Gaming the system: closing anti-money laundering gaps in the digital entertainment economy

by Adam Rousselle and Galen Lamphere-Englund

Gaming platforms now operate as parallel financial systems. What began as microtransactions and virtual rewards has grown into a multibillion-dollar marketplace where users buy, sell, and trade assets with real monetary value. These flows create exchangeable currencies, digital wallets, and peer-to-peer markets that criminals can exploit to move money across borders with limited oversight.[1]

This process creates a laundering loop that hides the origin of funds while blending them into massive, legitimate transaction volumes

Money launderers, organized criminals, terrorists, and violent extremist organizations (VEOs) increasingly test these tools. They convert in-game tokens into fiat or cryptocurrency, route funds through streaming donations, and exploit loopholes in marketplace policies. Regulators, however, remain slow to respond. The Financial Action Task Force (FATF) first warned about these risks in 2018, but most gaming platforms still operate without meaningful anti-money laundering (AML) obligations.[2]

Emerging typologies in gaming and streaming

Criminals exploit gaming ecosystems because they offer liquidity, scale, and weak oversight. Several typologies already show how illicit finance flows through these platforms.

In-game currency laundering. Platforms like Roblox and Fortnite generate nearly $10 billion in annual revenue through virtual currencies such as Robux[3] and V-Bucks.[4] Criminals can buy tokens with illicit funds, trade them inside the game, and then cash out through developers or secondary markets.[5] This process creates a laundering loop that hides the origin of funds while blending them into massive, legitimate transaction volumes.

Loot box and in-game item exploitation. Loot boxes — randomized purchased rewards often delivered as in-game items — let users assign monetary value to digital assets that regulators cannot easily trace. Launderers purchase loot boxes with illicit funds, resell high-value items on external marketplaces, and convert the proceeds back into fiat or cryptocurrency.[6] The opacity of these probability-based rewards makes it difficult for authorities to track flows.[7]

Third-party currency conversion. A growing industry of external exchanges converts both "non-convertible" and "convertible" in-game currencies into cash or crypto.[8] These services bypass platform-level controls — operating in regulatory gray zones — enabling criminals to arbitrage value cross-jurisdictionally.[9]

Blockchain-enabled livestreaming. Streaming platforms like DLive integrate crypto payment rails directly into content ecosystems. Even after crackdowns on mainstream ser-

1 "Money in Video Games: It's Virtually Everywhere!", *Northbrook Bank*, 2023.
2 *FATF*, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", 2019.
3 Moshe Klein, "Video Games Might Matter for Terrorist Financing", *Lawfare Media,* May 2024.
4 Greg Belding, "In-game Currency & Money Laundering Schemes: Fortnite, World of Warcraft & More", *Infosec*, June 2021.
5 Skye Jacobs, "Microtransactions Accounted for 58% of PC Gaming Revenue Last Year", *TechSpot,* April 2025.
6 Mavis Bennett, "The Potential Perils of Online Gaming", *Acams Today,* June 2023.
7 Leon Y. Xiao, "Regulating Loot Boxes as Gambling? Towards a Combined Legal and Self-Regulatory Consumer Protection Approach", *Interactive Entertainment Law Review*, June 2021.
8 *Consumer Financial Protection Bureau*, "Banking in Video Games and Virtual Worlds", April 2024.
9 Shane Kelly, "Money Laundering through Virtual Worlds of Video Games: Recommendations for a New Approach to AMLRegulation", *Syracuse University College of Law*, 2022.

vices, these ecosystems allow users to solicit donations and monetize propaganda with little oversight, giving banned actors a resilient financial lifeline.[10]

Violent extremist experimentation. Some VEOs have begun experimenting with non-fungible tokens (NFTs), currency, and crypto collectibles hosted on blockchain platforms.[11] While not yet actualized, these efforts suggest growing adaptation to new financetech mediums. Given that VEOs tend to probe early and scale later, this experimentation could represent an emerging threat vector.

Collectively, these typologies show why gaming economies matter in the global finance landscape. They blend entertainment, finance, and social media in ways that regulators still treat as peripheral.

In practice, they function as global value-transfer systems with billions in legitimate flows, the kind of environment illicit actors seek to exploit.
By understanding these typologies, we can better understand global regulatory gaps and how to address them.

10 Ariel Bogle, "Buying and Selling Extremism: New Funding Opportunities in the Right-Wing Extremist Online Ecosystem", *ASPI*, 2021; Ben Makuch, "Trump's Promise to Loosen Crypto Regulations May Be Boon for Extremist Groups", *The Guardian*, November 2024.

11 Mahmoud Firas, "The Gamification of Jihad: Playing with Religion", *Danish Institute for International Studies*, 2022; Julia Handle and Louis Jarvers, "Extremist NFTs Across Blockchains", *Lawfare Media*, May 2023.

Regulatory landscape and gaps

Governments have begun sketching frameworks for digital finance, but gaming and streaming ecosystems remain largely unaddressed. The Algeria Principles, adopted by the UN Security Council in 2025, call for better understanding of terrorist financing risks in emerging technologies and for proportionate regulation.[12] In 2018, FATF added Recommendation 15, urging states to regulate virtual assets and services tied to new technologies.[13] Yet neither framework translates directly into gaming.

The picture remains uneven across jurisdictions. The European Union's Digital Services Act and Terrorist Content Online rules impose broad content obligations but leave gaming platforms in a gray zone.[14] The United Kingdom and Australia emphasize online safety and child protection via Ofcom and the E-Safety Commissioner, not anti-money laundering per se.[15] In the United States, proposals like the Children's Online Privacy Protection Act (COPPA) 2.0 point to greater accountability, but stop short of imposing AML standards on gaming-related flows.[16] Each region touches a piece of the problem, yet none imposes consistent financial scrutiny.

> **Gaming companies that handle billions in microtransactions have no universal AML obligations, even though their systems function like financial intermediaries**

These gaps converge into structural blind spots. Gaming companies that handle billions in microtransactions have no universal AML obligations, even though their systems function like financial intermediaries. Jurisdictional arbitrage lets bad actors exploit inconsistencies, moving value through platforms headquartered in permissive environments. Crowdfunding and tipping systems, particularly on livestreaming services, further widen the gap: users can convert attention directly into money with little oversight or traceability.

The result is a patchwork of digital safety laws that largely ignore the financial threats posed by in-game economies. This mismatch leaves governments chasing symptoms rather than building coherent oversight.

Ireland's strategic role

Ireland occupies a unique position in this landscape. As the European headquarters for Apple, Google, and many leading game publishers, Ireland processes much of the global revenue from in-game purchases and digital wallet flows. That puts Dublin at the nexus of streaming, gaming, and fintech flows — making its regulatory posture internationally critical to how platforms manage AML, wallet conversions, and microtransaction rails.

In recent years, the Central Bank of Ireland has expanded its supervision of Virtual Asset Service Providers (VASPs) and pushed for stronger anti-money laundering measures across fintech ecosystems.[17] These frameworks extend pressure onto companies routing

12 UN Security Council – Counter Terrorism Committee, "Algeria Guiding Principles".

13 FATF, "Public Statement on Virtual Assets and Related Providers", 2019.

14 European Commission, "Terrorist Content Online".

15 Jonathan Frost, "Fraud and the UK's Online Safety Act", *BioCatch; E-Safety Commissioner*, "Online Safety Act".

16 "COPPA 2.0 Reintroduced – What You Need to Know", *BBB National Programs*, May 2025.

17 Central Bank of Ireland, "Central Bank Highlights Weaknesses in Virtual Asset Service Providers' AML/CFT Frameworks", July 2022; Jennifer Flannery, "Unveiling the Financial Crime/Anti-Money Laundering (AML) Dynamics of Ireland's Payments Sector", *Grand Thornton*, May 2024.

gaming transactions through Irish subsidiaries. That leverage matters. Because item and loot box sales, microtransactions, and streaming monetization often pass through Irish-registered entities, decisions made in Dublin ripple globally. By tightening AML standards, Ireland can set de facto norms for the industry and force multinational firms to apply compliance standards worldwide. Although not the largest regulator, Ireland's jurisdictional rules can reshape how digital economies handle illicit finance far beyond its borders.

Conclusion: convergence risks

Gaming and streaming ecosystems are no longer fringe — they are now embedded in the wider architecture of global financial flows. With billions moving through microtransactions, gift economies, and crypto-linked rails, these platforms represent a growing vector for illicit liquidity. Absent harmonized oversight, jurisdictional gaps will continue to be exploited at scale, enabling threat actors to launder value as easily as they share content, making systemic exploitation inevitable. Ireland's expanding VASP supervision highlights the role that forward-leaning jurisdictions can play, but systemic resilience will require coordinated action from regulators, platforms, and financial authorities working in tandem.

ABOUT THE AUTHORS

Adam Rousselle is an analyst and advisor specialising in threat finance. His work has been cited by the Financial Action Task Force (FATF), the United Nations (UN), and multiple government reports. He is the founder of Between the Lines Research and advises on illicit-finance issues internationally.

Galen Lamphere-Englund is an international security advisor specialising in counter-terrorism and technology-driven online harms. He has delivered research and advisory work for UN agencies, governments, NGOs, and major tech firms. He co-founded the Extremism and Gaming Research Network and serves as team lead at the Christchurch Call Foundation.

Criminals exploit gaming ecosystems because they offer liquidity, scale, and weak oversight