

## **BUSTED:**

# The Top 5 Myths About Online Gaming and Fraud



## Contents

- 3** Introduction
- 4** **Myth 1:** Fraud is not a significant problem in gaming
- 6** **Myth 2:** My payment controls will stop fraud
- 8** **Myth 3:** Identity verification and fraud checks at onboarding annoy our players
- 9** **Myth 4:** There's no ROI to KYC
- 11** **Myth 5:** All KYC and fraud prevention is the same



---

The gaming industry has not quite realized the danger of advancing fraud threats. But it's hard to fault operators who prefer to stick to the status quo.

---

## Introduction

Identity fraudsters are increasingly targeting online gaming platforms and their customers—and reaping substantial rewards. The gaming industry has not quite realized the danger of these advancing fraud threats . . . but it's hard to fault operators who prefer to stick to the status quo. Effective fraud prediction gets more complicated every day. It's understandably tempting to ignore the circling cyber fraudsters—and the risks they pose to revenue, resources, and reputation.

At Socure, we've fortified top online gaming operators against the looming threats of fraud and work closely with many in the field. In this guide, we break down the five most common identity verification and fraud prevention misconceptions we hear from online gaming professionals like yourself—and show you how to keep these outdated misconceptions from holding you back from safe, scalable growth.

## MYTH

## Fraud is not a significant problem in gaming

As any experienced player knows, winning is a mix of risk and reward. Gaming operators often perceive fraud prevention as a low risk, low reward pursuit. Many think it is not a significant problem, so they don't see the point in spending time and resources exploring how to solve identity theft, synthetic identity fraud, or any of the other vulnerabilities that fraudsters exploit.

Operators who do recognize fraud as a problem often see it simply as a cost of doing business. With the fast pace of growth across the online gaming industry, most operators have instead focused on growing their player base, scaling their platforms to meet demand, and other competitive challenges.

## TRUTH

## Fraud rings are targeting online gaming—and the impacts are substantial

**Fraud follows money and opportunity. Today's online gaming industry is overflowing with both.**

As the volume of online gaming has grown dramatically over the past few years, so has the allure for fraudsters. They know how to identify risk control gaps in any type of fast-paced, high-value arena.

Within Socure, we've seen several highly sophisticated fraud rings attempting to attack our online gaming clients. These attacks could have resulted in substantial financial losses, damage to relationships with payment providers and networks, and significant operational burn-in for those providers. Luckily, our clients were already leveraging Socure's fraud suite to prevent that destruction. Any perception that fraud is not a significant problem for online gaming likely means that fraudsters are simply going undetected in your system, along with the true scale of the associated losses.

## 1 in every 20

new digital gaming accounts created is connected to online gaming fraud<sup>1</sup>

Up to  
**50%**

of daily traffic in online gaming is made of bot attacks during peak periods<sup>1</sup>

### KEY TAKEAWAY

These fraud rings aren't new, but they are increasingly nefarious. Online gaming operators that have experienced attacks know the high costs all too well. And for those who have yet to be targeted, it's only a matter of time: better to learn from others' mistakes and get ahead than deal with the hefty fines and damaged reputation following a costly attack.



## MYTH

## My payment controls will stop fraud

Many operators simply check for fraud at payment withdrawal and think they're covered. After all, if money is checked at the point when it comes in or out, that means the fraud can be identified and stopped at the crucial point of fund transfer, right?



### What is Synthetic Identity Fraud?

Synthetic identities are created through a mix of real and fake (or wholly fake) personal information that is then used to open an account. When that synthetic identity goes on to open a real-world account, it's synthetic identity fraud. Younger people—that is, gaming industry's prime demographic—are the prime target for synthetic identity fraudsters, who use the fact that the 20-something and under crowd likely have little to no credit history, so are less likely to be flagged by banks when applications are made in their names under false identities.

## TRUTH

## Fraud risk starts at onboarding—and so should fraud management

Relying on payment controls for fraud prevention dangerously assumes that all accounts are legitimate. Synthetic identity fraud and similar financial crimes take advantage of this assumption: they use a fictitious identity to open a real account that will fly under the payment control radar.

Banks are notoriously bad at detecting synthetic identity fraud.<sup>3</sup> Fraudsters can easily set up a synthetic bank account, break through payment controls, and “bust out” with your money before they're tracked. The reality is, if you're only stopping fraud at payment, then synthetic identity fraudsters have already beaten the system because once they're “in,” they appear to be legitimate. They've wagered and withdrawn money before you can stop it.

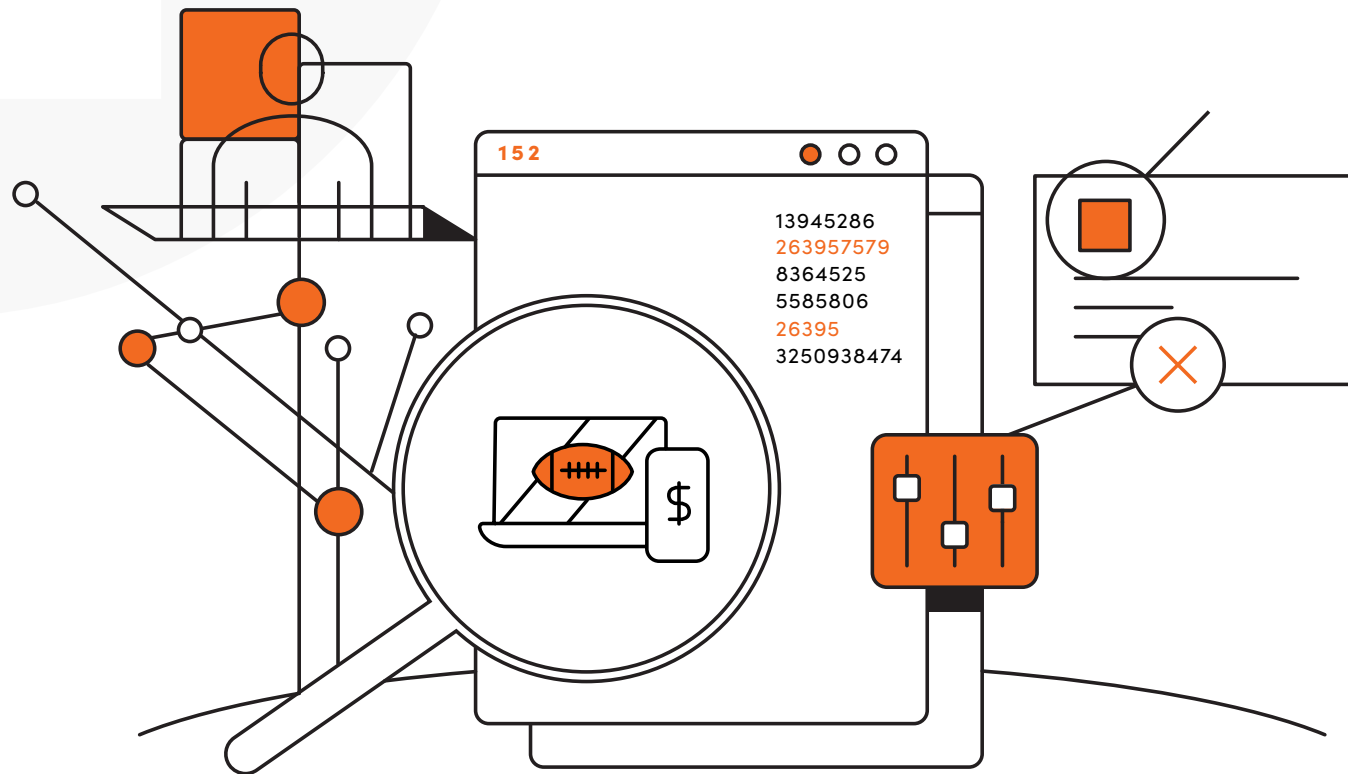
In addition, alternative payment methods, such as eWallets and cryptocurrency, are only going to continue to grow in popularity and become bigger targets for fraud.<sup>4</sup> As banks roll out faster payment services, operators will have very limited time to investigate suspicious transactions at the point of payment.

Identity verification and fraud prediction that takes place right at onboarding—and ensures that fraudsters don't have the chance to exploit vulnerabilities in money movement—is the best way to lock the door on bad actors.

Identity verification and fraud prediction that takes place right at onboarding is the best way to lock the door on bad actors.

### KEY TAKEAWAY

Fraudsters excel at evading payment controls. If you're only checking for fraud at payment control, you're likely letting a lot of bad actors into your ecosystem. Modern identity verification and fraud prediction solutions that measure fraud indicators right at onboarding are a much more effective way to ensure only the most trustworthy players get into your platform.



## MYTH

## Identity verification and fraud checks at onboarding annoy our players

The last thing operators want to do is spoil players' fun—or even slow it down—with a cumbersome onboarding experience. Operators need to pull players into the platform with a fast and frictionless process: identity verification is an unnecessary buzzkill at a crucial point during onboarding.



## TRUTH

## The right identity verification solution is invisible and invaluable

Onboarding is always a delicate balance of user experience and security protocols. The best identity verification solution uses advanced technology, such as predictive machine learning, to recognize trustworthy players almost immediately without making players wait hours—or even days—for identity checks or manual reviews. With the right solution, operators can overcome these challenges and provide a safe, rapid, seamless onboarding process that protects the player experience while mitigating risk.

For example, Socure's identity verification and fraud platform uses predictive risk signals and advanced algorithms specifically targeted at detecting any new levels of identity fraud across Socure's extensive consortium of customer data. This means that the more a fraudster tries to break through, the smarter Socure's machine learning gets at recognizing them, and the harder it is for them to perpetrate fraud. This level of sophisticated identity verification is built on technology that was created to reduce friction while increasing accessibility and accuracy. With this best-in-class identity verification, you can not only quickly authenticate players and expedite their time to play, but also confidently increase betting limits and GGR.

## KEY TAKEAWAY

The best identity verification and fraud prediction solutions are built to keep onboarding seamless and identities secure. A best-in-class solution will detect and deter fraudsters, while staying nearly-invisible to the good players you want to pull in at onboarding.



## MYTH

## There's no ROI to KYC

Online gaming operators are legally obligated to verify user identity, age, location, and other categories to protect their users and platform from bad actors and fraud—those are baseline Know Your Customer (KYC) requirements.

Without effective KYC, platforms are at risk of money laundering and other fraud, along with the associated sky-high non-compliance fines from regulators.

As a result, many operators approach KYC as a simple checkbox meant to appease regulators, and nothing more.



## TRUTH

## The right KYC approach has a direct impact on revenue

Providing accurate and seamless KYC verification with minimal friction dramatically increases player conversion rates, which in turn improves player lifetime value, GGR, and customer acquisition costs. Plus, it saves operators from paying regulatory fines in the future. A best-in-class KYC solution provides a broad array of data sources across each player's entire identity, including email, phone, device, address, IP, geolocation, DMV, insurance data, and more, to ensure operators can fully trust players and thus reward them with higher handle limits and optimize lifetime player value.

**In summary, with better KYC, you get better auto-approval for a vast increase in player accounts: a direct line to your bottom line.**

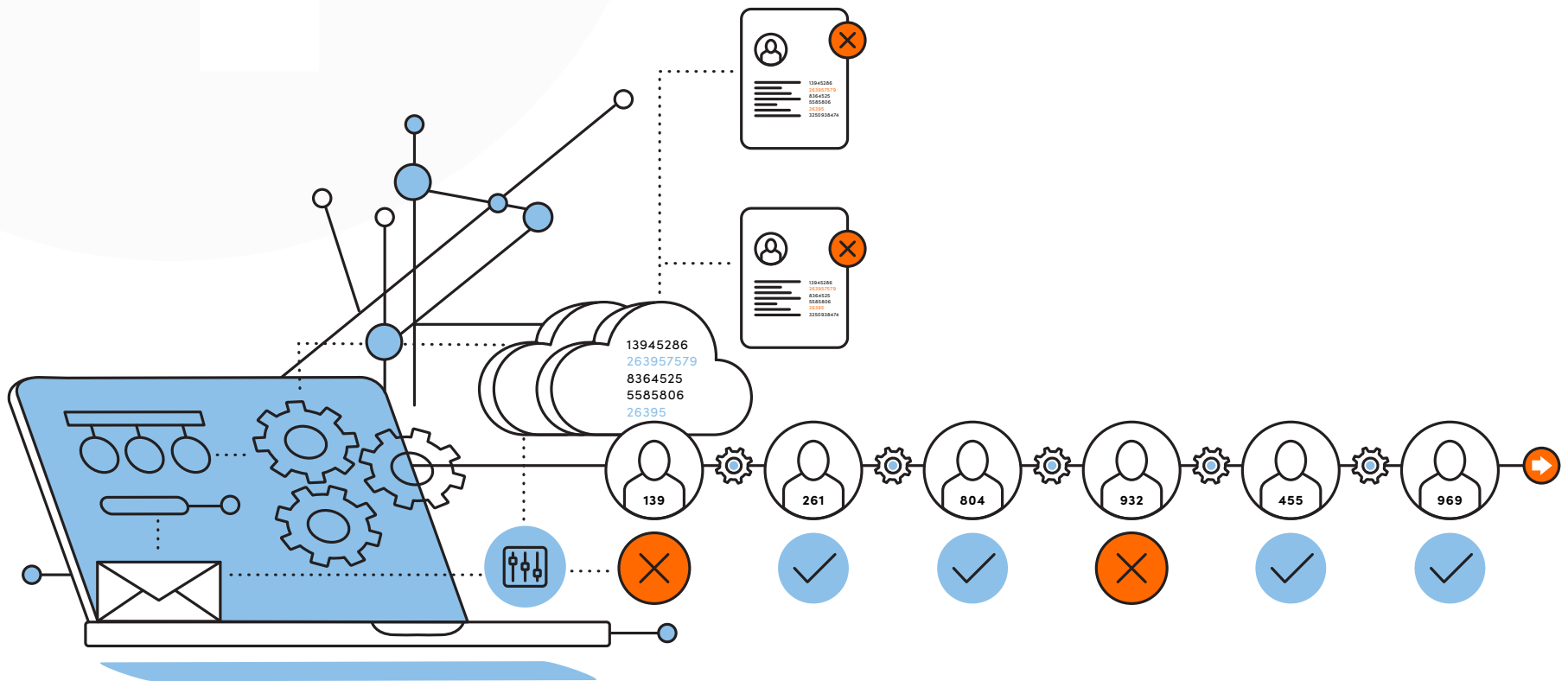
In addition, KYC is a key component to preventing money laundering. Just like fraudsters pay attention to the volume and velocity of money movements, regulators pay attention to vulnerabilities for different technologies. Anti-money laundering (AML) fines have been steadily increasing across the online landscape, with more than \$2B in fines issued in 2021 alone. While banks and financial institutions bore the brunt of those wrist-slaps, the fact that banks are actively trying to avoid those fines by locking down money laundering gaps will likely lead to fraudsters seeking new outlets—and digital gaming is a prime target. In fact, in 2019, major AML fines were levied against three digital gaming operators in the U.K., with the highest having to pay more than \$7.2M. Regulators in the U.S. have started paying even closer attention since then, as the scrutiny and need for strict AML compliance is growing in parallel with the online gaming industry.<sup>5</sup>

**“You must establish and implement procedures for using all available information to detect and report suspicious transactions, or suspicious patterns of transactions.”**

– FinCEN Director Kenneth A. Blanco

**KEY TAKEAWAY**

KYC is more than just a compliance checkbox to save you from costly fines: it’s a bottom-line revenue-driver. Working in tandem with fraud prevention goals, KYC ensures that you’re only dealing with qualified players and are able to trust them with higher handle limits for a greater lifetime player value.



## MYTH

## All KYC and fraud prevention is the same

With the explosive growth of the gaming industry, it's easy to consider KYC and fraud prevention approaches as just one more to-do on a list of problems to solve. Many operators take a set-it-and-forget-it approach to just get something onboarded quickly without looking at how it might compare across the market, because in the end they see KYC and fraud as basic frameworks that don't have value beyond their immediate purpose.



## TRUTH

## There are material and empirically provable differences across providers

Legacy KYC and fraud prediction systems can slow performance and response time at onboarding. In addition, if your legacy fraud system isn't sophisticated enough to verify and authenticate the younger, likely credit-invisible players who make up a prime market for gaming, then you're missing out on revenue.

Even if your KYC is aligned to regulatory requirements for compliant identity verification, players can still submit fraudulent identification details. The result: a fraudster gets past KYC by hiding behind valid identity elements, but the presented identity doesn't actually belong to that player (an example of synthetic identity fraud).


A sophisticated online fraud prediction solution is incomplete without integrated best-in-class KYC that ensures that only the most lucrative and trustworthy players are allowed into your platform. KYC solutions have considerable differences in terms of friction, population coverage, and data quality—and all of those factors impact conversion and revenue.


## KEY TAKEAWAY

Look for a KYC and fraud prediction solution that can empirically show its value through categorical revenue drivers such as higher player conversion rates, improved auto-approval rates, better fraud detection, and more.

**4-7%** Improve auto-approval rates to maximize player conversions

**14%+** Reduce manual reviews to decrease operational costs

 Reduce fraud losses & improve fraud capture rates

 Trusted by leading companies including 7 top online gaming operators



## Socure: Built for the reality of today's digital gaming world

It's never been more critical to let only the right players into your system. With Socure, operators can fully trust the players in their platform, reward them with higher handle limits, and optimize lifetime player value at scale.

Socure has helped leading gaming platforms auto-accept up to 97% of new customer applications, even from hard-to-identify or thin-file populations—including the younger generations that are often gaming platforms' prime customers and growth segments. Socure also helps operators achieve fraud capture up to 90% in the riskiest populations of users, and significantly reduces manual reviews and bad declines on overall transactions, opening the doors to increased revenue and automation for scale.

With the largest pool of known good and bad identities to verify against, Socure utilizes a broad array of data sources across each player's entire identity, including email, phone, device, address, IP, geolocation, ID document, insurance data, and much more. Socure delivers the most accurate KYC, identity verification, and fraud risk prediction solution in the industry by applying in-depth data science to determine identity. Socure's identity verification and fraud prediction solution delivers the highest degree of accuracy on the market, so gaming operators can use identity verification and fraud prediction in strategic ways that will raise both their gross gaming revenue (GRR) and the bar for competitors.

### Sources

- 1 [Chargebacks 911: Online Gaming Fraud](#)
- 2 [TransUnion: As COVID-19 Lockdowns Lift, Fraudsters Shift Focus](#)
- 3 [Socure: Synthetic Identity Fraud Attacks: How Banks and Fintechs Are Fighting Back](#)
- 4 [PewTrusts: Cryptocurrency Fraud Soars, Spurring State Action](#)
- 5 [Nasdaq: 5 Lessons From AML Bank Fines of 2021](#)



Ready to get started?

**SPEAK WITH AN EXPERT**

#### About Socure

Socure is the leading platform for digital identity verification and trust. Its predictive analytics platform applies artificial intelligence and machine learning techniques with trusted online/offline data intelligence from physical government-issued documents as well as email, phone, address, IP, device, velocity, date of birth, SSN, and the broader internet to verify identities in real time. The company has more than 1,800 customers across the financial services, government, gaming, healthcare, telecom, and e-commerce industries, including four of the top five banks, 13 of the top 15 card issuers, the top three MSBs, the top payroll provider, the top credit bureau, the top online gaming operator, the top Buy Now, Pay Later (BNPL) providers, and over 250 of the largest fintechs. Marquee customers include Chime, SoFi, Robinhood, Gusto, Public, Stash, DraftKings, State of California, and Florida's Homeowner Assistance Fund. Socure customers have become investors in the company including Citi Ventures, Wells Fargo Strategic Capital, Capital One Ventures, MVB Bank, and Synchrony. Additional investors include Accel, T. Rowe Price, Bain Capital Ventures, Tiger Global, Commerce Ventures, Scale Venture Partners, Sorenson, Flint Capital, Two Sigma Ventures, and others.