TransUnion

Optimising Performance in the Gaming Industry:

Countering Fraud and Financial Crime Threats in 2023

The current state of play:

Understanding the impact of digital crime on the UK gaming industry

In the 2023 State of Omnichannel Fraud Report, TransUnion brings together trends, benchmarks and expertise from across our identity and fraud prevention organisation. It provides insight and recommendations to those responsible for preventing fraud and streamlining online experiences to deliver better business outcomes.

4%

Digital fraud threats in the gaming industry increased by 4% between 2021 and 2022[1]

TransUnion 2023
State of Omnichannel
Fraud Report

Trends and strategies for enabling trusted commerce

Download

The current state of play:

Understanding the impact of digital crime on the UK gaming industry

Globally, in 2022, fraud returned to something closely resembling pre-pandemic levels. That said, with increased digital transaction volumes, the risk to organisations and individuals was even greater than before. Cybercriminals and fraudsters continued to show increasing sophistication – with stolen identity information at the centre of their strategies.

Despite these global trends, the UK gaming industry experienced a **4%** increase in suspected digital fraud threats between 2021 and 2022,[1] making it the second most impacted industry for suspected fraud growth in the country.

Currently the world's largest online gaming market (worth over £14.3bn per year), it's no surprise the UK gaming sector has become a target for organised crime and fraudulent activity. As economic uncertainty sustains and fraudsters adapt their tactics to meet changing consumer behaviours, instances of fraud continue to test gaming operators' fraud controls and impact bottom lines.

Of course, fraudsters don't respect national boundaries, which is evidenced by this trend continuing worldwide. The gaming industry experienced an **8%** digital fraud attempt rate in 2022[2] — the highest of all the sectors our global device intelligence network reports on — with promotion abuse and licence agreement violations, such as multiple accounts, being the most prolific.

As many UK gaming operators look to pursue growth and expand their operations internationally, there's a golden opportunity for them to reduce fraud risk and improve overall customer experience (CX) through cutting-edge, multilayered fraud and identity solutions.

In this guide, TransUnion brings together proprietary research, prevailing digital crime trends and actionable advice to help gaming operators mitigate the risk of fraud without sacrificing the safe, seamless transactions consumers have come to expect.

1 IN 7

One in seven people have committed online gaming fraud or know someone who has[3]

8%

Globally, the gaming industry had the highest suspected digital fraud attempt rate of 8%[4]

Top fraud and digital crime trends facing the gaming sector

There are many different types of fraud impacting on the gaming industry, meaning it's crucial to identify emerging trends and provide tips to help spot them. Working with our own datasets and research, and partnering with customers, TransUnion gaming SMEs identified several key criminal threats currently facing the UK industry. These occur at different stages of the customer lifecycle, underlining the importance of knowing your customer (KYC) and building trust during transactions.

£5m

It's estimated bonus abuse costs top tier gaming operators up to £5m each year.[5]

Top fraud and digital crime trends facing the gaming sector

Bonus abuse

Bonus abuse, also known as promotion abuse, continues to be one of the most prevalent threats facing gaming operators. With a suspected digital fraud attempt rate of **8%**,[6] it's estimated bonus abuse costs top tier gaming operators up to £5m each year.[7]

While bonus abuse comes in many forms, there are four types popular with fraudsters:

1

Collecting signup bonuses: Used to cash out their promotional offers with or without playing

2

Collusive play: Fraudsters can control multiple players in order to defraud unsuspecting, legitimate customers

3

Chip dumping: Similar to a collusive player, this takes place when a poker player intentionally "loses" their chips to another player in order to affect the outcome of a hand

4

Arbitrage: Placing bets simultaneously to increase the winning odds on betting platforms

Bonus abuse can be achieved through the use of compromised names, disposable email and phone numbers, and sometimes stolen debit card details, making this type of fraud notoriously difficult to detect. This creates a proverbial Catch-22 for fraud leaders: Either to enhance fraud controls and strengthen KYC checks and risk an increase in false positives that could deter genuine players or loosen these controls in favour of a better customer experience which could leave operators open to fraud losses, reputational damage and regulatory fines.

Top fraud and digital crime trends facing the gaming sector

Bonus abuse

Steps to detect and prevent bonus abuse

While fraudsters have increased the sophistication of their bonus hunting, their reliance on false identifying information and weak onboarding checks give gaming operators an advantage to prevent this fraud. **Steps operators should consider include:**

Device Risk with Behavioural Analytics at registration, and Device Risk at login and pay out:

Leverage device history, user behaviour insights, device-to-device and device-to-account associations from our global network to better detect and prevent instances of successful bonus abuse. By successfully screening suspicious form fill behaviour and device associations, additional risk checks can be applied to these individuals without impacting on the user journey for legitimate customers.

Create more complex bonus rules:

To reduce losses stemming from bonus abuse, consider implementing strict withdrawal requirements and/or rollovers where players must play the bonus amount multiple times before withdrawal.

Email and mobile verification:

Risk profiling email and mobile details can validate connections, assess risk indicators, and strengthen KYC checks to help identify and prevent instances of bonus abuse. For example, newly created email addresses being used to access promotional offers can be a strong indicator of fraudulent activity.

Utilise DataDNA and Real-Time Fraud Alerts (RTFA) to enhance responsible gaming:

An increasing number of consumers are opening more than one account with UK gaming operators. While some may do this to perpetrate bonus abuse, others may utilise this method to artificially inflate the amount of money they're able to spend. As those who suffer from gambling harms often hold multiple accounts or can open new ones easily, this behaviour is currently under increased scrutiny from the regulator and was called out in the government's recent Gambling Reform Whitepaper.

DataDNA can help operators meet these responsible gaming concerns whilst also curbing potential instances of bonus abuse by creating a single customer view across their consumer books. Designed to match consumer data to deliver a unique and persistent DNA number, this robust view highlights multiple relationships with each individual, even in circumstances where changes — such as those to names or addresses — have occurred over time. The use of Real-Time Fraud Alerts can also help operators overcome these issues. With the flexibility to derive fraud rules aligned to their fraud strategies, operators can return alerts to pinpoint suspicious activity of consumer data seen within TransUnion's network, helping reduce both risk and false positives.

Top fraud and digital crime trends facing the gaming sector

ID theft

Identity fraud is a growing problem across the UK; identity theft directly impacted over **13%** of consumers in 2022.[8] And as consumers increasingly fall victim to this type of fraud, the number of businesses being targeted — including those in the gaming sector — also continues to increase.

As consumer habits change, such as the shift toward online gambling necessitated by the COVID-19 pandemic, identity thieves continue to exploit new ways of stealing personal information and perpetrating identity fraud. In fact, between **2.5%–5%** of new players onboarded by gaming operators in the UK do so using fake identities.[9] However, because of improvements in KYC checks and other fraud controls, the majority of these identities were legitimate, stolen identities rather than synthetic ones.

Steps to detect and prevent ID theft

While identity theft is prevalent across several industries, fraud prevention leaders can take learnings from one another to help curb this type of fraud. **Strategies operators should consider include:**

Device Risk with Behavioural Analytics at registration, and Device Risk at login and pay out:

Gaming operators can utilise device history, user behaviour insights, device-to-device and device-to-account associations from our global network of billions of devices and transactions to better detect the use of synthetic or stolen identities. In instances where suspicious behaviours or devices are flagged, operators can add additional fraud controls without impacting the CX of legitimate customers.

International ID verification at registration:

Real-time international identity verification enables operators to make faster, more reliable identity decisions with match rates of up to **92%**.[10]

Utilise consortia and previous search data:

Detect patterns and uncover anomalies by widening the use of consortia and previous search data.

Top fraud and digital crime trends facing the gaming sector

Account takeover

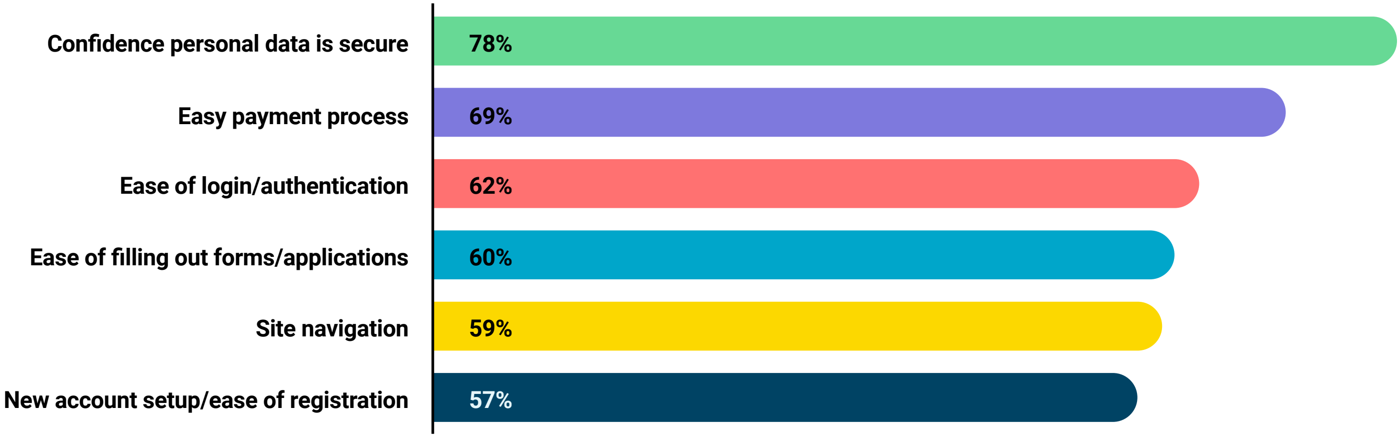
Global instances of account takeover fraud (ATO) increased by **81%** between 2019 and 2022,[11] costing the gaming industry billions each year. Often a direct result of ID theft, it's no surprise increased incidences of these types of fraud make account takeover a top concern for **41%** of UK consumers.[12]

As our reliance on and usage of online accounts accelerates with the digital age, consumer expectations for convenient, secure transactions continue to soar with security of personal data ranked as "very important" by **78%** of UK adults.[13]

There is, therefore, increased pressure on gaming operators to provide secure experiences that protect players from digital crime without compromising on the ease-of-use that attracts players in the first place.

Consumer concerns

Stated important - very important features when choosing who to transact with online



Top fraud and digital crime trends facing the gaming sector

Account takeover

Steps to detect and prevent account takeover

Consumer trust is essential to establish long-lasting and profitable player relationships. With account takeover repeatedly being named as a top concern for consumers, operators should consider:

Device authentication at login:

21% of consumers named device authentication as one of their preferred online security measures.[14] Authenticating devices at login using Device Risk and Device- Based Authentication reduces the likelihood of a successful account takeover without adding unnecessary friction for the customer.

Utilise multifactor authentication, such as one-time passcodes (OTP):

One-time passcodes are a valuable tool in helping prevent incidences of account takeover. While adding an extra layer of protection to player accounts, it's also favoured by most UK adults; **52%** named an OTP sent via SMS as their preferred security measure followed by email OTP (**40%**).[15]

Risk assess changes made to accounts:

Including email, direct debit or mobile, these are common elements of account takeover activity.

Get ahead of the game:

What's next for operators wanting to thwart fraud threats?

Forty-nine percent of UK consumers ranked the security of their personal data as their top expectation from online companies.[16] As more of our lives move online, it's no surprise customers increasingly value the security of their information and expect more from the companies that hold that data.

To successfully win out over competitors and secure growth in new markets, an effective and robust fraud and identity strategy is key. In order to achieve this, there are several levers gaming operators can use to strengthen efforts to better detect and prevent digital crime.

From a technology perspective, advances in data solutions are helping operators better spot the signs of fraudulent behaviours. TransUnion is the leading provider of ID verification for gaming operators in the UK, and our robust fraud and AML solutions designed specifically for the gaming sector enable leaders to better protect players and meet regulatory requirements. Our recent product release, Device Risk with Behavioural Analytics, also enables fraud prevention leaders to reduce false positives and identify risk by uncovering device behaviour, user behaviour and risk indicators in real time based on our platform's knowledge of billions of devices and transactions, and NeuroID's one trillion behaviour signals. In addition, our proprietary global device intelligence database and acquisition of businesses, such as iovation, Neustar and Sontiq, are helping operators counter increasingly sophisticated criminal activities.

57%

57% of consumers rank the ease of registration as "very important"[17]

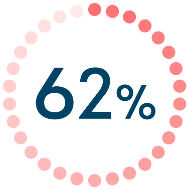
Get ahead of the game:

What's next for operators wanting to thwart fraud threats?

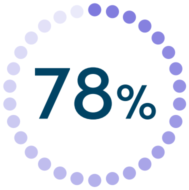
At a strategic level, leaders in the gaming sector should also think about ways to link to one another and other industries and share outcome data to better spot digital crime. This was called out in the recent Gambling Reform Whitepaper as The Gambling Commission looks to consult on mandating participation in a cross-operator, harm prevention system based on data sharing. Working with partners that can support fraud analytics, diversify data sources, and engineer optimal fraud prevention strategies could therefore not only help operators prepare for upcoming regulatory changes but also deliver business-wide benefits. TransUnion research found consumers rank the security of their personal data (**78%**), ease of registration (**57%**) and ease of authentication (**62%**) as "very important,"[18] emphasising the value of utilising experts who understand how to craft optimal consumer journeys.

Additionally, the release of the Gambling Reform Whitepaper, and regulatory focus on responsible gaming and the new Consumer Duty may impact operators and how they provide players with access to their products. The common denominator here is the need for operators to have access to rich, actionable data sources and better consumer insights.

Readers should use this guide to evaluate their current fraud prevention programmes in the context of the broader market. This information and insight should be shared across the organisation with the goal of securing growth through effective fraud prevention and safer, more convenient customer experiences.



62% of consumers rank the ease of authentication as "very important"[19]



78% of consumers rank the security of their personal data as "very important"[20]

Time to take action?

If you'd like to get an expert view of how fraud and digital crime is impacting your business, or understand how our TruValidate™ solutions could complement your fraud strategy, get in touch:

Contact us

Glossary

This guide blends proprietary insights from TransUnion's global intelligence network, third party research, TransUnion UK's Consumer Pulse study, and a specially commissioned TransUnion consumer survey in 18 countries and regions globally. TransUnion TruValidate™ suite comprises identity and fraud products that secure trust across channels and deliver seamless consumer experiences.

[1] TransUnion TruValidateTM global intelligence network

[2] TransUnion TruValidateTM global intelligence network

[3] Gaming Sector | Cifas

[4] TransUnion TruValidateTM global intelligence network

[5] Data from an anonymous UK gaming operator

[6] TransUnion TruValidateTM global intelligence network

[7] Data from an anonymous UK gaming operator

[8] TransUnion Consumer Pulse Survey

[9] Data from an anonymous UK gaming operator

[10] truvalidate-gaming-global-fraud-id-solutions-asset-sheet.pdf (transunion.co.uk)

[11] TransUnion TruValidateTM global intelligence network

[12] TransUnion Global Fraud Survey

[13] TransUnion Global Fraud Survey

[14] TransUnion Global Fraud Survey

[15] TransUnion Global Fraud Survey

[16] TransUnion Global Fraud Survey

[17] TransUnion Global Fraud Survey

[18] TransUnion Global Fraud Survey

[19] TransUnion Global Fraud Survey

[20] TransUnion Global Fraud Survey

TransUnion

TransUnion TruValidate™

Our TruValidate™ solutions encompass identity, device and behavioural insights to help organisations confidently and securely engage consumers at each stage of the customer journey, helping improve conversions, reduce fraud losses and deliver enhanced, friction-right user experiences.

For more information on how to enhance your fraud prevention strategies, get in touch:

transunion.co.uk

Registered office: One Park Lane, Leeds, West Yorkshire LS3 1EP.
Authorised and regulated by the Financial Conduct Authority.