

Money laundering in video games

A compliance argument written for people who do not play games, about an economy that behaves like a bank and is regulated like a toy shop.

WHITE PAPER, ROUGHLY 1,800 WORDS, WITH THREE CASE STUDIES

AUDIENCE	Compliance officers, regulators, platform policy teams
PROBLEM	The reader has to care about a subject they think is trivial
APPROACH	Open on scale, prove with named cases, close on the gap in oversight

Written by **Konstantinos Chatzimichail**. Marketing design, creative production, content and growth strategy.

WRITING SAMPLE

Once upon a time, video games were digital playgrounds. Today they are billion-dollar ecosystems, and criminals have noticed. This paper looks at how illicit funds are cleaned through in-game economies, digital goods and cryptocurrencies, and at why the response so far has been a patchwork.

01 Where real money meets virtual worlds

Gaming has gone from joystick fun to serious business inside a decade. The global industry is now worth more than two hundred billion dollars and shows no sign of slowing. But as games evolved, bringing in microtransactions, tradeable virtual goods and in-game currencies, they opened a door to something more dangerous than a final boss.

Criminals use illicit funds to buy digital assets, trade them across platforms, and cash them out as clean money. It is fast, it is close to anonymous, and for now it is mostly unchecked.

02 How it works

At its core, laundering is simple: turn dirty money into clean money. In gaming it runs in the same three steps it runs anywhere else.

PLACEMENT	Illicit funds buy in-game items or currency.
LAYERING	Those items are traded or resold across accounts and platforms, often through third-party marketplaces.
INTEGRATION	The cleaned value is cashed out through sales or exchanges, and arrives looking legitimate.

Gaming offers useful cover: global player bases, frequently anonymous transactions, and decentralised economies with little oversight. Not every game is equally exposed. The ones most at risk have real-money marketplaces, tradeable items or currency, and weak tracking.

03 Three cases that should raise eyebrows

CASE 01

In one court case, hundreds of users on a large user-generated platform were flagged for potential laundering. The method was disarmingly simple: buy the platform currency with illicit funds, then resell it to other players at a discount. Clean money out, dirty money gone, and on a platform with tens of millions of users that activity blends in easily.

CASE 02

A competitive shooter with one of gaming's most vibrant in-game economies let players unlock loot boxes by purchasing keys with real money. An investigation found those keys being bought in bulk with stolen funds and resold to unsuspecting players. The developer eventually shut key trading down altogether: a bold move that came only after the system had been deeply compromised.

CASE 03

And on a battle-royale title with a global player base, criminals bought virtual currency in bulk using stolen card data, then offloaded it through third-party marketplaces at a discount. The scam relied on the same payment rails everyone uses, cloaked beneath the casual act of buying another skin.

04 The new currency of crime

Buying game currency with a stolen card is amateur hour compared to what blockchain integration made possible. Non-fungible tokens, once presented as the future of digital ownership, double neatly as a laundering instrument. A launderer buys one with dirty cryptocurrency, flips it to another wallet that may also be theirs, and resells it for clean funds. There is no bank to flag the transfer, no identity check, and no border.

Cryptocurrency itself is now embedded in the mechanics of countless games. In play-to-earn models users earn tokens by completing missions or crafting items. If a criminal earns those tokens through fake or stolen accounts, they can convert them into real-world cash. Others go further and inject illicit crypto directly into a game economy, buy high-value items, and flip them outside the platform.

What makes this dangerous is that it is close to invisible to the systems we currently rely on. Anti-money-laundering frameworks are built around banks and institutions. In a decentralised environment where users transact without revealing identity, those frameworks have no central point of control to attach to.

05 Patching the problem, and why it is not enough

Developers are trying. One shut down the abused trading mechanism entirely, which was decisive and also wiped out a legitimate secondary market players had used for years. Another added restrictions on trading and selling, plus reporting tools, and schemes still slipped through. A third added two-factor authentication and better transaction monitoring, and closed loopholes as it found them.

All of them are struggling with the same impossible balance: how do you crack down on abuse without ruining the experience for the overwhelming majority who are just there to play? And the harder truth underneath it is that these platforms were never built for forensic monitoring. Most studios are not equipped, technically or operationally, to act like banks. Which is exactly why this cannot be solved by developers alone.

06 The missing piece is oversight

Banks, financial apps and fintech platforms are subject to strict anti-money-laundering law. They monitor transactions, verify identities, report suspicious activity and keep audit trails. Games get a pass, because they are not officially financial institutions. But introduce in-game currencies, real-money trading and blockchain assets, and the line blurs. Criminals thrive in exactly that grey.

Part of the answer is regulatory: bringing some elements of the gaming economy under the same compliance umbrella as financial services, with player verification, monitoring of high-risk transactions, and clearer guidance on how platforms let people cash out. But regulation alone is not enough. What is missing is a coordinated authority that can watch the intersection of gaming and financial crime, and whose job is to help platforms build better systems and share intelligence, and not only to hand out penalties.

07 The final word

Video games are no longer just games. They are digital economies, social networks and borderless marketplaces, and they are increasingly being used as instruments of financial crime. The loopholes are real and they are in use. Without clear frameworks, cross-platform oversight and shared intelligence, the system will keep being gamed.

This is not only about protecting gaming companies. It is about safeguarding the players, the platforms, and the integrity of the digital economy itself.

About the text

Written for a compliance and screening firm and published under their name. The closing product paragraph in the original has been left off here, since the sample is the argument and not the pitch.

Konstantinos Chatzimichail

Marketing design, creative production, content and growth strategy.

Based in Greece, working internationally.

Talk to me about a paper like this one: +30 694 645 0024.