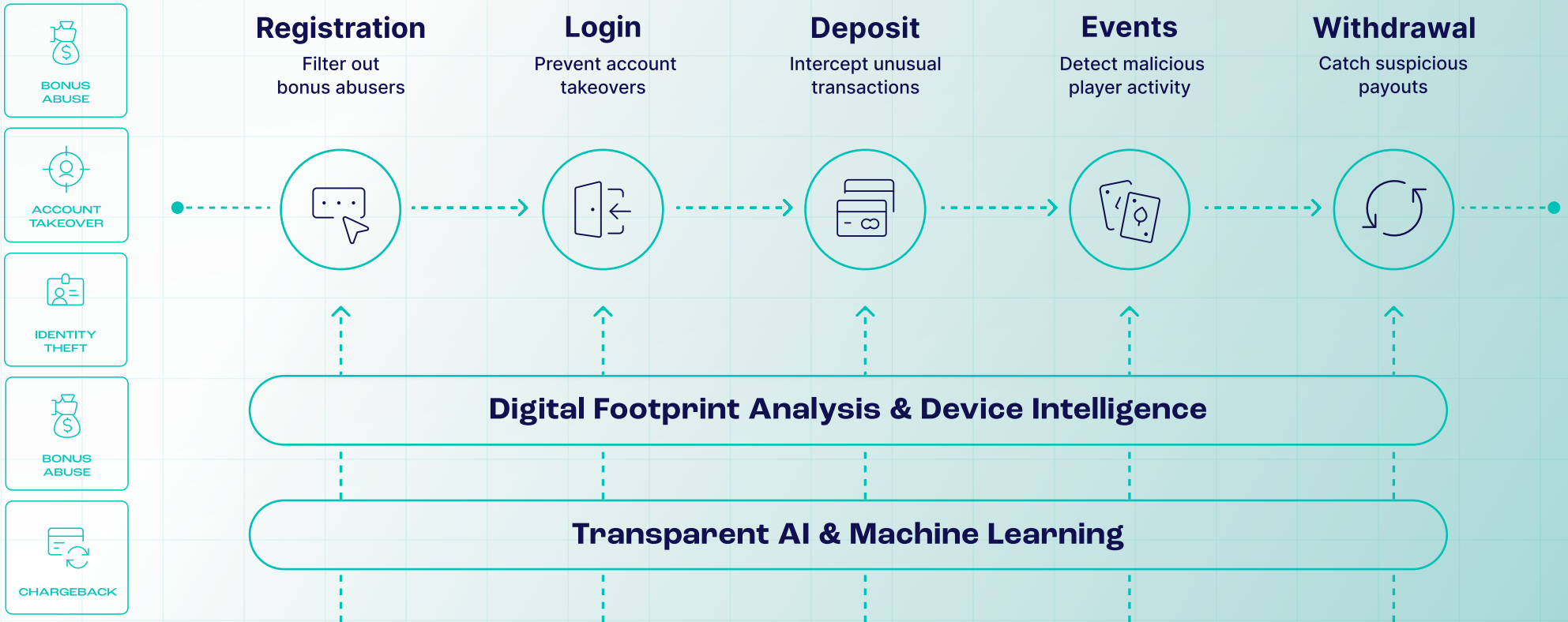
Number of Transactions by Label and Customers



% of Registrations from Affiliates by Label and Customers



STOP FRAUD EARLIER IN THE CUSTOMER JOURNEY



SEON

NO DICE: A 2025 OUTLOOK ON GLOBAL IGAMING FRAUD TRENDS