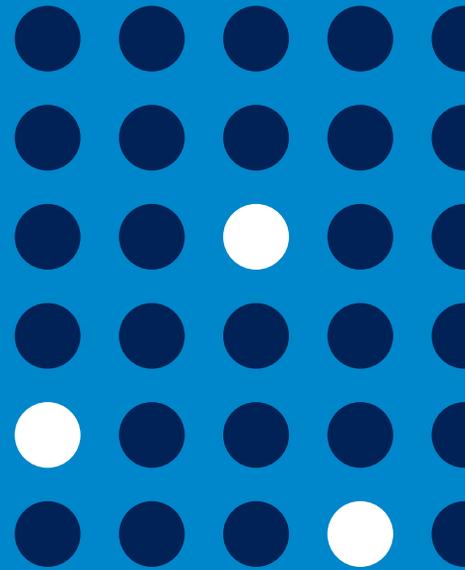## Solution Brief

—

Identify self-excluded players in real time to promote responsible gambling.

More than ever before, gambling operators are accountable for promoting responsible gambling across their online properties. When a player "self excludes" themselves from a gambling site, the operator is now answerable for ensuring the player does not resume gambling activities.

Unfortunately, gamblers will often go to excessive lengths to get back into the game, making it difficult for operators to responsibly protect the interests of their players while insulating themselves from costly regulatory complications.

Providing multi-industry and iGaming experience

Since 2004, iovation has maintained a globally-shared platform that is used by businesses across a range of industries including financial services, travel and leisure, e-commerce and insurance. More than 4,000 fraud managers leverage our best-in-class device reputation database, which is used to protect 25 million transactions and stop an average of 300,000 fraudulent activities every day.

We have worked with iGaming operators for 15 years and serve more than 100 gambling clients (operators and platform providers) such as Paf, PlayTech, EveryMartix, Betfred, SkyBet, SBTech and Leo Vegas.

Gambling Stats

Stats Over the Past 12 Months:

238K Self-exclusion records placed on iGaming accounts

73K Additional iGaming accounts impacted by self-exclusion that were associated to the above accounts via device

694K Devices impacted by self-exclusion records

20K Average rate of placement for self-exclusion ecords per month

Cross-Over Between Clients/Self Excluders:

44K Devices iovation sees at other iGaming sites even after self-exclusion records are placed

Impact of Self-Exclusion:

311K Transactions denied because of self-exclusion records

1.1M Transactions marked for review because of self-exclusion records

Get intelligence from over 4,000 fraud and risk professionals

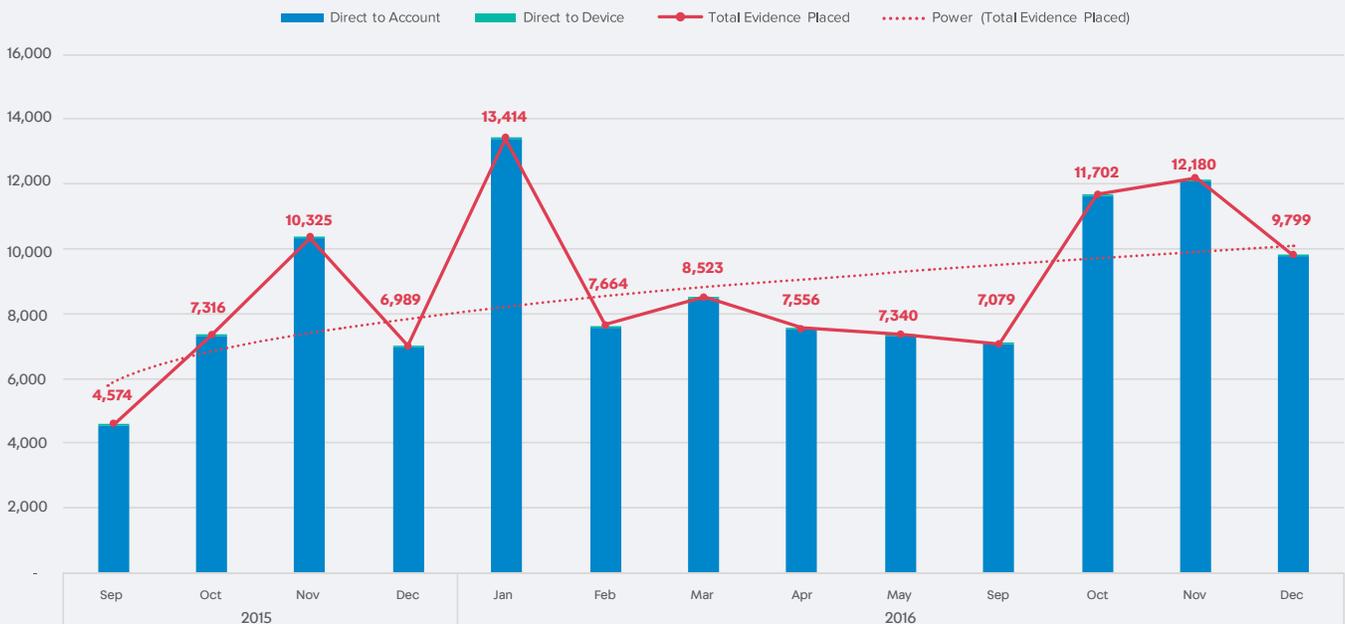**About iovation device intelligence**

As a market-leading provider of device intelligence solutions for online fraud prevention and authentication, we recognize any device connected to the web and provide helpful intelligence that operators and platform providers can use to detect and avoid risk.

- Uniquely recognize devices connecting to the web, even when they are intentionally trying to evade detection

- Recognize devices without requiring directly identifying personal data

- Recognize returning devices across multiple businesses, geographies and industries

- Associate multiple devices to each other and multiple online accounts across businesses, geographies and industries

- Identify the device's geolocation and detect if the device is manipulated or evading detection

- Perform velocity checks against your thresholds, such as the number of accounts accessed, number of transactions and number of accounts created from a device or group of devices

- Relay fraud and abuse reports associated with devices such as policy violations, self-exclusion, chargebacks, bonus abuse for specific devices and accounts

- Provide access to consortium intelligence and machine learning from billions of global transactions from more than 6 billion devices, and intelligence from 4,000 fraud and risk professionals

Trends in Placement of Self-Exclusion Records

Spikes in self-exclusion occur at the beginning of the year and again near the end of the summer. Both of these periods follow holiday and activity seasons, during which an increase in gambling activity and losses are expected. Self-exclusion reports made up 30% of all evidence placed in our system by gambling operators and platform providers.

Legend: Direct to Account | Direct to Device | Total Evidence Placed | Power (Total Evidence Placed)

Month	Total Evidence Placed
Sep 2015	4,574
Oct 2015	7,316
Nov 2015	10,325
Dec 2015	6,989
Jan 2016	13,414
Feb 2016	7,664
Mar 2016	8,523
Apr 2016	7,556
May 2016	7,340
Sep 2016	7,079
Oct 2016	11,702
Nov 2016	12,180
Dec 2016	9,799

Protecting operators and their self-excluded players

Our comprehensive service includes a self-exclusion tracking feature that enables operators to recognize, protect and respond to problem gamblers in a socially responsible manner. This can be done at both the device and account level. Once self-exclusion is marked on a particular device or account, other operators and platform providers using our service have upfront knowledge of this fact.

Because we are able to link – or associate – multiple devices and accounts, self-exclusion for one device could extend to other devices used by the player. Our device intelligence services are able to add a layer of independent protection to any existing implementation. Our technology is easily integrated into a website using JavaScript or directly into a mobile app through a SDK. Critical touch points such as account creation, login, place bet, deposit funds, etc. are protected with an API call to our services.

For regions with regulatory guidelines regarding self-exclusion, for example, the United Kingdom's National Online Self-Exclusion Scheme (NOSES), our service adds an additional and independent layer of protection based on the devices that players use. This protects players who may try to sign up for additional accounts using different personally identifiable information.

How it works

When a player self-excludes at a specific operator's gambling property, the operator marks the account and/or device as being self-excluded. If the player then comes back to that operator's site, it's affiliate sites, or even other gambling sites in our consortium with the same or related device – and those sites use our services – they will be notified that the player has previously self-excluded.

Recognizing self-excluders across multiple brands and operators

Self-excluded players often attempt to establish new accounts at other unrelated operators' sites by disguising or changing their identity details and/or payment method.
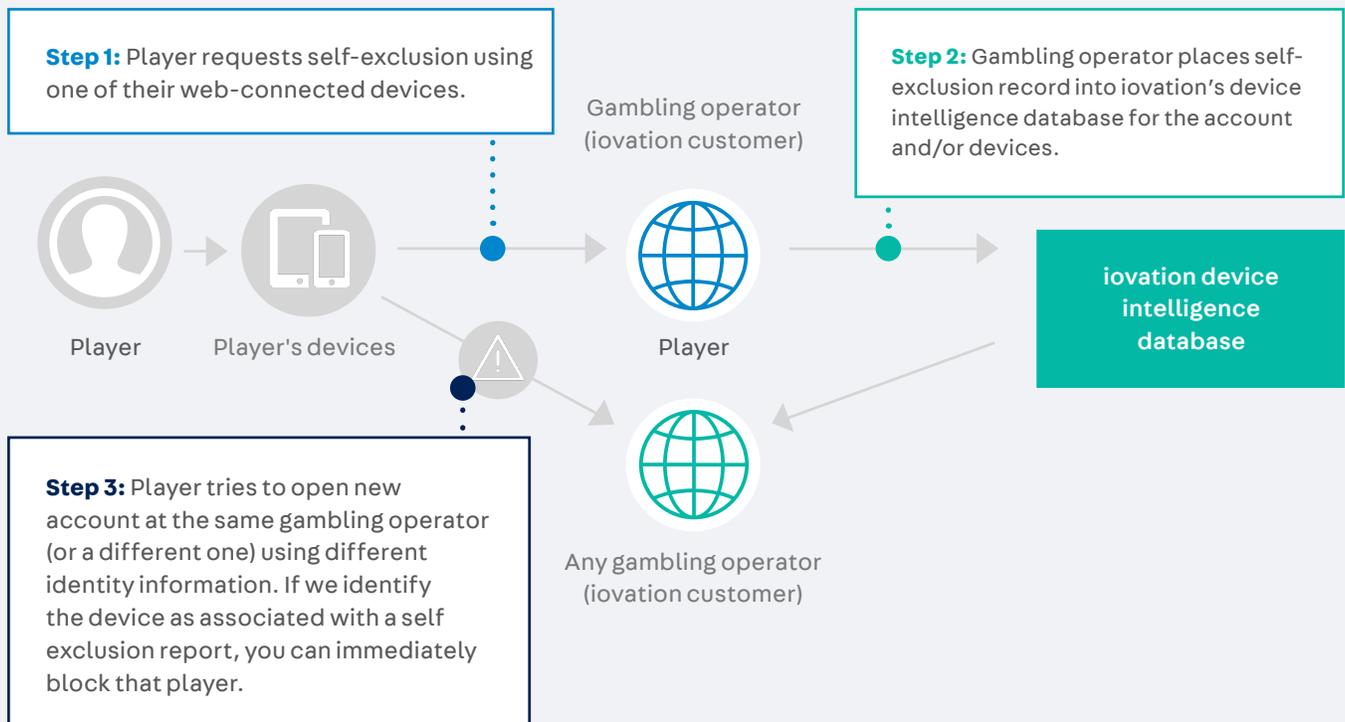
Key Benefits that Promote Responsible Gambling

(?)

Our service is based on global device intelligence and each device is given a uniquely identified, a self-excluded player's device will be recognized and immediately associated to the self-exclusion record in our database, triggering a real-time alert to review or deny the new account.

iovation enables operators and platform providers to:

- ◯ Strengthen social responsibility within your brands

- ◯ Proactively help protect your customers

- ◯ Know when gamblers, who have self-excluded, attempt to establish new accounts

- ◯ Respond to gamblers in a socially responsible manner in real time

- ◯ Avoid regulatory complications and potential liability

- ◯ Prevent self-excluded players from circumventing security measures when they attempt to disguise or change their identity and/or payment method

- ◯ Proactively pair a self-excluded player's group of devices (laptop, smartphone or tablet) to their accounts

Step 1: Player requests self-exclusion using one of their web-connected devices.

Step 2: Gambling operator places self-exclusion record into iovation's device intelligence database for the account and/or devices.

Gambling operator (iovation customer)

Player

Player's devices

Player

iovation device intelligence database

Step 3: Player tries to open new account at the same gambling operator (or a different one) using different identity information. If we identify the device as associated with a self exclusion report, you can immediately block that player.

Any gambling operator (iovation customer)

iovation®
A TransUnion® Company

Get in Touch

Find out more about our authentication and fraud prevention solutions. Contact us for a demo or visit iovation.com

About iovation

iovation, a TransUnion Company, was founded with a simple guiding mission: to make the Internet a safer place for people to conduct business. Since 2004, the company has been delivering against that goal, helping brands protect and engage their customers, and keeping them secure in the complex digital world. Armed with the world's largest and most precise database of reputation insights and cryptographically secure multifactor authentication methods, iovation safeguards tens of millions of digital transactions each day.

iovation®
A TransUnion® Company