2020 iGaming Report

Insights into online gambling fraud and building player trust
Contents

Summary 03

Three Key Market Drivers in iGaming 05

Trust is the New Currency in iGaming 06
Attract and Retain Players With a Mobile-First Approach 06
Threats to Winning in the Mobile Market 07
Balancing Security and Building Player Trust 08

Secure the Player Journey, Secure Your Long-Term Profitability 09
Expedite Onboarding to Grow New Accounts 09
Growth in Bonus Abuse 10
Payment Fraud Growth in iGaming 11

Improve the Customer Experience While Complying with Regulations 12
Social Responsibility and Player Self-Exclusion 12
Shut Down Fraud Rings and Money Laundering Operations 13
Meet PSD2 Requirements 14

Key Takeaways 15
Summary

As the iGaming industry rapidly evolves, new approaches to securing player trust are essential to protecting and growing your business.

iovation, a TransUnion Company, has worked with iGaming operators and platform providers for over 15 years to secure their online operations and improve the player experience. In fact, in that time iovation protected over 4 billion iGaming transactions and stopped tens of millions of fraudulent transactions. In our fourth annual industry report, we’ll share insights gained in 2019 and look at what to expect in 2020.
As players move online, it’s vital that operators protect the entire player journey from account registration all the way through to withdrawal.

Regardless of whether players log in through a website or mobile app, they all rely on their devices. iovation has a device reputation platform built on experience with billions of global devices. With our technology you can improve your digital fraud prevention, expedite player onboarding and provide a friction-right player experience.

---

**FRAUDULENT GAMBLING TRANSACTIONS STOPPED IN 2019**

7,900,000

---

**FRAUD AND ABUSE REPORTS PLACED IN 2019**

927,000

---

**ACTIVE IGAMING OPERATORS AND PLATFORM PROVIDERS**

100+
Three Key Market Drivers in iGaming

Through in-depth analysis of the 483 million gambling transactions we protected in 2019, collaboration with our iGaming customers and conversations with key industry leaders, we have defined three key market drivers that we believe will shape the iGaming industry in 2020:

**Trust is the New Currency in iGaming**

63% of consumers surveyed were deterred from opening an account via a mobile device because of concerns about the security of their information. Meanwhile, new iGaming products are arriving in the market every day, creating more competition and increasing player expectations. It’s never been more imperative to strike the right balance between security and the player experience.

**Secure the Player Journey, Secure Your Long-Term Profitability**

As operators launch in newly legalized markets or work to expand market share, it’s critical to attract new players – but player incentives are under attack. In 2019 we saw bonus abuse reports rise 72%. Equally as important is expediting player onboarding by the automation of functions such as Know Your Customer (KYC), age verification and identity proofing.

**Improve Customer Experience While Complying with Regulations**

Operators have a large number of regulations to comply with, ranging from privacy regulations to identity verification requirements such as age and address validation. It’s important to automate verification checks wherever possible to provide a friction-right experience for good players while ensuring compliance.
Trust is the New Currency in iGaming

Attract and Retain Players With a Mobile-First Approach

While this trend probably doesn’t surprise most, the importance of competing effectively in the mobile space cannot be overstated. In a recent study, 88% of online consumers indicated that they are less likely to return to a site after a bad experience. Additionally, 57% said they would not recommend a business with a poorly designed mobile website.¹

2019 saw continued adoption of mobile in iGaming, outpacing most other industries we help protect such as e-commerce and online banking.

Gambling transactions from mobile devices

https://www.sweor.com/firstimpressions
Threats to Winning in the Mobile Market

Consumers are growing more concerned about the privacy and security of their personal data, which has been amplified by new privacy regulations such as the GDPR and the CCPA. These concerns were echoed in a recent survey we conducted with over 1,600 consumers from the U.S. and the U.K. When asked about the reasons for not opening online accounts using a mobile phone, 65% responded that concern about the security of their information was a factor, with 42% of those indicating it was a major factor.

Respondents indicated the following factored into not opening an online account using a mobile phone:

- 65% of respondents were concerned about the security of their information
- 63% of respondents were concerned about greater risk of fraud
- 61% of respondents were concerned about the slowness or hassle of filling in data on mobile phones

Consumers have good reason to be concerned about the security and privacy of their data. We’ve seen significant growth in fraudulent transactions originating from mobile devices across all industries we work with, reaching 49% in 2019. This is a big jump from 2018 when iovation saw only 30% of risky transactions originating from mobile, a year over year increase of 63%.

---

2019 Financial Services Fraud and Consumer Trust Report
Balancing Security and Building Player Trust

If your customers don’t trust you, they will switch to a competitor. Fraud is a business problem, and from the boardroom to the marketing team to the fraud department, everyone should focus on securing player accounts.³

- **2 OUT OF 5** consumers surveyed stated they have closed an account due to security and fraud concerns
- **2 OUT OF 3** consumers surveyed indicated that they would switch companies for one that has more advanced security protocols in place

While consumers are concerned about the security and privacy of their accounts, this must be balanced with the player experience. Additional authentication can also add friction, so it’s important to consider consumer preferences and which technologies they trust the most. In our recent consumer survey we saw clear differences in authentication preferences between generations and even among different income levels.³

- Younger consumers (ages 18-34) and high income earners ($100K+) showed a preference for biometrics such as fingerprint and facial recognition methods (35% and 36%, respectively)
- Answering security questions was the most trusted method by 44% of consumers aged 55-74 and by 39% of lower income consumers
- For those aged 35-54, we saw an almost even split between preferences, with 32% trusting security questions the most and 31% trusting biometrics the most

Implementing the right strategy that balances security and player experience across digital channels can help protect player accounts, secure player trust and ultimately earn their loyalty.

---

³2019 Financial Services Fraud and Consumer Trust Report
Secure the Player Journey, Secure Your Long-Term Profitability

Expedite Onboarding to Grow New Accounts

As operators launch in newly legalized markets such as the U.S., the Netherlands, Singapore and India, it’s important to consider how you can automate the management of functions such as age and ID verification, Know Your Customer (KYC) and address verification. This has traditionally been a cumbersome process that creates barriers to play.

In a recent study, 87% of consumers agreed that brands need to put more effort into providing a seamless experience, while 90% of surveyed consumers expect consistent interactions across all channels, regardless of whether they are on mobile or web. Taking a mobile-first and friction-right approach enables you to balance a positive player experience while ensuring compliance, and gives you a competitive edge.

- Leverage predictive machine learning to recognize trustworthy customers in real time, even if they’re new to you
- Increase assurance with identity proofing, allowing you to raise betting limits and offer incentives with confidence
- Add geofencing right through your mobile app, allowing you to manage play by geographic boundaries without adding friction
- Authenticate players using their device as a transparent factor of authentication, expediting time to play

\(^{4}F25\) Amazing Omnichannel Statistics Every Marketer Should Know
Growth in Bonus Abuse

Bonuses are vital for attracting and retaining players, especially in newly legalized markets. Unfortunately, these offers also attract fraud and abuse. In fact, bonus abuse was the number one reported fraud by our iGaming customers for the third year in a row. Over the past year we saw bonus abuse reports rise 72%, underscoring just how large this problem is for the industry.

As a result, many operators limit new player deposits and deposit methods to minimize losses, undermining profitability. This is why it’s important to put robust controls in place to safeguard your player acquisition and retention programs so you can confidently grow revenue.

Over the past year we saw a 72% rise in bonus abuse reports.
Payment Fraud Growth in iGaming

iGaming continues to be a prime target for credit card and payment fraud. In 2019 alone, we saw a 37% growth in reports of credit card fraud in the iGaming industry.

Credit card fraud hits operators on a number of fronts. Not only are you out the lost revenue, but there’s also the cost of chargebacks – and if the fraud isn’t caught early, fraudsters can use these illegitimate funds to pocket real winnings. Operators are subsequently met with the challenge of reducing credit card fraud without increasing false declines, reviews and unnecessary step-ups.

Alternative payment methods such as eWallets, bitcoin and direct debits are seeing wide adoption globally. As they increase in usage, you’ll likely see them become a target for fraud as well. Plus, as faster payment services are rolled out by banks and adopted by operators, there will be less time to investigate potentially suspicious transactions. This will make it even more important to implement strong identity verification, and real-time risk decision solutions at all points of the customer journey.
Improve the Customer Experience While Complying with Regulations

Social Responsibility and Player Self-Exclusion

Managing self-excluded players is a challenge that iGaming operators continue to struggle with. Highlighting the scope of this problem, iovation received over 363,000 reports of player self-exclusion in 2019, a 63% increase over last year.

It can be difficult to manage legitimate problem gamblers who can easily move to another site, set up new accounts using falsified account details or even change payment methods, such as using a spouse's personal data and credit card. Another complication is fraudulent self-exclusion claims. This is a tactic often used by fraudsters who set up a new account, deposit funds using a stolen credit card and then self-exclude before the chargeback hits, making it more difficult for operators to pursue them.

Having multiple devices linked to a self-excluded account could point to a self-excluded player trying to use another device to set up a new account, or something more problematic such as a fraud ring. This is why device intelligence is so critical in managing problem gamblers. Plus, iGambling operators with device intelligence have the ability to better understand their players in order to make more informed decisions, and earn their trust.
Shut Down Fraud Rings and Money Laundering Operations

Globally, there was a big uptick in anti-money laundering (AML) fines in 2019. From January to August, **approximately $8.07 billion in AML fines were levied** – an increase of over 4.3 times compared to the same time frame in 2018. While most of these fines were aimed at the financial services industry, we’re seeing an increased focus on iGaming. AML fines were levied against three gambling operators in the U.K., the highest being $7.2 million.⁵

Operators are a prime target for fraud rings or cybercriminals attempting to launder money. One effective method to prevent such abuses is to use device and account associations to uncover hidden connections. Device mapping allows you to associate groups of devices and accounts that are related to one another, offering a clearer picture of what is normal consumer behavior versus a coordinated fraud ring exploiting your service.

⁵Corporate Compliance Insights
TechValidate Source: TVID: 8C2-2B3-3EF
Meet PSD2 Requirements While Providing a Great Player Experience

Many operators are still determining how to meet the Strong Customer Authentication (SCA) requirements under the second Payment Services Directive (PSD2) without adding too much friction to the player experience. The winners will be those that maximize SCA exemptions while implementing seamless authentication for those transactions that require SCA.

Maximize Exemptions

Alternative non card-based payment methods are not subject to SCA requirements, which will likely lead to wide adoption of payment methods such as direct debits and eWallets. It’s important to consider how to secure new payment methods to ensure you do not become a target for fraudsters.

Low risk transactions can also be exempted using transaction risk analysis (TRA) exemptions, and Payment Service Providers (PSPs) are able to request exemptions to SCA if they can attain target fraud rates.

Achieving the highest reference fraud rates will require close collaboration with PSPs, but could provide major competitive advantages. For example, being able to process transactions below 500 rather than the default exemption of 30 will result in cost savings by the reduced number of transactions subject to SCA checks and will reduce player friction.
Key Takeaways

Position your organization to combat threats, transact with higher confidence and secure player trust in 2020:

Continue or increase investment in mobile player experience

While consumers are making the move to mobile, they have never been more aware of their account security with 2 out of 3 surveyed consumers indicating that they would switch companies for one that has more advanced security protocols in place. Providing a secure and friction-right mobile experience has never been more important for competing effectively in the iGaming market.

Put data identity at the center of your fraud detection and authentication strategies

Fraudsters are continually evolving and adapting their techniques.

- Bonus abuse, payment fraud and other game abuses are still on the rise
- It’s never been more important to confidently identify good players
- Robust identity verification, device intelligence and friction-right consumer authentication are needed to optimize the entire player journey

Use device-based intelligence to create a friction-right experience that ensures compliance

Operators are contending with an increasingly complex regulatory environment.

- AML fines increased 4.3 times over 2018, making it critical to uncover and shut down fraud rings
- Managing and preventing self-excluded players from creating new accounts requires industry-wide collaboration
- Maximize exemptions while reducing friction for SCA transactions
ABOUT IOVATION

Get in Touch

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.

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

Global Headquarters
iovation, a TransUnion Company
555 SW Oak Street, Suite #300
Portland, OR 97204 USA
PH +1 (503) 224 6010
EMAIL info@iovation.com

United Kingdom
PH +44 (0) 800 058 8731
EMAIL uk@iovation.com

iovation.com