EBOOK

Preventing Evolving Fraud Attacks in the iGaming Industry

SEON Technologies Ltd.
seon.io

info@seon.io
0044-20-351-44790

Preventing Evolving Fraud Attacks in the iGaming Industry

It's no wonder every edition of the Online Gambling Quarterly begins with an assessment of the current industry climate: **iGaming is still one of the most dynamic and fast-changing verticals** to do business in.

New technologies, updated regulations, evolving marketplace. It all contributes to a feeling that the industry is in a state of perpetual transformation.

Unfortunately, this also makes it increasingly challenging for operators to prepare themselves against attacks, specifically those from fraudsters.

This is why, in this ebook, we've gathered our insights from years of protecting iGaming leaders. Part one will examine some important statistics we've gathered, and part two will then offer actionable prevention tips to bring peace of mind to iGaming operators, even in an ever changing business and fraud landscape.

Part 1:
The Challenges

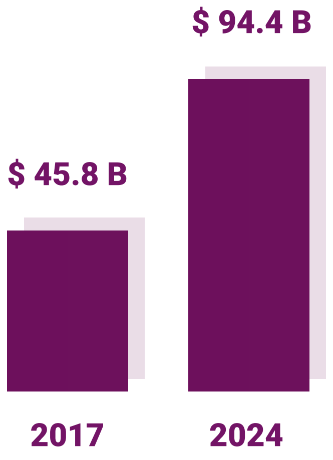
Mention future forecasts to any insider in the iGaming industry, and everyone will tell you the same thing: the business, like the games it promotes, is one of high risk and high reward.

But understanding where risk comes from is the best way of underwriting it. So let's first look at some very specific examples of how the market is transforming, and how these movements create the ideal environment for certain types of fraud.

1.1 Thriving in A Transforming Market

Online gambling: A growing market

- Business is growing
- New markets
- Accepting more payments



Source: Statista

Yes, iGaming is growing, but it's doing so in leaps and bounds that make it **difficult to feel like you're standing on firm ground.** According to iGaming leaders, this has mostly to do with market-specific challenges such as:

- Over taxation in France
- Excessive regulation by the UK gambling commission
- Move to countries with fewer regulations
- Congested and tougher markets
- Long-term shift in public opinion
- Gambling ad restrictions in Spain...

And while there is a silver lining with the opening of new markets (especially in the US, Brazil and Asia, and the boom in mobile gaming), the issue of fraud tends to complicate the picture.

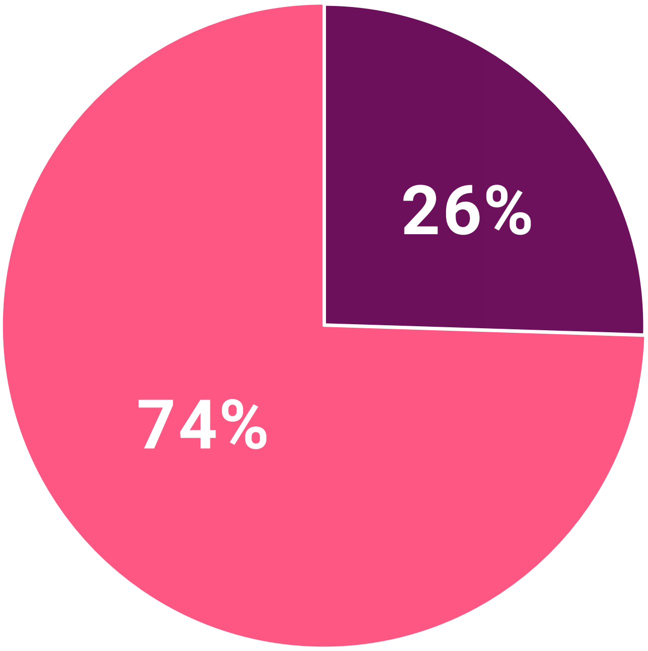
In fact, **the rate of fraudulent signups in iGaming can be as high as 26%,** a number that far surpasses that of other industries like ecommerce or entertainment.

What about fraud?

Payment fraud

Chargeback rates

Bonus abuse

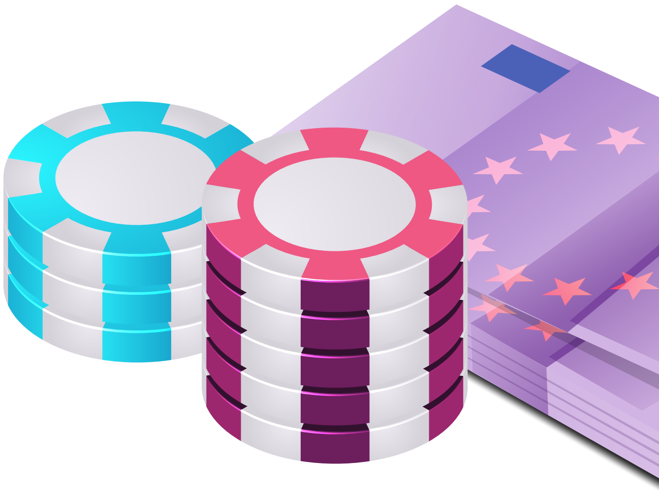


Source: SEON

● Fraudulent ● Normal

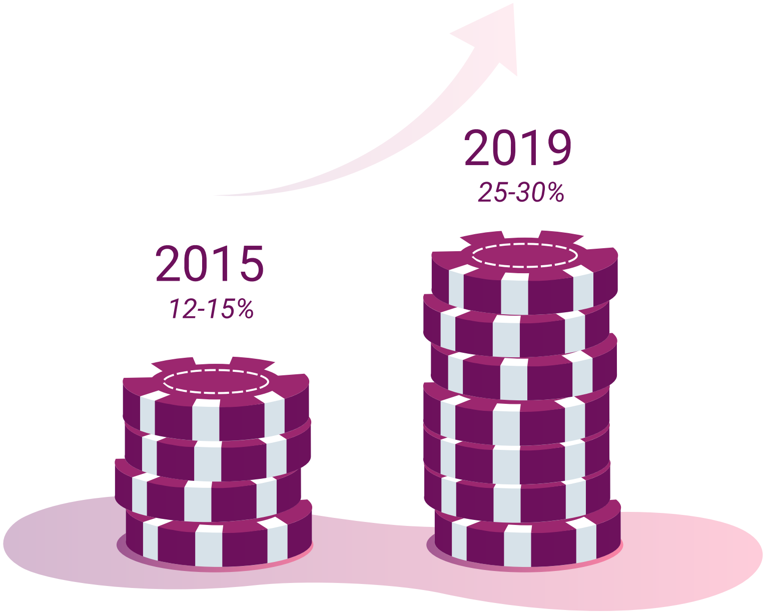
Rate of fraudulent signups

And at the top of these challenges is the issue of bonus abuse, which showed **a 72% rise between 2018 - 2019.**



1.2 Bonuses Abuse - 3 Ways it Hurts Vendors

While every business wants to attract new users to grow fast, very few industries offer bonuses as aggressively as the iGaming world. Typically, **marketing departments increased their spend on bonuses from 12-15% in 2015 to up to 30% in 2019.**



Increase in the average bonus spend from marketing departments between 2015-2019

Problem number one? These offers are almost too tempting for fraudsters, who sign up multiple times to collect their free spins or free cash.

In other words: **bonuses are a great incentive for multi accounting fraud.** Fraudsters will stop at nothing to bypass KYC checks and create as many accounts as possible, including:

Stolen ID **Synthetic identity** **Prepaid credit cards**

More sophisticated criminals will also have the resources to use emulators, virtual machines, and even residential IPs, for example by using Socks5 proxies or mobile networks to leverage fresh IP addresses.

BETTER BONUS RULES ATTRACT ORGANIZED CRIME

Bonus hunters will also create multiple accounts to increase their chances of winning the actual games, a process also known as **player or self collusion.**

Criminal rings will have members sign up, collect a bonus, and deliberately lose to siphon winnings towards another account controlled by the fraudsters. Similarly, **matched betting, arbitrage, and advantage playing** are often leveraged by organized teams who can automate the processes to extract maximum gains from the casinos.

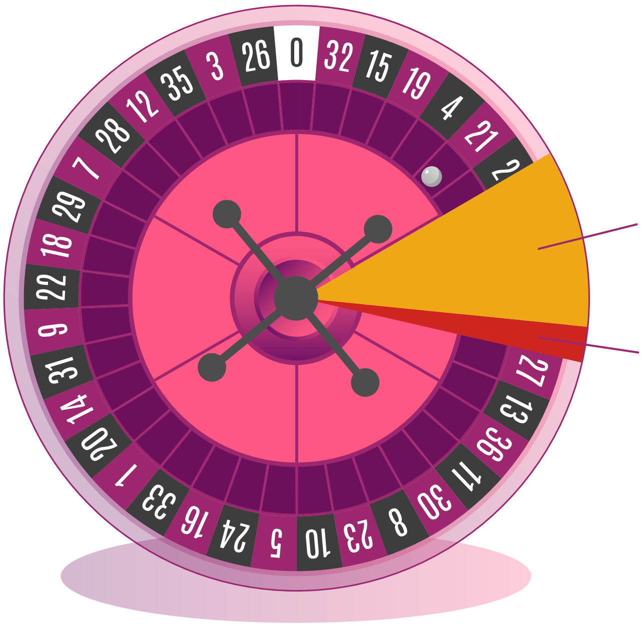
And while **operators are becoming better at creating more complex bonus rules,** lowering bonus payouts and blocking risky locations, even these tweaks don't fully stop the problem.

Individual fraudsters might be deterred, but criminal syndicates have the resources and experience to work together as a business in order to exploit the games.

MARKETING OFFERS TURN INTO MANUAL REVIEWS

According to our own data, the biggest challenge for fraud teams in iGaming is to perform efficient manual reviews. Unfortunately, more bonus offers means a heavier workload to approve or refuse signups, with a surprisingly low decline rate.

While 8-12% of all gambling transactions require manual review, only 1-4% end up in decline.



8-12 %

of all gambling transactions require manual review

only

1-4 %

end up in decline

This points to a fundamental issue in how risk thresholds are calculated before an operation is sent to be overseen by a fraud team. Businesses rarely have the courage to decline transactions because of the nature of the competitive landscape. They feel safer reviewing manually, which is hard to do fast, and efficiently.

1.3 Multi Accounting, Fines and Self-Exclusion Fraud

Aside from bonus abuse and collusive play, another issue with multi accounting arises when we look at self-exclusion rules. According to statistics gathered at our own webinars, we found that the **biggest challenge for iGaming operators was to spot customer connections.**

A swedish gambling operator learned that lesson that lesson the hard way, when it was issued a fine of SEK4M ($431,900) in 2019 for failing to block self-excluded players from accessing their websites with alternative accounts.

A bookmaker based in London was fined $31k for the same reason by the New Jersey DIvision of Gaming Enforcement (DGE) in December 2019.

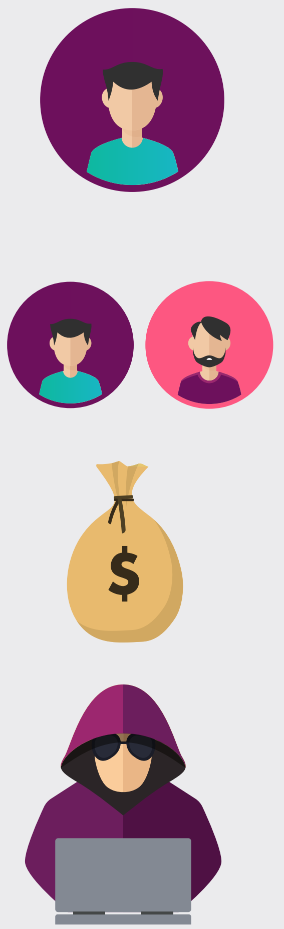
Unfortunately, it is extremely difficult for companies to protect all players, even with the best intentions in mind. Self-exclusion programmes are usually taken seriously by iGaming operators, which is why it can be so disheartening to be punished by a fine.

And this is doubly more unfair when **unscrupulous players try to leverage these fines against the operators via self-exclusion fraud.**

An unwelcome consequence of the increase in regulations, **self-exclusion fraud. It was reported by** one of clients as the fastest growing area of fraud in their business in the past 18 months — and it is particularly affecting UK operators, where one player's self exclusion must be carried across all the casinos run by the same parent company.

As there are very few systems in place to flag self-exclusion issues as fraud, it's no wonder regulations make operators nervous when dealing with these new kinds of attacks.

HOW SELF EXCLUSION FRAUD WORKS



A fraudster opens an account, sometimes uses it to play, and self-excludes it.

They open a second account with the same operator, or those that fall under the same license as the parent company.

They deposit large amounts and play volatile games at max bet.

If they lose, they blackmail the operator into getting a refund, by claiming their self-exclusion was not respected.

A variation also sees fraudsters claim chargebacks by opening two different accounts with the same card number. They self-exclude one account, which means the card should be blacklisted under the UKGC Responsible Gambling regulation.

If, after playing, they lose funds on the second account, they initiate a chargeback directly with their bank, which ends up costing money for the iGaming operator, and could incur fines.

1.4 Account Takeover Damages Brands and Reputation

Building safety and trust is primordial for iGaming operators, which is why they ought to pay great attention to the problem of account takeover, whereby individuals manage to log into an account which isn't theirs. In 2018, these attacks accounted for $4 billion of losses for businesses worldwide.

But account takeovers are just as taxing for users: it is estimated that victims end up paying $263 out of their own pocket to resolve an ATO, not to mention the time, stress, and efforts needed to overcome the problem.

Unsurprisingly, the loss of trust and brand reputation that ensues can be enough to sink a successful gambling operator.

1.5 Affiliate Fraud Erodes Trust With Partners

Another area where marketing spends can backfire against casinos: affiliate fraud. Marketers who reward affiliates for directing visitors towards their site are often the victims of:

- **Spammed referral links:** which bring in low-quality players
- **Bot automation:** whereby fraudsters use software to imitate human behavior and generate fake clicks and transactions
- **Maliciously diverted traffic:** which sends unwilling visitors to the page, increasing bounce rates and corrupting analytics.

In some cases the affiliate fraudsters will go as far as cloning the operator's website, and host it on a domain name that looks similar. More advanced techniques include malicious browser extensions that swap legitimate affiliate URLs for their own, and even inject ads with referral links into ad-free web pages.

1.6 Payment Fraud, Chargebacks and Friendly Fraud

Last but not least, the trio of classic fraud techniques that still cost operators too much, especially as a report found **it rose by 37% from 2018 to 2019.**

Friendly fraud, when customers claim they are victims, is the fastest growing reason for chargebacks. It happens when players experience remorse, they refuse to pay for a family member's bets, or simply want to exploit the operator to withdraw funds without paying for anything.

The interesting point to note is that we find these fraud attacks are often the main target of fraud teams. Meanwhile, bonus abuse and account takeover are often ignored, simply because prevention teams have a harder time spotting customer connections.

As we'll see in the solutions below, you can actually use similar tools to defend your organization against all fraudulent attack vectors, whether it's to reduce false positives or chargeback costs.

Part 2:
The Solutions

The key challenge of iGaming operators is therefore to combat traditional fraud (chargebacks, transaction fraud), along with multiple specific attack vectors, such as self-exclusion or affiliate fraud.

Luckily, you will find that the right fraud prevention tools can meet multiple needs, and fight fraudsters on all fronts.

2.1 Digital Footprint Tools For a 360 View of Users

HOW IT HELPS: CREATE A FULL PICTURE OF USERS WITH MINIMAL DATA POINTS.

When it comes to fraud prevention in iGaming, the golden rule is simple: the more data, the better. At **SEON**, we combine a number of modules to gather and enrich data, all of which answer the following questions about a user:

- **Device fingerprinting:** the phone, computer or tablet that players use to connect to the gambling platform contains tons of info. Are they using private mode or an emulator? This could increase suspicion that they are not who they claim to be.

  Multi-accounters favour desktop and laptop devices to access their records and fraud guides. They also allow them to install auto spin features and to work more efficiently. If the device is a laptop or desktop using mobile data (dongle) and no phone or email history, we can be pretty confident we are dealing with a multi-accounting operation.

- **Email profiling:** does the email address exist? Is it from a suspicious, disposable domain? Or one that doesn't require any verification during sign up?

  Fraudsters will create an email address fast, and without linking to Twitter, Facebook or other social media accounts. This is not the typical behaviour of a genuine customer, who would use an aged email address, probably used to sign into multiple social media platforms.

- **Phone analysis:** are they signing up with a real phone number? From a fixed line or mobile? And did they use that number for messaging services?

  Fraudsters are unlikely to register the phone number with messenger apps and other platforms. We can also flag phone numbers that come from "burner" apps, which allow people to enable numerous phone numbers on one device only.

- **IP analysis:** one of the oldest and easiest forms of security available: looking at the origin of the connection. Is it from the right location? Or likely to be masked via TOR or a VPN?

  Fraudsters often rely on mobile IP addresses to hide their multiple accounts. This is because these IPs show no geographical info, and are harder to identify than data centers. Laptops with dongles are the most popular setup amongst multi-accounters, and not typical for genuine players.

2.2 Adaptable KYC Triggers at Signup

HOW IT HELPS: REDUCE BONUS ABUSE, MULTI ACCOUNTING, POTENTIAL TRANSACTION FRAUD...

The registration stage is often the best time to apply fraud prevention techniques, whether it's to reduce bonus abuse, multi accounting, account takeover or future transaction fraud.

But there is a big caveat: legitimate users who have to go through too many verification processes are more likely to jump ship to other competitors. **Avoiding churn is primordial for iGaming operators** who wish to onboard new users without letting the bad guys in.

The solution: adaptable KYC triggers. These are based on digital footprint analysis (more on that below), and let you leverage both light and heavy KYC.

- **Light KYC:** Light KYC includes frictionless customer risk scoring methods that don't affect user experience nor increases the churn. It's much cheaper to implement on a large scale and works well combined with heavy KYC processes.

- **Heavy KYC:** Meanwhile, ID or other document verification processes are providing a higher level of security. They have also downsides, as they are expensive to check, and negatively impacts user experience. Fraudsters are also increasingly adept at bypassing them.

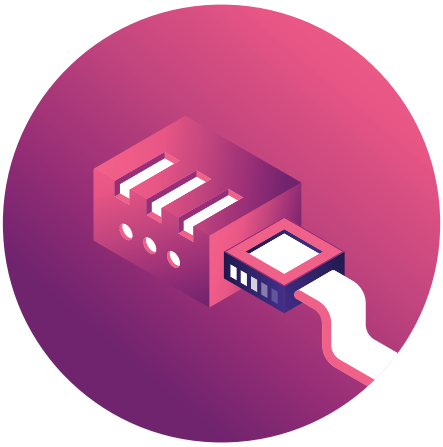
It's worth noting that the withdrawal stage always benefits from mandatory heavy KYC, which won't be so frustrating for legitimate users who had no trouble signing up.

2.3 Better Precision With Velocity Rules and Machine Learning Insights

HOW IT HELPS: REFINING YOUR RULES WITH THE RIGHT PARAMETERS WILL REDUCE AFFILIATE FRAUD, FALSE POSITIVES, FRIENDLY FRAUD, AND MULTI ACCOUNTING.

Based on our data, iGaming operators rarely use one data point only, favouring at least two, but sometimes up to 8 to create complex rules that meet their specific needs to prevent fraud.

3 frequently used data points for reducing fraud

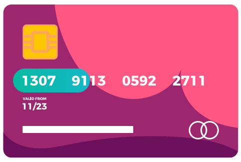


IP address

Location (geolocation, addresses)

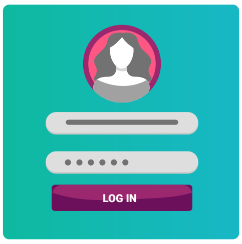
Credit Card data

But unexpected data points can also help reduce false positives and improve the efficiency of the manual review team:



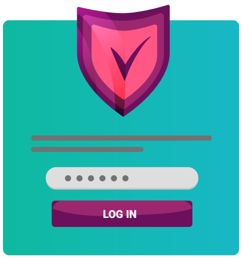
Card BIN range:
It can identify a prepaid card, which should increase suspicions. Expiration dates can also reveal risk. The fresher a card is, the higher the risk.

Site referral:
Traffic coming from a bonus abuse forum or excel sheet increases risk.



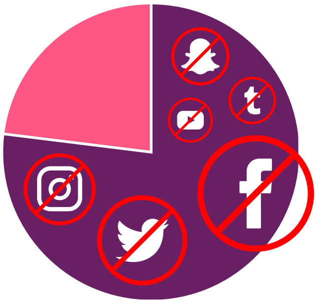
Password:
The passwords shared with multiple customers can indicate fraudulent syndicates.

Security question and answer:
Finding the same in use by multiple accounts is a strong indicator of multi accounting.

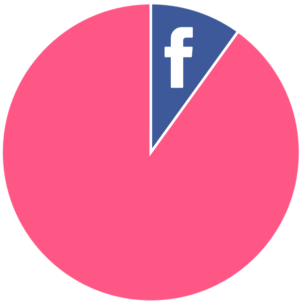


Deposit sizes:
Users who take the full bonus value and assume there is no winnings cap should be marked as suspicious.

It is by looking at a wide range of available data points that we uncovered some fascinating insights about fraudster behaviours. For instance, through real-life data fed into our email analysis tool, we found that:

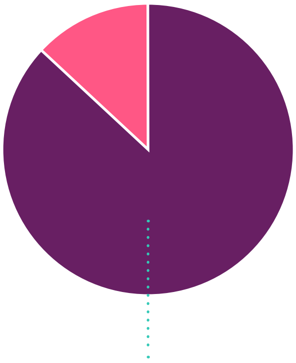


77% of bonus abusers do not have any social media presence related to their email address

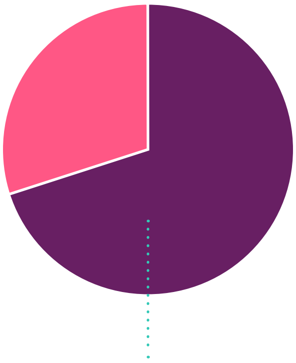


Only **10%** of bonus abusers have a Facebook account registered with their email address

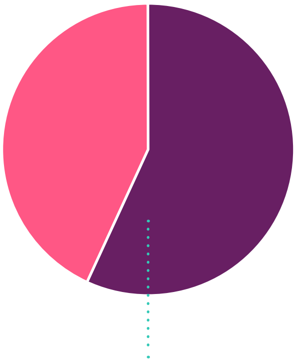
Similarly, our IP and email analysis modules revealed the following insights, which can be used to refine rules and risk thresholds:



87% of bonus abusers use a free email provider



70% of bonus abusers use a proxy to access the operator website



57% of bonus abusers use a data center IP address -> IP address

All that data is **particularly useful when used with complex tools like velocity rules,** a great way to find connections by comparing specific data points during a set timeframe. For instance, velocity rules could look at how many users have used the same IP address before completing a transaction within 30 seconds, 1 minute or 1 day.

The timeframes (or the velocity part) also revealed some interesting numbers, as more than **40% of the rules worked with a timeframes set within one day** (and as low as a few minutes only).

Now, the main challenge with velocity rules is in finding the right combinations. Because comparing numerous data sets results in enormous amounts of possibilities, however, an AI-driven system should help you filter unnecessary combinations.

The key takeaway here is that trying every single rule configuration simply isn't a task possible for humans. It's only with Intelligence and Machine Learning that you can truly experiment, refine, and improve your rule prevention strategy in the long run.

And as a bonus, the same tools can be used to assist manual reviews, and to help with your self exclusion programs.

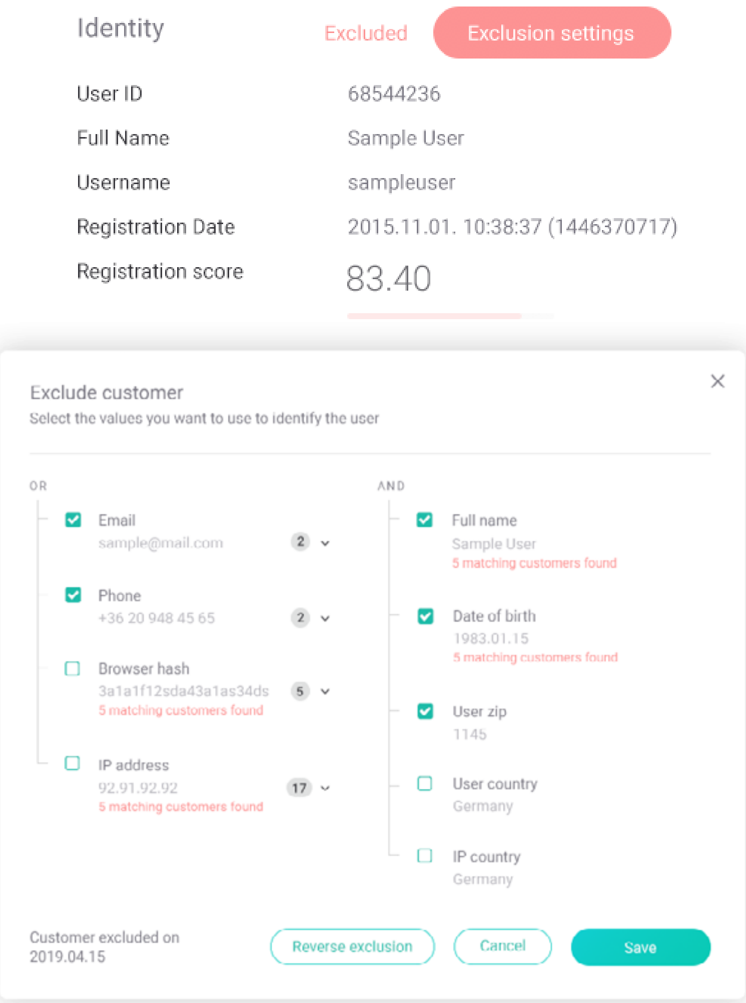
2.4 AI for Self-Exclusion Programs

HOW IT HELPS: REDUCE SELF-EXCLUSION FRAUD BY FLAGGING ADDICTIVE BEHAVIOUR YOURSELF, AND SPOTTING CONNECTIONS BETWEEN MULTIPLE ACCOUNTS.

Fraud prevention tools are already your best bet for meeting legal requirements pertaining to KYC and strong customer authentication. So why not employ the same tools to deliver self-exclusion programs?

The crossovers are numerous. For instance, our SEON self-exclusion feature uses the same powerful data analysis as for fraud prevention, but offers to flag users based on increasing daily or weekly deposits, and hours spent on games.

Moreover, we provide a clear button to instantly mark users wishing to be self-excluded. It adds specific data points to a flag list and matches new registrations to the database, leveraging machine learning to tag suspicious, or at-risk players.



Identity Excluded Exclusion settings

User ID	68544236
Full Name	Sample User
Username	sampleuser
Registration Date	2015.11.01. 10:38:37 (1446370717)
Registration score	83.40

Exclude customer

Select the values you want to use to identify the user

OR

☑ Email
sample@mail.com 2

☑ Phone
+36 20 948 45 65 2

☐ Browser hash
3a1a1f12sda43a1as34ds 5
5 matching customers found

☐ IP address
92.91.92.92 17
5 matching customers found

AND

☑ Full name
Sample User
5 matching customers found

☑ Date of birth
1983.01.15
5 matching customers found

☑ User zip
1145

☐ User country
Germany

☐ IP country
Germany

Customer excluded on 2019.04.15

2.5 Multi Layered Prevention That Fits your Business Infrastructure

HOW IT HELPS: SAVE ON MANUAL RESOURCES AND COSTS BY STACKING FRAUD PREVENTION TOOLS THAT BLOCK BONUS ABUSE OR MULTI ACCOUNTING IN A WAY THAT WORKS BEST FOR YOUR BUSINESS MODEL.

Many operators with older, legacy solutions, are having a hard time integrating a brand new fraud prevention tool from scratch. But all hope isn't lost, as modern companies like SEON are working on flexible integrations.

These are designed to enable a multi-layered protection, where multiple tools and processes can be combined for a number of reasons:

- **To enrich the data:** A lot of legacy systems were designed to gather and analyze single data points. But companies might realize they also need external (or enriched) data to learn more about users. Instead of throwing the whole system away, they can take a multi-layered approach and simply integrate a third-party data enrichment tool.

- **To meet scalability issues:** if an operator is growing fast and the fraud prevention is lagging behind, fraud managers can integrate an external tool to boost the efficiency of the current system without too much disruption.

- **To patch holes in the line of defense:** Instead of completely rebuilding their fraud prevention systems, some companies will add 3rd party solutions with very specific goals. For instance, a reverse email lookup tool, reverse phone lookup tool or device fingerprinting solution that was originally missing.

- **To speed up manual reviews:** if you can't tweak your system to reduce manual reviews, you can add another solution to help. For instance, certain companies use additional tools like plugins that query external databases to get a final say on approving / denying a transaction.

At SEON, we're continuously working to make integrations faster, smoother and more cost effective, which is how a tailored solution helped online casino **Maxent increase multi accounting detection by up to 60%.**

Conclusion: Fighting iGaming Fraud on All Fronts

As the iGaming landscape continues to change from year to year, so must the tools used to reduce fraud in the industry.

Unfortunately, operators tend to play catch up with fraudsters, who are agile and quick to leverage new attack vectors, as demonstrated by the recent surge in self-exclusion fraud.

The good news is that, in the prevention camp, companies like **SEON** are always striving to **develop new tools, share insights, and refine rules that will eventually defeat the fraudsters.**

Even if the business feels unpredictable (and exciting), we truly believe iGaming operators should at least have peace of mind when it comes to scaling their operations while reducing the costs, resources, and headaches lost to fraud.

To see how SEON can help your company prepare for the future, please visit seon.io

Or schedule a personalised product showcase call now.

Visit our website

Schedule a call

SEON

SEON Technologies Ltd.
seon.io

info@seon.io
+44 20 8089 2900