Combating Money Laundering in Online Gaming Ecosystem

October 2024

Table of Contents

FOREWORD

India's growing digital economy presents both opportunities and challenges in equal measure. While the sector is a driver of innovation, employment, and economic growth, it also introduces new risks, particularly in the realm of national security and the integrity of digital platforms. Among these challenges is the rising concern over money laundering activities within the online gaming ecosystem, which threatens to undermine trust and accountability in this fast-growing sector.

This report is both timely and necessary and provides a comprehensive analysis of the potential mechanisms of money laundering within the online gaming ecosystem, highlights critical vulnerabilities, and offers clear recommendations to safeguard our digital economy. The recommendations outlined will not only help protect the sector but also strengthen national security by ensuring that digital platforms cannot be exploited for nefarious activities.

As we advance towards a more digitally empowered India, safeguarding the nation's cyberspace must be a top priority. I commend the Digital India Foundation's team under the prolific leadership of Dr. Arvind Gupta for their collaborative efforts with key stakeholders to foster a secure, transparent, and accountable online gaming environment. This report will undoubtedly serve as an essential resource for policymakers, regulators, and industry leaders as they work collaboratively to protect India's digital future.

Lt General (Dr) Rajesh Pant
Former National Cyber Security Coordinator
PMO, Government of India

EXECUTIVE SUMMARY

India's online gaming industry is emerging as the dynamic sunrise industry, positioning itself as a key player in the global market. With a CAGR of 28% from FY20 to FY23, the sector's revenue is projected to reach USD 7.5 billion within the next five years. India's thriving gaming community of 568 million gamers is driving this immense growth while also creating employment opportunities in ancillary sectors like fintech, cloud services, and cyber-security.

To support the sustainable growth of India's online gaming industry, we conducted extensive multi-stakeholder consultations. These discussions revealed several challenges that could impede progress, particularly in the areas of financial integrity, cybersecurity, and user protection. Our report focuses on the critical issue of money laundering within the online gaming ecosystem, emphasizing how in-game currencies, cryptocurrencies, and offshore betting platforms are increasingly being used for illicit activities. Despite ongoing regulatory efforts to curb illegal operators, many platforms bypass restrictions through mirror sites and VPNs, underscoring the urgent need for stronger oversight and enforcement. Money laundering stands out as a key threat to the industry's integrity and long-term success.

Based on our findings and stakeholder consultations, we recommend the following:

- Establish a 'Whitelist' of compliant gaming companies, ensuring payment gateways and ISPs serve only listed operators.
- The law should incorporate principles of financial integrity:
    a. Operators must perform a business risk assessment and develop robust internal policies to mitigate associated financial risks.
    b. Online gaming operators should verify the identity of every user before accepting deposits, and strict policies should be in place to prevent duplicate accounts.
    c. Deposits should only be allowed via verified financial entities, excluding cash or unverified methods.
- An in-depth vulnerability assessment of in-game assets and currencies by the appropriate regulatory authority is necessary.
- Financial institutions, especially banks should enhance AML systems to prevent the use of mule accounts, a prevalent technique for laundering money through gaming platforms.
- International cooperation must be prioritized, with India playing a lead role in cross-border efforts to combat illegal online gambling and associated money laundering activities.

We hope this report not only contributes to the existing body of literature but also inspires meaningful policy changes and informed decision-making to address the challenges outlined in the report.

LIST OF ABBREVIATIONS

4AMLD	Fourth Anti-Money Laundering Directive
5AMLD	Fifth Anti-Money Laundering Directive
AML	Anti-Money Laundering
API	Application Programming Interface
AVGC	Animation, Visual Effects, Gaming, and Comics
BSA	Bank Secrecy Act
CAGR	Compound Annual Growth Rate
CFT	Combating the Financing of Terrorism
CDD	Customer Due Diligence
CVC	Convertible Virtual Currency
ED	Enforcement Directorate
EUR	Euro
FATF	Financial Action Task Force
FDI	Foreign Direct Investment
FIU	Financial Intelligence Unit
FY	Fiscal Year
GDP	Gross Domestic Product
GST	Goods and Services Tax
HM	Home Minister
IFSC	Indian Financial System Code
IB	Intelligence Bureau
INR	Indian Rupee
KYC	Know Your Customer
LCCP	Licence Conditions and Codes of Practice
MMORPG	Massively Multiplayer Online Role-Playing Games
MOBAs	Multiplayer Online Battle Arenas
MeitY	Ministry of Electronics and Information Technology

PMLA	Prevention of Money Laundering Act, 2002
POCA	Proceeds of Crime Act 2002
R&AW	Research and Analysis Wing
RBI	Reserve Bank of India
RMG	Real Money Games
SAL	Strategic Analysis Lab
SARs	Suspicious Activity Reports
SRBs	Self-Regulatory Bodies
SNRA	Supra-National Risk Assessment
TDS	Tax Deducted at Source
TACT	Terrorism Act 2000
UAE	United Arab Emirates
UK	United Kingdom
US	United States
UNODC	United Nations Office on Drugs and Crime
VASP	Virtual Asset Service Providers
VDA	Virtual Digital Asset
VPN	Virtual Private Network
OTTs	Over-The-Top Services

RESEARCH METHODOLOGY AND LIST OF CONTRIBUTORS

To ensure this report is both informative and insightful, our process began with an extensive review of the relevant literature to establish a solid foundation. This was followed by crafting targeted questions for discussions with the experts, which helped shape the first draft. The draft then underwent a series of review cycles, during which stakeholder feedback was carefully considered and integrated, ultimately leading to the final version of this report.

We would like to thank everyone who has contributed to this report. We are especially grateful to the following people for their expertise and valuable time, which played a crucial role in the formulation of this report. The names of the contributors have been masked, as the consultations were conducted under the Chatham House rules.

- Former Secretary, Ministry of Electronics and Information Technology, Government of India.
- Former Scientist, Ministry of Electronics and Information Technology, Government of India.
- Professor and Dean, Kautilya School of Public Policy
- Associate Professor, Indian School of Business
- Assistant Professor, Kautilya School of Public Policy
- Partner & Gaming Expert, Cyril Amarchand Mangaldas
- Public Policy Expert, Cyril Amarchand Mangaldas
- White Collar/Investigations Expert, Cyril Amarchand Mangaldas
- Founder & Head AI Research - Pradhi AI
- Senior representative (Cyber and Security Professional), Deepstrat

INTRODUCTION

In the evolving Media & Entertainment ('**M&E**') sector, traditional media like television, print, filmed entertainment, out-of-home media, music and radio saw their revenue share drop from 76% in 2019 to 57% in 2023. On the other hand, digital media, including OTTs, social media and online gaming, experienced significant growth. Online gaming, in particular, grew rapidly at a CAGR of 28% from FY20 to FY23. In 2023, revenue from the online gaming sector surged to USD 3.1 billion and is expected to grow to USD 7.5 billion in the next five years. It is anticipated that digital media including OTTs, social media, and online gaming will become key contributors to the M&E sector's growth, potentially accounting for over 50% of the M&E sector in the near future.[1]

The significant increase in digital entertainment consumption can be attributed to the widespread availability of fast and affordable internet, increasing incomes, and surge in consumer durable purchases, all of which have significantly bolstered the entertainment sector. As per World Economic Forum, India is evolving into one of the world's most dynamic consumption environments. By 2030, India is set to become the 'largest young consumer' market in the world, elevating consumption levels to new heights. Households moving to higher income brackets are likely to spend three to four times more on entertainment services, particularly favouring digital forms. India now hosts an enormous gaming community with 568 million gamers and over 9.5 billion gaming app downloads in 2023 alone, amounting to 15% of the world's total mobile game downloads.[2] With the forecasts and trends pointing towards a growing demand for experiential entertainment, online gaming is set to become the third largest segment of the Indian M&E sector.[3]

This notable growth in the online gaming sector, together with other subsets of the M&E such as OTT platforms and digital platforms such as social media, has also brought forth various challenges. Issues such as user harm, cybersecurity threats, and privacy breaches are common to all. Particularly in online gaming, there is an additional layer of concern regarding financial frauds.

In July 2023, the Parliamentary Standing Committee on Finance presented a report identifying four major trends in cybercrime.[4] One of these trends highlighted the use of international online betting sites for money laundering. The Financial Intelligence Unit ('**FIU**') flagged several concerning trends related to suspected money laundering. A

[1] *"Windows of opportunity: India's media & entertainment sector - maximizing across segments,"* FICCI and EY, April 2023, https://assets.ey.com/content/dam/ey-sites/ey-com/en_in/topics/media-and-entertainment/2023/05/ey-me-report-executive-summary.pdf.

[2] *"Gaming Blueprint,"* Blume Ventures, June 21, 2024, https://blume.vc/reports/gaming-bluprint.

[3] *"Windows of opportunity: India's media & entertainment sector - maximizing across segments,"* FICCI and EY, April 2023, https://assets.ey.com/content/dam/ey-sites/ey-com/en_in/topics/media-and-entertainment/2023/05/ey-me-report-executive-summary.pdf.

[4] *"Cyber Security and Rising Incidence of Cyber/White Collar Crimes,"* Fifty Ninth Report, Standing Committee on Finance (2022-2023), July 27, 2023, https://sansad.in/getFile/lsscommittee/Finance/17_Finance_59.pdf?source=loksabhadocs.

significant issue was the discovery of suspicious transactions linked to offshore illegal betting and gambling companies, primarily registered in countries like Curacao, Malta, and Cyprus.

While there are no official statistics available on the extent of money laundering via illegal online gaming/gambling operators, in May 2023, India's Enforcement Directorate ('**ED**') tracked and conducted a nationwide crackdown on foreign-registered online gaming companies suspected of laundering INR 40 billion (USD 480 million). According to an independent study, the illegal betting market in India receives upwards of USD 100 billion per annum in deposits.[5] This market grew at 7% CAGR from 2012 to 2018[6] and is expected to grow at an annual rate of 30% in the coming years.[7]

In light of these incidents, including the widely publicised Mahadev Betting App scam, news surfaced in December last year that an informal Group of Ministers had been constituted. This group consisted of the Minister of Electronics & Information Technology; Minister of Sports, Youth Affairs, and Information & Broadcasting; the Minister of Finance, and the Minister of Home Affairs. Reports indicated that the initial focus of their agenda was strategies to combat money laundering within the online gaming ecosystem.

While the meeting may not have taken place as planned, the issue remains pertinent. It appears that the government is exploring options for integrating the online gaming sector into a robust AML/KYC regime. Discussions have even extended to the international level, focusing on the need for global cooperation in establishing AML/KYC standards, reporting requirements, and the exchange of information across jurisdictions.

Prima facie, in its efforts to curb these illegal activities, there appears to be a conflation between legitimate online skill gaming operators and illegal betting and gambling platforms. The lack of a fully operational regulatory framework exacerbates the issue, as there are currently no statutory requirements for the legitimate online gaming industry to implement customer identification, due diligence, or transaction monitoring and reporting measures.

In this context, the question arises: *What are the mechanisms of money laundering in the online gaming sector, who are the risky actors, and what are the risk factors that need to be considered? How should the ecosystem respond to and mitigate these risks, and what is the role of the government in addressing them?*

To this end, the present report maps the mechanisms of money laundering in the online gaming ecosystem, provides a risk assessment, and recommends mitigation strategies.

---

[5] *"State of Betting & Gambling in India,"* Think Change Forum, 2024.
[6] *Id.*
[7] *Id.*

The report is structured into two *parts*:

> ***Part I*** identifies various money laundering mechanisms (*modi operandi*) that pose risks at the national level, considering multiple risk factors such as users, product offerings, services, payment transactions, and delivery channels. This section also examines the international framework for money laundering in online gaming and concludes with key recommendations.
>
> ***Part II*** focuses on assessing the specific vulnerabilities within the Real Money Gaming sector. This section evaluates the effectiveness of existing safeguards, identifies gaps, and describes the prevailing risks. Similar to *Part I*, *Part II* concludes with key observations and provides targeted recommendations to address money laundering risks within the RMG sector.

For the purposes of this report, the connotation 'Online Game' refers to Real Money Games of Skill ('**RMG**'), Casual and Hyper Casual Games, and Midcore and Hardcore Games (for definitions, *see ahead*). It is worth noting that the estimated user base for RMG is around 100 million, while more than 500 million of online users are primarily engaged in Casual Games, illustrating the varied landscape of online gaming.

The reference to illegal gambling and betting includes both offshore and domestic gambling and betting operators. However, in states where gambling and betting are allowed and regulated, entities that are registered and in compliance with applicable state laws will be considered legal. All other operators, including domestic and offshore operators not in compliance, will be considered illegal.

MAPPING OF THE ONLINE GAMING SECTOR

The online gaming industry in India has witnessed remarkable growth in recent years, showcasing immense economic potential. With a sizable gaming community of 442 million online gamers,[8] India ranks as the world's second-largest market after China. The sector attracts substantial foreign direct investment ('**FDI**'), generates employment opportunities and boosts investments across various sectors. Additionally, it serves as a catalyst for ancillary industries such as fintech, cloud services, data analytics, and cybersecurity.

Between FY20 and FY23, the Indian online gaming segment demonstrated a notable CAGR of 28%, reaching a market size of INR 16,428 crore in FY23. Projections indicate further growth, with the market expected to reach INR 33,243 crore by FY28, showcasing a 15% CAGR.[9] Significant investments, totaling INR 22,931 crore between FY20 and FY24 YTD,[10] have been poured into this segment from both domestic and foreign sources.

The online gaming sector accounted for 3.4% of the M&E industry in 2019, a figure anticipated to rise to 12.6% by 2026.[11] Within the AVGC sector, online gaming's share is projected to increase from 41% in 2019 to 68% by 2026.[12] Additionally, the contribution of online gaming to GDP experienced a CAGR of 27.5% from 2019 to 2022.[13] The sector directly and indirectly employs approximately one lakh individuals, with the potential to create 250,000 job opportunities by 2025.[14]

The Indian online gaming market encompasses RMG, Casual and Hyper Casual Games, Midcore and Hardcore Games, and E-sports.

REAL MONEY GAMES

RMGs refers to an online skill game where a user makes a deposit, either in cash or kind, with the expectation of earning winnings on that deposit. The sector encompasses a variety of games, including fantasy sports and card-based games such as rummy and poker. These games are available on either Single-Game Platforms, which offer a single game, or Multi-Game Platforms which provide multiple games on one platform. The primary revenue streams for RMG is platform fees, and other sources such as in-app purchases, virtual tipping, and merchandising contribute minimally.

8 *"Guardians of safe play: Ethical gaming for Vibrant Bharat,"* Grant Thornton and E-Gaming Federation, July 2024, https://www.grantthornton.in/globalassets/1.-member-firms/india/assets/pdfs/ethical_gaming.pdf.

9 *"New Frontiers: Navigating the evolving landscape for online gaming in India,"* EY, December 2023, https://assets.ey.com/content/dam/ey-sites/ey-com/en_in/news/2023/12/ey-new-frontier-online-gaming-report.pdf.

10 *Id.*

11 *"India's Booming Online Gaming Industry - A Potential Powerhouse,"* EGROW Foundation, July 2024, https://egrowfoundation.org/research/indias-booming-online-gaming-industry-a-potential-powerhouse/.

12 *Id.*

13 *Id.*

14 *"Indian gaming likely to hit $7.5 billion, create 250,000 jobs by 2025: Meta India head,"* The Economic Times, March 14, 2024, *https://economictimes.indiatimes.com/tech/startups/indian-gaming-likely-to-hit-7-5-billion-create-250000-jobs-by-2025-meta-executive/articleshow/108500177.cms?from=mdr*.

The RMG sector is a significant part of the online gaming ecosystem, contributing 83-84% of its revenue.[15] With around 100 million daily online gamers, including 90 million who pay to play,[16] the sector is supported by over 400 homegrown startups.[17] This vibrant ecosystem not only engages millions of users but also serves as a key driver of tax revenues for the government.

Effective October 1, 2023, the GST regime for the RMG sector underwent a significant shift. The earlier 18% tax on platform fees, which generated an annual contribution of INR 1,700 crore, was replaced by a 28% tax on deposits. As per the recent GST Council meeting, the sector contributed approximately INR 7,000 crore in the initial 6 months. Over the period from FY 2024 to FY 2028, the total GST contribution is estimated to range between INR 80,000 crore and INR 85,000 crore.

On the direct tax front, new clauses introduced from April 1, 2023, eliminated the minimum threshold of INR 10,000 for TDS, requiring platforms to deduct tax at rate of 30% on net winnings. This updated framework is expected to generate TDS contributions of INR 6,500 crore to INR 6,800 crore between FY 2024 and FY 2028.[18]

Casual, Midcore and Hardcore

Casual and Hyper Casual Games are easy to play, typically free-to-play and feature minimalist user interface (e.g., Candy Crush, Temple Run, etc.).

Midcore and Hardcore Games offer challenging gameplay with detailed graphics, intricate storylines, and competitive elements. While Hyper Casual and Casual Games often focus on individual play, Midcore and Hardcore offer multiplayer modes. Examples include Clash of Clans and PUB G. Hardcore Games consists of categories such as Massively Multiplayer Online Role Playing Games (‘**MMORPG**’), Multiplayer Online Battle Arenas (‘**MOBAs**’) and first-person shooters.

Hyper Casual Games generate revenue through in-app advertising, while all other categories primarily generate revenue through pay-to-play or in-app purchases for additional skills, gameplay sessions, hints, and ad removal.

---

[15] *“Guardians of safe play: Ethical gaming for Vibrant Bharat,”* Grant Thornton and E-Gaming Federation, July 2024, https://www.grantthornton.in/globalassets/1.-member-firms/india/assets/pdfs/ethical_gaming.pdf.
[16] *Id.*
[17] *“Top investors ask PM Modi to review online gaming tax,”* LiveMint, July 22, 2023, https://www.livemint.com/companies/news/top-investors-ask-pm-modi-to-review-online-gaming-tax-11689965504691.html.
[18] Industry estimates; *“New Frontiers: Navigating the evolving landscape for online gaming in India,”* EY, December 2023, https://assets.ey.com/content/dam/ey-sites/ey-com/en_in/news/2023/12/ey-new-frontier-online-gaming-report.pdf

WHAT IS MONEY LAUNDERING?

'Money laundering' is the act by which the proceeds of crime are made to appear legitimate. The UN Convention Against Transnational Organized Crime criminalizes the laundering of proceeds of crime under *Article 6(1)(a)*[19].

The act of conversion and concealment constitutes the 'laundering' of criminal proceeds. However, these proceeds only possess the 'appearance' of legitimacy, not the reality, even though the money trail may be complex and obscure the original criminal source. This is typically associated with organised crime activities that generate massive cash profits, such as drug trafficking, arms trafficking, human trafficking, and fraud.

While it is not possible to measure money laundering as one would legitimate economic activity, the scale of the problem is enormous. The United Nations Office on Drugs and Crime ('**UNODC**') estimates that between EUR 715 billion and 1.87 trillion is laundered each year, amounting to between 2% and 5% of global GDP.

[19] *Article 6(1)(a)*, UN Convention Against Transnational Organized Crime and the Protocols thereto: https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf.

'Money laundering' is defined as: (i) The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action; (ii) the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime.

GROWING EVIDENCE OF MONEY LAUNDERING IN INDIA

In July 2023, the Parliamentary Standing Committee on Finance presented a report identifying four major trends in cybercrime.[20] Notably, one of these trends includes the use of international online betting sites for purposes such as money laundering.

On the question of trends in cybercrime, the Department of Revenue stated that:

> *"There are four major trends that we have seen. The first one is the use of crypto for money laundering and terror financing. The second is the use of mule accounts with false addresses. That is the second typology. The third typology is the use of international online betting sites both for the purpose of money laundering and terror financing. The fourth trend we have seen is the lending apps and apps for investments which have been used and which have been caught in the system. So, these four typologies have been primarily reported. As regards the mule account, it is mostly in India. But in the three other instances, the offshore entities are involved. It may be crypto. It may be the online betting sites. There is a clear set of online betting sites which are based out of tax havens."*

As per FIU's Annual Report 2022-23, the Strategic Analysis Lab ('**SAL**') produced a typology report on *Risk Analysis of Online Gaming and Gambling in India*.[21] The report, which is not in public domain, is understood to have highlighted the ML risks associated with the use of convertible and non-convertible currencies in gaming and gambling platforms. Additionally, it examined the relevant laws and regulations, the Know Your Customer ('**KYC**') processes followed by these platforms, and assessed the vulnerabilities and risks. The report also identified various ML techniques and typologies prevalent in these industries.

The observations in the Parliamentary Standing Committee report appears to be based on SAL-generated reports covering *Risk Analysis of Online Gaming and Gambling in India, Virtual Digital Assets, and Cybercrime Type and Data Analysis.*

Recognizing the seriousness of the issue, the Ministry of Electronics and Information Technology ('**MeitY'**) has so far blocked a total of 174 applications related to betting and gambling under *Section 69A* of the Information Technology Act, 2000 (**'IT Act**'). However, these bans have largely proven ineffective in curbing illegal activities.

While there are no official statistics available on the extent of money laundering via online gaming/gambling in India, in May 2023, the ED tracked and conducted a nationwide crackdown on foreign-registered online gaming companies suspected of laundering INR 40 billion (USD 480 million). These companies were registered in tax havens like Curaçao, Malta, and Cyprus, and were linked to Indian bank accounts opened in the names of proxy

---

[20] *"Cyber Security and Rising Incidence of Cyber/White Collar Crimes,"* Fifty Ninth Report, Standing Committee on Finance (2022-2023), July 27, 2023, https://sansad.in/getFile/lsscommittee/Finance/17_Finance_59.pdf?source=loksabhadocs.

[21] "*FIU-India Annual Report FY 2022-23,"* FIU-India, 2023, *https://fiuindia.gov.in/pdfs/downloads/AnnualReport2022_23.pdf.*

persons with no links to online gaming activity. They were only tracked because they violated the provisions of the Foreign Exchange Management Act, 1999 (‘**FEMA**’), which would not have been the case had the laundering occurred via virtual currencies.

The Curious Case of Mahadev Betting App

Mahadev, an online betting operator, allowed users to illegally gamble across a spectrum of games. The app was operationalised via a vast network, involving franchising “Panel/Branches” to known associates on a 70-30 profit basis. Agents were used to deceptively entice and enrol new customers onto the app, and money generated was laundered through a complex web of benami bank accounts. Entire illicit operation brought in roughly INR 200 crores daily. The ED has frozen assets amounting to INR 417 crore in this case, but it suspects the total value could exceed INR 5,000 crore.

Pari-Match Scam

Parimatch, a Cyprus-based online gaming platform, allegedly syphoned off around INR 700 crores from Indian users through a network of 400 entities. The app displayed live scores of European football matches and facilitated betting, enticing locals with promises of wealth. Some of these applications are also linked to China, further raising national security concerns.

Caught in Illegal Betting

An Ahmedabad-based fintech company was accused of using 150 bank accounts to launder INR 170.70 crore generated from illegal betting. The accused were alleged to have transacted these funds through a bank account opened without the consent of the actual account holder, using account holder’s PAN and Aadhaar details. The money is suspected to have been generated through the online betting site www.wolf777.com. The customers had to deposit money into the accused’s accounts to purchase credits or coins through online transactions. Once the funds were deposited, users could log in and place bets on the website.

Recently, the Financial Action Task Force (‘**FATF**’) released its Mutual Evaluation Report (‘**MER**’) for India. The report highlights that, despite the size of its economy and population, India is generally not considered a prime destination for criminal proceeds. However, cross-border risks for money laundering and terrorist financing remain, with funds flowing in and out of the country.

According to the MER, the primary sources of money laundering in India stem from illegal domestic activities, with the largest money laundering risks relating to cyber-enabled fraud, corruption, and drug trafficking. These illicit proceeds may either be laundered within India, sent abroad for laundering, or reintroduced into India’s legitimate economy after being laundered overseas.

The report reiterates the legal distinction in India between games of skill and games of chance, noting that under the PMLA, only activities involving games of chance for cash or kind, such as those related to casinos, are designated as AML/CFT reporting entities.

In assessing various sectors of the Indian economy, the MER assigns importance based on their materiality and associated ML/TF risks. This ranking system informs the report's conclusions, with higher emphasis placed on sectors posing significant risks, while sectors with lower risks are weighted less heavily.

Casinos, while covered under FATF Recommendations, are considered a lower-risk sector in India due to limited evidence of their misuse for laundering criminal proceeds. However, the report acknowledges the rapid growth of the internet-based gaming sector and notes several instances where online gambling and betting platforms have been exploited for money laundering purposes.

PART I:

MONEY LAUNDERING MECHANISM IN ONLINE GAMING THAT CONSTITUTE RISKS AT INDIA LEVEL AND DISCUSSION ON INTERNATIONAL FRAMEWORK

IDENTIFICATION OF MECHANISMS IN ONLINE GAMING THAT CONSTITUTES RISKS AT INDIA LEVEL

Traditionally, money laundering involves a three-step process:[22]

Placement: The initial stage involves injecting illicit funds into the financial system. This is often done by using such illicit funds to purchase in-game currency/items or to play a game. Alternatively, they may create user accounts using stolen credit cards or hacked credentials to make these transactions.

Layering: Next, complex layers are constructed to conceal the origin and ownership of the illegally-obtained funds. Once funds are placed in the online gaming ecosystem, the beneficiaries engage in countless transactions, creating a web of money transfers to and from entities registered around the world. In doing so, the launderer obscures the audit trail. For instance, in the online gaming context, this could involve trading or selling the purchased in-game items or currency, often across different games or platforms.

Integration: Finally, the laundered proceeds are reintroduced into the economy. This can be done through various means, one of which is selling the items on third-party marketplaces or using the in-game currency to purchase other items that can then be sold for real money. At this point, if the laundering was executed successfully, it is nearly impossible to identify the initial source of the value.

Each step of the process of money laundering carries its own risks and challenges. These 3-stages are commonly viewed as the basis of all modern money laundering, however methods vary and not all methods utilise all three steps.

These three key stages can be achieved through various methods—whether they operate independently or simultaneously—that pose significant money laundering risks in the online gaming sector. The following methods illustrate how these stages can manifest and the vulnerabilities they exploit:

A. Illegal Operators

The illegal betting market in India receives upwards of USD 100 billion per annum in deposits.[23] While there is scarcity of statistics on the subject, independent statistics suggest that this market grew at 7% CAGR from 2012 to 2018.[24] In addition to this, it is expected that the market will grow at an annual rate of 30% in the coming years due to regulatory uncertainty surrounding the sector.[25]

[22] S Kelly, *"Money Laundering Through Virtual Worlds of Video Games: Recommendations for a New Approach to AML Regulation,"* Syracuse Law Review, https://lawreview.syr.edu/wp-content/uploads/2022/01/1487-1512-Kelly.pdf.
[23] *"State of Betting & Gambling in India,"* Think Change Forum, 2024.
[24] *Id.*
[25] *Id.*

Most recently, the FATF's MER for India notes enumerates instances where illegal online gambling and betting platforms have played an integral role in money laundering:

Tracing Illicit Funds Through Betting Platforms

Information surfaced in Zonal Offices regarding gambling and betting sites promoted through a social media platform. To trace the money trail, the Enforcement Directorate (ED) created an online ID and deposited a small sum using the link shared on the site. Investigators engaged with users on the platform, uncovering that individuals across India were being enticed to invest in gambling activities. Funds were collected via a Payment Gateway Service and transferred to a company account.[26] Further investigation revealed this company to be a shell entity with minimal share capital and no active business operations. It was part of a larger network of 56 companies with shared directors and shareholders, all controlled by a foreign national.

A detailed analysis of transaction patterns revealed that small amounts were funneled into multiple bank accounts, which were then pooled into a select few. The use of controlled delivery and undercover operators led to operations that resulted in search and seizure of documentary evidence. The ED also secured bank documents to finalize the investigation.

Investigations have exposed the complex web of illicit funds generated through betting apps. Fictitious entities open bank accounts, which are used to route and layer illegal funds. These funds, after passing through multiple layers, are eventually transferred abroad, disguised as transactions for bogus entities posing as legitimate imports. One stark example is the Mahadev online betting app, where money from Indian users was laundered to the UAE using a complex network of benami bank accounts.[27]

The Reserve Bank of India ('**RBI**') has set regulations prohibiting the use of Indian payment instruments for transactions on foreign gambling and forex sites. However, offshore gambling websites have developed methods to circumvent these regulations, facilitating deposits and withdrawals while avoiding legal oversight.[28]

According to our analysis, while the methods may vary, the core operations of these schemes remain the same. Illegal gambling and betting platforms are widely available for download,

---

[26] A common misconception is that proceeds of crime are always in the form of physical cash or cryptocurrency. However, criminals often already possess these funds in digital form, obtained through various illicit methods. This money could originate from stolen credit cards, or deposits into bank accounts created using forged documents. Even though the funds exist digitally, they remain 'dirty' because they are tied to illegal activities. These funds must still be laundered to obscure their criminal origins and legitimise them. A classic example of this process is seen in platforms like Fiewin, which reportedly collected funds via UPI IDs. Here, the initial 'placement' of illicit money doesn't occur in the traditional sense. Instead, such betting companies gather large sums of money, aggregate them into few accounts, and use complex methods, such as converting the funds into cryptocurrency, to obscure the source and eventually integrate it into the formal economy.

For a deeper insight into how these operations are structured and how launderers work to obscure financial trails, refer to the case study on Fiewin below in this subsection.

[27] *"Gambling Away India's Sovereignty,"* Centre for Knowledge Sovereignty, May 18, 2024, https://cksindia.org/gambling-away-indias-sovereignty/.

[28] *Id.*

often accessible even after being blocked through unauthorised channels like Telegram, websites, and other unofficial platforms.

Users are attracted to these applications through advertisements featuring influencers across various online platforms. These illegal websites consistently promote their services through multiple online channels. Despite numerous warnings against direct and surrogate advertisements for gambling and betting, offshore and illegal platforms continue to aggressively target Indian consumers, particularly during high-profile events such as the IPL season and other major tournaments.

Unsuspecting users often fall prey to these schemes by making deposits. For instance, deposits can be made to a specific UPI ID, which could either belong to an accomplice (as was the case in Fiewin case, *see below*) or be linked to a mule account, such as an unsuspecting shopper or a kirana store. Additionally, local agents sell cash recharge vouchers, while proxy retailers in India disguise themselves as online grocery or clothing stores, converting order values into gambling portal account balances.

Once users are drawn into the system, illegal operators lure them to continuously add more money, ultimately halting withdrawals and transferring the funds to their own accounts. The "pig butchering" scheme involves victims being gradually enticed to increase their deposits through small initial wins. Once they attempt to withdraw larger amounts, they find themselves cut off from accessing their funds. This method allows operators to maximize their profits while leaving victims with no means to recover their money.

Money laundering within online gaming often manifests in two primary forms: either the operators of unlawful platforms directly engage in laundering activities, or users exploit these platforms to channel illicit funds. In the second case, if the operator is following loose KYC or compliance, then the likelihood becomes higher.

A notable example is the case of Fiewin, a platform deliberately structured to accumulate funds from users, which were then laundered through various financial channels before being funnelled into the digital wallets of Chinese nationals. This instance highlights the intricate schemes used to mask the origin and movement of illicit money by online operators.

Recent Case Involving Fiewin Scam

The Fiewin app facilitated money laundering in a systematic way by involving Indian nationals, Chinese nationals, and companies like Studio21.

Step 1: User Acquisition

Users are typically drawn to platforms like Fiewin through targeted advertising campaigns, often featuring influencers and circulating across various online platforms. Further, there are numerous videos on YouTube that claim to offer tips on how to earn money using Fiewin. While the official ED press release does not explicitly detail Fiewin's promotional strategies, media reports suggest that the platform was marketed as a quick and easy way to make money, leveraging channels like YouTube, Facebook, and other digital platforms.

Step 2: User Deposits

Unsuspecting users deposited funds to gamble or participate in games, and these funds were routed to Indian intermediaries known as 'recharge persons,' specifically Arun Sahu and Alok Sahu, based in Odisha. These recharge persons received commissions (3-5%) for allowing the use of their bank accounts. According to the ED, the user deposits were funnelled into the bank accounts of these recharge persons, but the precise method of how deposits reached these intermediaries remains unclear.

Some news reports suggest that UPI transactions were used; users either made UPI payments directly to these 'recharge persons' or their deposits were later transferred to the recharge persons' accounts.

Step 3: Conversion of User Funds to Crypto

Once the recharge persons – Arun and Alok, received the money from the users, the funds were converted into cryptocurrency, specifically USDT. The ED press release states that *"the funds received in their bank accounts* [Arun Sahu and Alok Sahu] *from the Fiewin app were converted into crypto currency."* The press release further states that *"Chetan Prakash, an engineer based out of Patna, Bihar played a key role in the money laundering activities by helping such 'recharge persons' in conversion of INR into crypto currency (USDT)."*

The recharge persons would wait until a certain threshold of user funds had accumulated in their accounts before converting the bank account balance into cryptocurrency. Cryptocurrency—specifically USDT—was purchased from black market sellers. The USDT sellers received payments (either in their bank accounts or through hawala) and, in exchange, credited the recharge persons' wallets, such as Binance, with the equivalent amount in cryptocurrency.

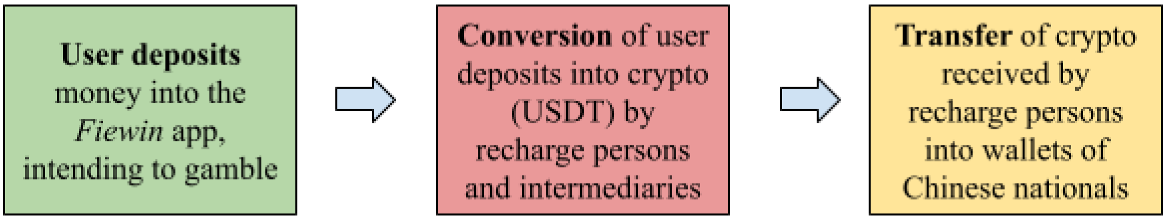
While the ED press release does not provide specifics on the cryptocurrency sellers, news reports indicate that contact information for these sellers was regularly shared in a Telegram group, presumably for the benefit of the recharge persons. Additionally, the reports suggest that USDT sellers earned a premium on these transactions compared to regular crypto trades on exchanges.

There are gaps in understanding whether Chetan Prakash received pooled cash from the recharge persons for conversion into cryptocurrency or if the transfers to him were made directly. The full extent of his involvement remains unclear, but he acted as an intermediary, further complicating the money trail.

Step 4: Transferring Crypto to the Wallets of Chinese Nationals

Eventually, the recharge persons *"deposited and laundered the crypto currency so earned from the Fiewin app to the wallets of Chinese nationals on foreign crypto exchange namely Binance,"* as per the ED press release. Thus, the crypto in recharge persons' wallets was later deposited into foreign crypto wallets (on Binance) controlled by Chinese nationals.

The involvement of crypto transactions in this stage exemplifies the *Layering* phase of money laundering, where the movement and transformation of money serve to conceal its origin. It remains unclear whether the cryptocurrency in the Chinese nationals' wallets (transferred by recharge persons) was eventually converted into fiat currency and withdrawn, or how exactly it was utilised.



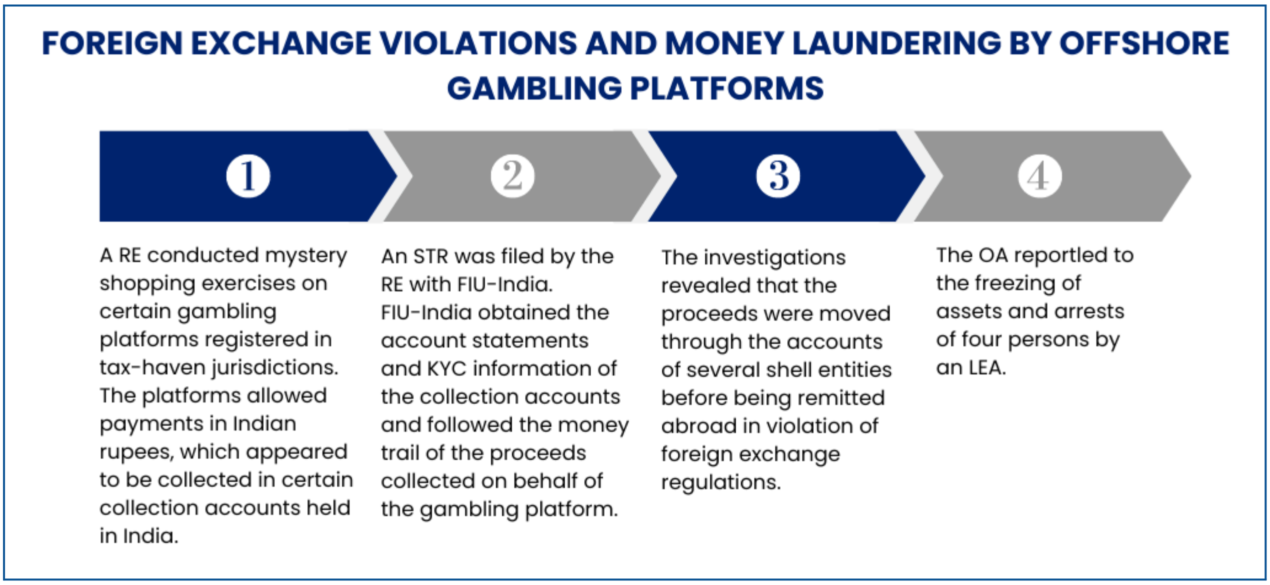
Payout Services on Fiewin

A parallel process was also in operation, involving payout services, where Joseph Stalin played a key role. As per ED's press release, *"Joseph Stalin, a software engineer based out of Chennai, helped [a] Chinese national named Pie Pengyun from Gansu province to become co-director of Studio 21 Pvt ltd, a company owned by him."*

The press release further states: *"Pie Pengyun used the account of Studio 21 pvt ltd for bulk payout services related to the app which helped them gain confidence of gamers in the beginning and provoked larger bets from the app users. The funds used for payout services were received by Joseph Stalin as crypto currency in his Binance account from the wallets controlled by the Chinese handlers. He in turn converted the USDT crypto currency into INR by selling the crypto through P2P mode on Binance."*

Studio21 Technologies Pvt. Ltd., a company registered in Thiruvallur in Chennai, played an important role in facilitating payouts to users. The bank account of Studio21, operated by Pei Pengyun, was used to facilitate bulk payouts to Fiewin users, creating an appearance of trust and encouraging users to place large bets. Joseph Stalin received cryptocurrency (USDT) in his Binance account from wallets controlled by Chinese handlers and then converted it into INR, into Studio 21's bank account.

The money was subsequently used to fund payouts to Fiewin app users, using various bulk payment platforms like Cashfree, Paytm, etc. (as per an *Economic Times* report) creating the appearance that the app was actually making payments, thereby reinforcing trust in the platform.



Source: *FIU-India Annual Report FY 2022-23*[29]

Additionally, technical analysis by the Intelligence Bureau ('**IB**') and Research and Analysis Wing ('**R&AW**') of certain betting apps uncovered alarming features in their latest upgrades.[30] These apps, operating on both Android and iOS platforms, were found to be engaging in stealing and transmitting of user data to servers located outside the country, along with monitoring of users' real-time activity. The upgraded versions of these apps required extensive user permissions to function, effectively allowing those running the apps to access the device's camera, monitor user movement, and to transfer users' backup data onto their servers. This development poses serious privacy concerns, presenting risks for personal and financial data of the users, with many believing that such tools could enable mass surveillance.

B. In-Game Currencies and Assets

Microtransactions have transformed how revenue is generated within the gaming industry. These transactions, often of nominal value, enable users to acquire virtual in-game items. Many online games, particularly those offered for free, rely heavily on this model.[31] Presently, in-app or in-game purchases constitute a significant portion of revenue for casual, mid and hardcore games. As per a recent report released by Lumikai, revenue from in-app purchases in India was USD 0.5 billion in FY23 and is expected to grow at a CAGR of 46%

[29] *"FIU-India Annual Report FY 2022-23,"* FIU-India, 2023, https://fiuindia.gov.in/pdfs/downloads/AnnualReport2022_23.pdf.

[30] *"Weapon of Mass Surveillance: How Upgraded Illegal Betting Apps are Posing Threat to National Security,"* News18, November 07, 2023: https://www.news18.com/india/weapon-of-mass-surveillance-how-upgraded-illegal-betting-apps-are-posing-threat-to-national-security-8651906.html.

[31] "*Game On! Roadmap For User Centric Gaming Regulation In India*," Koan Advisory, July 2022, https://www.koanadvisory.com/storage/2022/07/Koan-Game-On-Report_July-2022.pdf.

to reach USD 3.3 billion by FY28.[32] This rapidly growing market may pose a high risk of money laundering.

Players are incentivised to purchase in-game items due to the significant advantages they provide in gameplay. These items include virtual weapons, vehicles, mission packs, additional playtime, and aesthetic enhancements like skins. Some games use in-game currencies for these transactions, while others employ lootboxes, where the contents are revealed only after purchase.

Money laundering risks arise when players can trade in-game goods with each other or engage in secondary markets where these assets—and sometimes entire accounts—are exchanged. This issue is not new; a 2014 UNODC publication[33] highlighted how criminals have exploited MMORPGs for money laundering. They achieve this by channelling illicit funds into alternate or compromised accounts and then using them to purchase or trade in-game currency for real-world money.

Secondary Markets in Online Gaming

Secondary marketplaces are run using game assets but have no support or affiliation with the actual developer or game itself. For instance, the developer of an online game provides no support or platform for real world trading in the game, where a user can convert their in-game wealth to fiat currencies. However, there exist a number of external websites that offer the means to do this, where the value of the currency can be directly linked to in-game items and wealth essentially valuing each in-game item that can be traded player to player to a real-world price. This particular game therefore, has no primary marketplace but several secondary marketplaces.

How Money Laundering Happens in Online Gaming?

In a 2018 interview, cybercrime expert Professor Jean-Loup Richet explains how a hypothetical criminal could use World of Warcraft gold to launder stolen funds:

Let's say, for instance, that I have stolen a Paypal account and let's say that this Paypal account has about 1,000 euros," . . . . "The first step is to make things look fuzzy. A hacker will not send the stolen Paypal money directly into his personal bank account. So first, I will forward the amount of this Paypal account to two other fake Paypal accounts that I will create with remote administration tools . . . ."

"Then I will use an exchanger and will change the money to any online currency. Depending on my level of paranoia, I might exchange it into bitcoin, and then I might use another exchanger to turn it into World of Warcraft gold coins."

---

32 *"Leveling up: State of India Gaming FY'23,"* Lumikai and Google, October 2023, https://www.lumikai.com/post/indian-gaming-industry-poised-for-strong-growth-projected-to-reach-7-5-bn-by-fy28.

33 *"Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies,"* UNODC, June 2014: https://www.unodc.org/documents/middleeastandnorthafrica/money-laundering/FULL10-UNODCVirtualCurrencies-final.pdf.pdf.

Making use of popular gold selling websites or "exchangers," . . . the hacker could then buy World of Warcraft gold using their stolen money and either meet the seller in-game or receive an in-game mail with the gold included. The hacker would then turn around and sell their newly bought sum of gold—either for cryptocurrency like bitcoin or, if they choose, using another method. At this point, the origins of their money would be nearly untraceable.

Case Studies

Counter-Strike: Valve Corporation's Counter-Strike: Global Offensive ('**CS:GO**') has also been exploited for money laundering. CS:GO, which boasts over 18 million unique users per month, had an in-game economy that allowed players to earn "loot boxes". To open these boxes, players had to purchase a key from Valve using real money. However, an investigation found that most transactions involving these keys were part of a global fraud network. Criminals were using the keys as a means to launder money. Consequently, Valve halted trading of some in-game items after discovering that "nearly all" of the trading was part of a money-laundering scheme run by worldwide fraud networks.

Fortnite: Epic Games' Fortnite, one of the most popular video games in the world, has not been immune to these issues. Cybercriminals were found to be using stolen credit cards to purchase V-bucks, Fortnite's in-game currency, in large quantities. These V-bucks were then sold in bulk on the internet for a discounted price, effectively laundering the money from the stolen cards.

Epic Games took steps to combat fraud and money laundering on its platform by implementing two-factor authentication and closely monitoring transactions involving V-bucks.

Further, the integration of chance-based elements like lootboxes into skill-based online games poses challenges for regulators, blurring the lines between gaming and gambling.[34] By 2025, revenue from lootboxes is estimated to surpass USD 20 billion.[35] Lootboxes involve purchasing an in-game item without prior knowledge of its contents, which can range from cosmetic items to special abilities.

Investigations have revealed that some lootbox prizes hold market value, enticing criminals to use illegally obtained funds to acquire and trade them. In a study of 10 popular video games offering lootboxes, the Netherlands Gaming Authority discovered that 40% were in direct contravention of the applicable law, since the content of these lootboxes were determined by chance and thus, making them susceptible to external trading.[36] Investigations have revealed that criminals exploit unlawfully acquired funds to procure lootboxes and gather coveted items highly valued by players. These ill-gotten gains are then offloaded to other players via third-party platforms, exchanged for either fiat currency or convertible

[34] "*Game On! Roadmap For User Centric Gaming Regulation In India*," Koan Advisory, July 2022, https://www.koanadvisory.com/storage/2022/07/Koan-Game-On-Report_July-2022.pdf.
[35] *"The New Trends Shaping the Loot Box Landscape,"* Juniper Research, March 2021, https://www.juniperresearch.com/resources/blog/the-new-trends-shaping-the-loot-box-landscape/.
[36] *"Study into loot boxes: A treasure or a burden?,"* Netherlands Gaming Authority, April 2018, https://kansspelautoriteit.nl/publish/library/17/onderzoek_naar_loot_boxes_-_een_buit_of_een_last_-_nl.pdf.

virtual currencies. The fact that these virtual assets possess real-world financial value outside of the gaming environment facilitates the transfer of illegally obtained funds.[37]

C. Cryptocurrencies

Another trend that merits discussion is the uptick in the use of digital or virtual currencies. Numerous online gaming enterprises now accept virtual currencies like Bitcoin[38] and Ether[39] as payment options for in-game transactions. Similarly, traditional gaming platforms have adapted formats wherein players can possess virtual in-game assets. This ownership extends beyond mere gaming, allowing users to monetise these assets by trading them for virtual currency. With a vast global community of gamers spanning various countries, opportunities arise for cross-border trading of such items. Virtual currencies emerge as the preferred medium for these transactions due to their swift processing and elimination of currency conversion hassles.

Virtual currencies may be broadly categorised as: convertible (open) and non-convertible (closed).[40] Open or convertible virtual currencies, such as Bitcoin (a cryptocurrency), are employed for microtransactions in online gaming.[41] Their convertibility enables exchange for fiat currency, backed by a market demand. It is important to note that CVCs lack legal backing and derive their convertibility from the perceived value among users who engage in buying and selling. They can also be swapped for other virtual currencies on specialised exchange platforms.

From a law enforcement standpoint, convertible currencies generally fall under AML and CFT regulations due to their potential for money movement between sources.[42]

On the other hand, non-convertible currencies like in-game currency, cannot be traded for fiat currency and are confined to specific virtual environments. They are referred to as closed currencies since they remain within the bounds of their respective virtual worlds. Nonetheless, in practice, closed virtual currencies, even when only transferable within a particular virtual environment, may find their way into secondary black markets, where they are exchanged for fiat or virtual currencies (*as also explained above*)[43] In such scenarios, in

---

[37] "*Game On! Roadmap For User Centric Gaming Regulation In India*," Koan Advisory, July 2022, https://www.koanadvisory.com/storage/2022/07/Koan-Game-On-Report_July-2022.pdf.

[38] 'Bitcoin' (capitalised) refers to the open-source software and the peer-to-peer network that underpin the virtual currency. 'bitcoin' (lowercase) denotes the individual units of the virtual currency.

[39] Ether is the native token used to facilitate transactions and operations on the Ethereum network. It is the world's second-largest virtual currency by market capitalization, second only to Bitcoin.

[40] *"Virtual Currencies – Key Definitions and Potential AML/CFT Risks,"* Financial Action Task Force Report, June 2014, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

[41] *Id.*

[42] "*Game On! Roadmap For User Centric Gaming Regulation In India*," Koan Advisory, July 2022, https://www.koanadvisory.com/storage/2022/07/Koan-Game-On-Report_July-2022.pdf.

[43] *"Guidance for a Risk-based Approach - Virtual Currencies,"* Financial Action Task Force, June 2015, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-RBA-Virtual-Currencies.pdf.coredownload.inline.pdf.

practical terms, non-convertible virtual currencies can effectively transform into a convertible currency,[44] thus should be subject to AML/CFT regulations.

D. Mule Accounts

In India, digital payment volumes have grown exponentially over the past few years, reflecting a major shift from cash-based transactions to online financial activities. While this transition offers unparalleled convenience and scale, it has also led to increased financial crime, including the rise of money mules. ‘Money mules’ or ‘mules’ are people who, whether unintentionally or otherwise, help move illegal funds, making them seem lawful.

A recent report by BioCatch highlights the severity of this problem.[45] It reveals that third-party account takeover fraud now accounts for 55% of all fraud cases in the country. The same report also indicates that fraudsters may be accessing these Indian mule accounts from outside the country.

Realising the gravity of the situation, on October 17, 2023, the RBI amended the Master Direction — KYC Guidelines of 2016, underscoring its commitment to combating money laundering activities involving money mules.[46]

Criminals often recruit money mules to use their legitimate accounts for laundering illicit funds during the layering stage, which involves moving money to obscure its illegal origins. These accounts receive funds from illegal activities and then transfer them elsewhere, acting as intermediaries in the money laundering process. Mules then deposit these funds into the financial system by transferring them between accounts, eventually returning the laundered money to the criminals. This process complicates law enforcement’s efforts to trace the money trails. When such activities are detected, the ‘money mules’ often become the focus of investigations due to their direct involvement.

According to a recent KPMG report on money mules, the increase in mule operations is driven by several factors:[47] rising cyber threats, the digital banking boom, economic uncertainties, sophisticated fraud schemes, technological advancements, and a lack of awareness and education, alongside the tech-savvy nature of criminals.

---

[44] *Id.*

[45] *“2024 Digital Banking Fraud Trends in India,”* BioCatch, February 21, 2024, https://www.biocatch.com/press-release/biocatch-releases-2024-digital-banking-fraud-trends-report-in-india.

[46] Rule 59, Chapter X, *“Master Direction - Know Your Customer (KYC) Direction, 2016,”* RBI, Updated as on January 04, 2024, https://www.rbi.org.in/CommonPerson/english/scripts/notification.aspx?id=2607.

[47] *“Money Mules: FinCrime’s Trojan Horse Unveiled,”* KPMG, July 2024, https://assets.kpmg.com/content/dam/kpmg/in/pdf/2024/07/money-mules-fincrimes-trojan-horse-unveiled.pdf.

Investigation Uncovers Fraudulent Use of Mule Accounts in Online Betting Scam[48]

India Today conducted an investigation to understand the methods used by scammers in online betting platforms. The team followed a deepfake advertisement that led to the betting site Cricplus.club. Upon creating an account, they were instructed via WhatsApp to pay a mandatory INR 100 fee to a specific bank account. Notably, the payment was directed to a 'kirana'/ mom & pop store or grocery store, with an account at the Bank of Maharashtra.

Suspicious of this request, India Today team traced the account to its home branch using the Indian Financial System Code ('**IFSC**'). The branch manager, speaking anonymously, confirmed that the account belonged to a local departmental store and noted unusual transaction patterns. Although the manager declined to provide specific transaction details, they revealed that an official inquiry had been initiated after India Today contacted the Bank of Maharashtra's head office. The account was subsequently monitored, and withdrawals were frozen as a precaution.

These instances majorly involved the use of mule accounts connected to Mahadev Betting syndicate. In this particular case, the individuals were unaware that their bank accounts were being exploited for fraudulent purposes. In exchange for a small sum, these individuals agreed to let others use their accounts, not realising the underlying illegal activity. This particular case was eventually reported to the FIU for further investigation.

Uncovering a Money Mule Network in Narayangaon, Pune[49]

In Narayangaon, Pune, an intricate operation involving over 450 bank accounts was uncovered, where these accounts were used as money mule accounts for illegal betting activities linked to the Lotus 365, affiliate of Mahadev Betting Syndicate. Most of these accounts were opened in the names of individuals who were likely unaware of their existence or use.

The local crime branch discovered a BPO-like setup with 96 employees operating out of a multi-storey building in the Vision Galaxy Complex. During the investigation, police found numerous 'bank account kits'—including passbooks, debit cards, and cheque books—belonging to these third-party individuals. These kits were controlled by the BPO operators, who used the accounts to receive money from app users and transfer winnings to other accounts.

The scale of the operation was significant, with authorities seizing 45 laptops, 89 mobile phones, 101 personal phones of employees, and 452 bank passbooks from the site. The discovery highlights the widespread use of mule accounts in facilitating illegal betting transactions.

---

[48] *"Click, bet, lose: How online swindlers lure, trap and exploit people in India,"* India Today, August 10, 2024, https://www.indiatoday.in/fact-check/story/betting-apps-mahadev-deepfake-election-cricket-cybercrime-artificial-intelligence-online-fraud-2580004-2024-08-09.

[49] *"450 mule accounts used for illegal operations of Pune Mahadev betting app,"* The Indian Express, May 18, 2024, https://indianexpress.com/article/cities/pune/450-mule-accounts-used-for-illegal-operations-of-mahadev-betting-app-9336049/.

E. Smurfing

Smurfing, also referred to as structuring or the fragmentation of large sums of money into smaller, less conspicuous amounts, serves as a prevalent money laundering tactic with distinct objectives. Its primary purpose is to circumvent detection and reporting thresholds established by financial institutions and regulators. Additionally, smurfing is utilised to distort economic data and expedite tax evasion schemes.

Smurfing operations often entail the collaboration of multiple individuals, dubbed 'smurfs,' who each contribute small sums of money to various accounts, thereby evading suspicion and thwarting efforts to aggregate funds that might otherwise trigger scrutiny. The utilisation of smurfs serves to complicate the identification of suspicious transactions, as larger transactions typically garner more attention than numerous smaller deposits. In practice, however, high transaction cost deters individuals from entering into such transactions.

F. Money Dumping

Criminals may also launder illicit funds by collaborating with an accomplice during gaming activities. In this scheme, the money launderer intentionally loses to their counterpart in an online game, allowing the accomplice to claim the winnings as legitimate gaming earnings. Similar to smurfing, the likelihood of this tactic being used decreases when transaction costs, such as taxes or platform fees, are high.

INTERNATIONAL FRAMEWORK ON MONEY LAUNDERING IN ONLINE GAMING

This section lays down Anti-Money Laundering (‘**AML**’**)** requirements imposed on online gaming across various jurisdictions. The section has reference to certain gambling laws and regulations, depending on how certain games or instruments are treated within respective national legislations. This approach is intended to draw relevant insights and best practices, but it should not be construed as equating the two sectors. Gaming and gambling are treated as distinct categories under Indian law (*as detailed in the sub-section ahead*), nevertheless, gambling regulations may provide useful parallels for identifying best practices applicable to the gaming industry.

A. Financial Action Task Force (‘FATF’)

The FATF Recommendations, also known as the FATF Standards, are a comprehensive set of measures developed by the Financial Action Task Force[50] to help countries combat money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction. The FATF Recommendations explicitly cover casinos, including those operating online or aboard ships. Casinos are categorised as ‘designated non-financial businesses and professions,’ imposing distinct obligations aimed at combating money laundering and terrorist financing.

It is important to note that the Recommendations, most recently updated in November 2023, do not include recommendations for online gaming.

However, in 2019, the FATF extended its AML and CFT measures to include virtual assets and virtual asset service providers (‘**VASPs**’). Since then, jurisdictions worldwide have been expanding their regulatory frameworks to address these new domains.[51] Along with this global advancements in extending the AML/CFT net to virtual assets, there is a growing realisation of emerging risks related to in-game currencies, which mimic the functions of convertible virtual currencies (‘**CVCs**’).

B. European Union (‘EU’)

Within the EU, online gaming is regulated at the Member State-level, characterised by country-specific regulations and definitions. However, overarching EU laws, such as the Fourth Anti-Money Laundering Directive (‘**4AMLD**’) establish baseline standards that all

---

[50] The FATF spearheads global efforts to combat money laundering, terrorist financing, and proliferation financing. The FATF conducts research on methods of money laundering and terrorism funding, promotes global standards to mitigate these risks, and evaluates whether countries are taking effective measures. The FATF monitors countries to ensure they fully and effectively implement its standards. Over 200 countries and jurisdictions have committed to adopting the FATF's standards.

[51] For instance, the EU amended its 4AMLD with the 5AMLD to cover providers engaged in exchange services between virtual currencies and fiat currencies. Similarly, on March 7, 2023, the Central government of India designated entities engaging in specific virtual digital asset activities as ‘reporting entities’ under the PMLA regime.

Member States must comply with, ensuring a unified approach to combating money laundering and terrorist financing across the region.[52]

On October 27, 2022, the European Commission conducted a revision of its assessment of money laundering risks impacting the EU and published the updated Supra-National Risk Assessment (‘**SNRA**’)[53]

The SNRA sparked discussions on whether in-game currencies/tokens should fall under AML regulations. According to the report, since online gaming platforms enable the trade of *de facto* convertible in-game currency, they should be considered and thus regulated like crypto-asset service providers. It observed that when used anonymously, gaming tokens qualify as crypto-assets enabling swift transactions without disclosing the owner's identity. These tokens are accessible online, and their cross-border nature presents a significant risk, facilitating interactions with high-risk areas or unidentifiable high-risk customers. Consequently, SNRA concluded that owing to their similarity with crypto-assets, the threat assessment of gaming tokens should follow the same regime, and be regarded as high.

Concurrently, countries such as Belgium and Austria have taken a firm stance against loot boxes, categorising them as ‘games of chance’. This move underscores a proactive approach to regulating potential money laundering conduits within the gaming sector.

In addition, gambling services[54] were first brought under the purview of the EU's AML laws by the 4AMLD.[55] It was further amended by the Fifth Anti-Money Laundering Directive (‘**5AMLD**’).[56] According to these directives:[57]

> *"With the exception of casinos, and following an appropriate risk assessment, Member States may decide to exempt, in full or in part, providers of certain gambling services from national provisions transposing this Directive on the basis of the proven low risk posed by the nature and, where appropriate, the scale of operations of such services. Among the factors considered in their risk assessments, Member States shall*

---

[52] The First Anti-Money Laundering Directive (1AMLD) was introduced in 1990 to prevent the financial system from being exploited for money laundering purposes. Since then, EU regulations have been continuously updated to counter emerging money laundering and terrorist financing risks.

[53] Commission Staff Working Document, European Commission, October 27, 2022: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0344&qid=1668133326304&from=EN

[54] ‘Gambling services’ are defined under 4AMLD, as amended by 5AMLD, to mean "a service which involves wagering a stake with monetary value in games of chance, including those with an element of skill such as lotteries, casino games, poker games and betting transactions that are provided at a physical location, or by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services."

[55] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

[56] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

[57] *Article 2(2)*, Directive (EU) 2015/849: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02015L0849-20210630.

> *assess the degree of vulnerability of the applicable transactions, including with respect to the payment methods used."*

Therefore, the EU adopts a risk-based approach to mitigate money laundering risks within the gambling industry. In the risk-based approach, the risks are foreseen and hence alleviated preemptively. Such an approach prevents over-regulation and hence does not hamper technological advancement. This approach also allows EU Member States to exempt certain gambling service providers from fully complying with the AML directive, provided that these services pose a low risk of money laundering or terrorist financing. Such exemptions are granted only after a thorough risk assessment that considers the nature and scale of the operations and evaluates the degree of vulnerability of the applicable transactions, primarily the payment methods used. Consequently, games of higher chance, such as casino games, are not eligible for these exemptions.

The European Gaming and Betting Association Guidelines on Fighting Money Laundering ('**EGBA Guidelines**')[58] has noted that the risk associated with payment methods and transactions varies based on the level of anonymity and traceability they offer:

> "*Some payment methods are more vulnerable to criminal exploitation because they provide customers with the possibility to mask their identity and their source of funding, such as pre-paid vouchers for depositing on the player account. These pose a high ML/TF risk as the purchaser of the vouchers might not be legitimate and it is difficult to carry out the same level of checks as may be performed on accounts held with financial institutions. On the other hand, where a customer transfers funds from a bank account or a card linked to a bank account held in their name with an institution established in a reputable jurisdiction, the ML/TF risk is low. Particular attention needs to be paid to customers who might be funding their play through money derived from crypto assets, since these are usually subject to specific requirements due to their high-risk nature.*"

On May 31, 2024, the Council of the European Union adopted a new AML/CFT package and the Sixth Anti-Money Laundering Directive ('**6AMLD**'),[59] which will replace the 4AMLD and will need to be transposed by member states by July 10, 2027. The 6AMLD requires that member states regulate gambling services to minimise the risk of money laundering.

[58] *"Guidelines on fighting money laundering and terrorist financing for the European online gambling sector,"* EGBA, March 2023: https://www.egba.eu/uploads/2023/03/230306-EGBA-Guidelines-on-AML-for-Online-Gambling-FINAL.pdf.

[59] Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849.

C. United States ('US')

The Bank Secrecy Act ('**BSA**') in the US classifies casinos and card clubs as financial institutions for the purposes of AML controls and federal reporting obligations. However, games of skill are typically not considered 'financial institutions' as per the BSA, and thus, are not directly subject to its AML rules and regulations. Further, such platforms often delegate AML compliance responsibilities to their financial partners, such as banks and payment processors, who handle customer payments and account funding.

Nevertheless, skill gaming operators proactively implement measures to curb money laundering on their platforms. For instance, platforms such as Star Fantasy Leagues regularly check their customer lists against the Office of Foreign Assets Control's databases to confirm that their users are not on any sanction lists.

The 2024 National Money Laundering Risk Assessment, released by the US Department of Treasury,[60] highlights that while online gaming can take a number of forms, there are several emergent money laundering risks particular to sports betting, offshore sports betting,[61] and virtual asset gambling. The assessment notes that these activities share many of the same risks found in traditional brick-and-mortar casinos but also present unique challenges due to their rapid growth, varying regulatory standards, and the anonymity they offer.

D. United Kingdom ('UK')

In the UK, online gambling is regulated by the Gambling Commission, established under the Gambling Act 2005. The gambling sector in the UK encompasses various activities, including remote and non-remote licensed casinos, remote and on-course and off-course betting, remote and non-remote bingo, lotteries, and arcades.

Presently, only remote and non-remote casinos are regulated under national money laundering regulation. All other gambling activities are governed by the Gambling Act 2005 wherein, gambling operators have obligations under Gambling Commission's Licence Conditions and Codes of Practice ('**LCCP**'); and all gambling operators have legal duties under the Proceeds of Crime Act 2002 ('**POCA**') and the Terrorism Act 2000 ('**TACT**') to mitigate financial crime.

Gambling operators are required to take note of relevant provisions under LCCP, particularly, *Licence condition 12.1.1*, which requires operators to:

- Conduct an assessment of the risks of their business being used for money laundering and terrorist financing.
- Have appropriate policies, procedures, and controls to prevent money laundering and terrorist financing.

---

[60] *"2024 National Money Laundering Risk Assessment,"* US Department of Treasury, February 2024, https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf.

[61] It is important to note that sports betting is distinct from daily fantasy sports contests, as daily fantasy sports contests are predominantly skill-based and thus do not constitute gambling under the US laws.

- Ensure that such policies, procedures, and controls are implemented effectively, kept under review, and revised appropriately to ensure they remain effective.
- Take into account any applicable learning or guidelines published by the Gambling Commission from time to time.

The national risk assessment conducted by HM Treasury and the Home Office provides a comprehensive overview of the relative risks of money laundering across various regulated financial sectors and designated non-financial businesses and professionals. Within this context, as per 2020 assessment, the gambling sector is currently rated as a low-risk area for money laundering compared to other sectors such as banks, credit institutions, money service businesses, legal services, high-value dealers, art, and accountancy.[62]

E. Indian Position

The offence of 'money laundering' is defined under *Section 3* of Prevention of Money Laundering Act, 2002 ('**PMLA**') as:

> *"Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of offence of money-laundering."*

As per *Section 2(1)(wa)* of PMLA, a 'reporting entity' means a banking company, financial institution, intermediary or a person carrying on a designated business or profession. Further, 'a person carrying on designated business or profession' is defined under *Section 2(1)(sa)* of PMLA, among others, as:

> *"(i) a person carrying on activities for playing games of chance for cash or kind, and includes such activities associated with casino;*

Presently, the PMLA does not classify an operator offering games of skill as a reporting entity and thus, obligations under the PMLA currently do not apply to a game of skill operator. However, games of chance, including casinos were designated as reporting entities post the FATF India assessment in 2009-2010 under 'designated business or profession' via an amendment in 2013.[63] The objective for introduction of the amendments in 2013 was:[64]

> *"The problem of money-laundering is no longer restricted to the geopolitical boundaries of any country. It is a global menace that cannot be contained by any nation alone. In view of this, India has become a member of the Financial Action Task*

[62] *"National risk assessment of money laundering and terrorist financing 2020,"* HM Treasury and Home Office, December 2020, https://assets.publishing.service.gov.uk/media/5fdb34abe90e071be47feb2c/NRA_2020_v1.2_FOR_PUBLICATION.pdf.

[63] The Prevention of Money Laundering (Amendment) Act, 2012, Ministry of Law and Justice, January 3, 2013, https://sansad.in/getFile/BillsPDFFiles/Notification/2011-133-gaz.pdf?source=loksabhadocs.

[64] *Para 2*, Statement of Objects and Reasons, The Prevention of Money-Laundering (Amendment) Bill, 2012.

> *Force and Asia Pacific Group on money-laundering, which are committed to the effective implementation and enforcement of internationally accepted standards against money-laundering and the financing of terrorism. Consequent to the submission of an action plan to the Financial Action Task Force to bring anti money-laundering legislation of India at par with the international standards and to obviate some of the deficiencies in the Act that have been experienced by the implementing agencies, the need to amend the Prevention of Money-Laundering Act, 2002 has become necessary."*

While casinos have long been subject to the PMLA, on March 7, 2023, the Central government issued a notification classifying entities engaging in specific virtual digital asset ('**VDA**') activities as 'persons carrying on designated business or profession'.[65] As a result, activities such as exchanging virtual digital assets with fiat currencies, exchanging different forms of virtual digital assets, and transferring virtual digital assets now classify an entity as a reporting entity.

This could potentially expand the application of the PMLA to include certain activities carried out by online gaming operators. In-game tokens and objects, which often have value and can be transferred, stored, or traded, might be included under this framework. However, it is still uncertain whether these in-game tokens and objects are currently regulated as VDAs.[66]

---

[65] Gazette notification, Ministry of Finance, March 7, 2023, https://egazette.gov.in/WriteReadData/2023/244184.pdf

[66] *"PMLA Concerns for the Skill Gaming Sector?,"* Cyril Amarchand Mangaldas, March 16, 2023, https://corporate.cyrilamarchandblogs.com/2023/03/pmla-concerns-for-the-skill-gaming-sector/#_ftn2.

KEY OBSERVATIONS OF PART I

Risk Factors of Money Laundering in Online Gaming Sector in India

In the Indian context, key risks include illegal operators, in-game currencies and artefacts, the use of cryptocurrencies, and mule accounts. In a few instances, money dumping may also be employed.

Illegal Markets are Highest Risk Factor

India's illegal gambling and betting market sees deposits exceeding USD 100 billion annually, facilitated by sophisticated methods and compounded by weak regulatory oversight.[67]

Even when authorities block these operators, they often find ways to bypass the restrictions. For instance, blocked websites often circumvent these measures by launching mirror sites with slightly modified URLs. Current strategies, such as website blocking, are easily circumvented by using VPNs or geoblockers, highlighting the need for more effective enforcement measures.

Advertisements on the Internet are Facilitating Operations of Illegal Betting Operators

Illegal operators have successfully defrauded users through their advertising practices. These advertisements are often highly exaggerated and frequently promoted by internet and influencers with millions of followers, allowing these operators to attract a large number of users.

This is likely the most effective method to deceive individuals into spending significant amounts of money on such dubious platforms.

As In-Game Economies Become More Sophisticated, It is Crucial to Assess the Vulnerability of Systems Offering In-Game Assets

The ability to transfer and convert gaming assets into fiat currency or crypto-assets has resulted in a rise in money laundering and fraud on online gaming platforms. Despite this, there has been limited investigation into this issue and the methods to control or eliminate these risks.

However, as companies push further into the advanced technologies such as metaverse for offering gaming experience, the threat of money laundering could loom larger. As such, this is an area that policymakers should watch closely.

---

[67] CKSIndia. 2024a. "*GAMBLING AWAY INDIA'S SOVEREIGNTY – CKS*." May 18, 2024. https://cksindia.org/gambling-away-indias-sovereignty/#_Toc165628282.

Application of Anti-money Laundering Framework in Online Gaming: International Perspective

Online games, especially those with higher skill levels fall outside the scope of AML regulations. Casinos, as recommended by the FATF, are subject to AML laws in all the jurisdictions we studied. Recently, due to increased concerns about the potential for money laundering, calls for including online gaming platforms that enable the trade of *de facto* convertible in-game currency to be regulated similarly to crypto-asset service providers is growing.

Payment Methods are Crucial Determinant of Money Laundering Risks

Payment methods vary in their risk of money laundering, with some, such as cryptocurrencies, cash, and payments through unauthorised channels, present higher risks. Conversely, transactions made through verified bank accounts or cards issued by authorised institutions are generally lower risk, as these institutions implement rigorous customer due diligence processes and ensure traceability of funds.

Regulation is Key to Ensuring Financial Integrity

Across all the jurisdictions examined, gaming operators are mandated to adhere to specific obligations designed to uphold financial integrity on their platforms. These requirements are typically embedded in licensing conditions or regulatory frameworks governing these platforms.

To effectively enhance financial integrity and mitigate money laundering risks within the sector, it is essential to incorporate principles of financial integrity into the law and establish a consistent framework for operators to follow.

RECOMMENDATIONS OF PART I

Key Policy Proposals	
Illegal Operators	• **Dedicated Task Force for Illegal Operators:** Establish a dedicated task force consisting of experts to recommend policy measures for combating illegal operators. For instance, determining the legality of platforms, ensuring compliance with KYC norms, promoting the use of digital payments, and maintaining proper fund transfer discipline, thus creating a more secure and accountable ecosystem. • **Implement a Whitelisting Mechanism based on GST Registration:** Online RMG operators must register under the CGST Act, 2017, within thirty days of becoming liable for registration. Likewise, offshore online money gaming operators are also required to obtain mandatory GST registration. However, the most recent update from the Parliament indicates that no offshore entities have registered to date. In a related effort to combat rising cyber fraud, whitelisting frameworks have proven successful in the fintech space. For example, the Reserve Bank of India has shared with MeitY a whitelist of 442 approved digital lending apps to curtail illegal operations. Similarly, a whitelist of legal online RMG could be published and updated from time to time. This initiative would ensure that payment gateways, hosting providers, and ISPs provide services only to listed operators, further requiring ongoing monitoring and enforcement to ensure compliance and making it extremely difficult for illegal operators to operate. • **Combat Advertising of Illegal Betting and Gambling Platforms:** The Ministry of Information and Broadcasting, being the nodal body for online advertising, should issue an Advisory that only whitelisted online gaming applications can advertise. The Advisory should be directed to all relevant stakeholders, including intermediaries, advertising agencies, and influencers, ensuring they only partner with whitelisted online gaming platforms. • **Blocking Transactions to Illegal Operators:** The government must collaborate with banks and payment system providers to establish a protocol for blocking transactions to known illegal gambling and betting operators. • **International Cooperation:** Given the global reach of online gambling and betting, the Indian Government should lead efforts to develop multilateral agreements with international organisations and other countries to enhance cross-border cooperation in combating illegal online gambling. • **Public Awareness and Education:** Most users are often unaware of the intentions behind illegal platforms, as evidenced by recent cases like Fiewin. To assist users in distinguishing between legitimate and illegitimate platforms, the government should develop guidelines based on the whitelisting framework mentioned in above. By providing clear criteria and easily understandable illustrations, users can make informed decisions and avoid platforms that engage in deceptive practices.

In-Game Assets and Currencies	● **Vulnerability Assessment:** A vulnerability assessment is essential to fully understand how in-game assets and currencies contribute to money laundering risks and to determine the scale of secondary markets for these assets. A comprehensive assessment of in-game assets could enable the government to provide clear guidelines on whether these tokens and objects fall within the regulatory scope of VDAs for the purposes of the PMLA regime. ● **Need for Suitable Measures:** On the basis of the vulnerability assessment, if required, the government should suitably develop law to mitigate and address these challenges. ● **Lootboxes:** There should also be a thorough deliberation on whether loot boxes constitute gambling and their potential impact on money laundering, with appropriate regulations introduced accordingly.
Money Mules	Financial institutions must implement a robust AML program and take decisive actions to combat money mules. Key strategies include: ● Enhance AML systems and customer onboarding processes to detect suspicious behaviours linked to money mule activities. ● Deploy AI/ML-driven detection models and other innovative solutions for better identification of money mules. ● Periodically review key systems and controls to evaluate their effectiveness against emerging risks like money mules. ● Develop comprehensive training programs for staff and raise awareness among customers about the risks of money mules. ● Promptly report suspicious or fraudulent transactions to regulators by filing Suspicious Activity Reports (‘**SARs**’). ● Build a strong investigative team equipped with advanced analytical capabilities to respond swiftly to identified risks. ● Establish open communication channels with regulatory authorities, industry, and enforcement agencies to gather credible intelligence on evolving risk themes.

PART II:

VULNERABILITY ASSESSMENT OF MONEY LAUNDERING IN RMG SECTOR

Building on the discussion in *Part I*, it is crucial for each sub-segment of online gaming to conduct a vulnerability assessment to identify potential threats and risks. This section evaluates the vulnerability of money laundering within the RMG sub-segment. Vulnerability levels are determined by the presence and effectiveness of controls; inadequate or poorly implemented controls signify higher vulnerability.

For this assessment, the focus areas are: Customer Due Diligence (‘**CDD**’), Acceptable Payment Methods, Transaction Monitoring, Reporting Mechanisms, Employee Training, Technological Safeguards, and the presence of Supervisory Authority for compliance and safeguards.

REGULATION AND INDUSTRY PRACTICES

In April 2023, pursuant to powers vested with the Central government under the Constitution, the MeitY took a significant step by introducing a new central regulatory framework for online gaming. Leveraging its rule-making authority, MeitY brought amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (‘**Online Gaming Rules**’) to effectively regulate online gaming.[68]

The Online Gaming Rules marked a new era of responsible online gaming by establishing strict guidelines to ensure the safety of citizens and the accountability of the gaming industry. They introduced the concept of ‘permissible online game’ and allowed only such online real money games in India that are verified by Self-Regulatory Bodies (‘**SRBs**’), notified by MeitY. However, it is important to note that the SRBs are yet to be notified, which has impacted the implementation of the Online Gaming Rules.

Given that the Online Gaming Rules have not yet been operationalised, operators within the RMG sector continue to deploy individualised controls to address these risks. Within this landscape, there are operators who demonstrate greater responsibility by being members of various federations and associations, complying with the self-regulatory charters established by these bodies—albeit with varying degrees of success.

To assess the effectiveness of these controls, where they exist, we examined various Codes of Conduct adopted by major gaming federations and associations, which outline self-regulation guidelines for RMG operators. However, it is important to note that, while these practices are detailed in the Codes of Conduct, there are no independent audit reports available in the public domain that verify the degree of adherence to these practices or identify existing gaps.

[68] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023, Ministry of Electronics and Information Technology, April 6, 2023, https://www.meity.gov.in/content/gazette-notification-vide-gsr-275e-dated-642023-regarding-amendments-it-intermediary.

Description	Provisions
Customer Due Diligence	Operators are mandated to undertake KYC as per applicable law. These Codes of Conduct generally mandate that the KYC is conducted at the stage of first withdrawal request or making a cumulative deposit of INR 50,000 or more, whichever is earlier.
Payments	One Code of Conduct requires operators to verify that the bank account details provided by the player match those in the operator's database to ensure that the person receiving the funds is the same as the depositor. Another Code of Conduct mandates that all transactions conducted on the platform must be carried out in digital mode exclusively, through recognised digital banking channels, credit/debit cards, and approved mobile wallets, and transactions in cash or cryptocurrencies should not be allowed. The same Code of Conduct mandates that operators must ensure that they do not allow or facilitate transactions through unauthorised payment systems, and/or encourage or facilitate money laundering activities or transactions which are non-compliant with applicable laws.
Monitoring	Operators are required under all Codes of Conduct to implement internal controls, systems, and measures, along with appropriate policies and procedures to prevent the use of their platform for money laundering or other unlawful activities. This includes implementing geo-fencing technology to restrict access to gaming platforms in unauthorized regions, ensuring compliance with local regulations.
Technological Safeguards	One Code of Conduct requires operators to adhere to the necessary internal financial controls as provided under *Section 143(3)(i) of the* Indian Companies Act, 2013. This provision deals with the auditor's report to stipulate whether the company has adequate internal financial controls with reference to financial statements in place and the operating effectiveness of such controls. Operators are also required to appoint a Grievance Officer to address customer complaints and maintain records of grievance resolutions, thereby enhancing transparency and accountability.
Others	**Record-keeping** One Code of Conduct mandates that operators maintain records of all transactions on their platforms for a period of 3 years from the date of cessation of transactions between the user and the operator, while another Code of Conduct requires operators to keep all logs of request of ID, address and bank account change by the player for the purposes of compliance. **Auditing** One Code of Conduct requires an external audit of these practices to verify that the code is being properly implemented in practice. **Annual Risk Assessment** One Code of Conduct requires controls and preventive measures put in place to be commensurate to the risk identified in annual risk assessment. Another Code of Conduct requires operators to conduct annual assessment of risks on their platform related to money laundering and terrorist financing.

EXISTENCE OF GAPS WITHIN THE RMG SECTOR

The RMG sector, despite adhering to compliance measures, exhibits gaps that may increase its vulnerability:

A. Lack of Regulation and Uniform Standards

Progress in regulating the sector has been impeded by the non-implementation of Online Gaming Rules. Consequently, RMG operators are left to follow disparate rules. This inconsistency may sometimes lead to channels for unethical practices. When compliance requirements are inconsistent and unclear or non-existent, some operators may be discouraged from adhering to best practices.

Further, the absence of an operationalised framework has blurred the distinction between legal and illegal activities, creating fertile ground for illegal betting and gambling operators to operate without repercussions.

B. Non-Existence of Supervisory Authority

At present, the online gaming sector in India is devoid of a designated supervisory or regulatory authority. Consequently, there is no established framework or requirement for operators to implement policies and controls aimed at mitigating the risks of financial fraud or money laundering. International experience demonstrates that the presence and efficacy of a supervisory authority, responsible for monitoring compliance and enforcing safeguards, are essential for ensuring financial integrity within the online gaming sector.

C. Absence of Published External Audit Reports

Although self-regulatory measures such as KYC, transaction monitoring, and technological safeguards are in place, their implementation appears to be inconsistent. Moreover, as mentioned earlier, it is important to note that while some federations conduct external audits, there is a lack of transparency in these audits, and no reports are made publicly available.

D. Lack of Appropriate Enforcement Mechanisms

Internationally, jurisdictions have standardised processes in place, either as part of licensing requirements or specialised legislation, to minimise the risk of money laundering. In India, the absence of regulation or uniform standards means there are currently no consistent enforcement mechanisms for non-compliance. Enforcement is fragmented, with various ministries taking sporadic action against notorious offenders.

TYPOLOGY OF RISK

The below table delineates prevalent risks within the RMG sector, stemming from operators, customers, payment methods, and the government. These risks, if realised, may pose threat of facilitating financial misconduct and money laundering activities:

DESCRIPTION OF RISK	POTENTIAL FOR FINANCIAL MISCONDUCT & MONEY LAUNDERING
OPERATOR	
Operators failing to comply with self-regulatory charters issued by gaming federations or associations	Allows operators to engage in unethical activities.
Operators engaging with and winning directly and indirectly on their own products	Facilitates direct manipulation of gaming outcomes.
Lack of competence of key personnel to mitigate and deal with money laundering risks	Lead to insufficient oversight and enforcement, creating gaps in effectively addressing and mitigating risks.
Inadequate or lack of KYC checks	Allows for the entry of illegitimate users and obscures identities.
Gaming operations run or acquired by organised criminals to launder criminally-derived funds	Enables large-scale laundering of criminal proceeds through gaming activities.
Lack of processes to deter money dumping	The absence of robust processes to detect and prevent player-to-player collusion increases the risk, where players collude to manipulate game outcomes for mutual benefit.
CUSTOMER	
False or stolen documentation used to bypass controls to launder criminally-derived funds	Facilitates entry onto the platform under false identities to launder money.
Accessibility to multiple accounts	Smoothes the process of breaking down large sums into smaller, less detectable transactions.
Customers from high risk or non-cooperative jurisdictions using remote facilities to launder criminally-derived funds	Exploits regulatory differences between jurisdictions to launder funds through online gaming.
'Smurfing' to break large transactions into smaller, less suspicious amounts	Aids in disguising the origin and intent of funds through segmented transactions.
'Mule' accounts	Involves participants, sometimes unwitting in transferring illicit funds to evade detection.
Use of third parties or agents to obscure the source or ownership of money	Utilises intermediaries to mask the trail of funds laundered through gaming platforms.

GOVERNMENT	
Absence of Supervisory Authority / Regulator	Leads to inconsistent oversight and enforcement of regulations, increasing the risk of financial misconduct and inadequate management of financial risks.
MEANS OF PAYMENT	
Payment through cash or unauthorised methods	Presents opportunities for transactions that bypass digital scrutiny.
Crypto asset transactions	In some cases, provide alternative payment methods that are harder to trace.
If withdrawals are not directed back to the original deposit source	Allows for potential gaps in tracking and verifying transactions.

KEY OBSERVATIONS OF PART II

Existence of Vulnerabilities in the Indian RMG Sector

Money laundering in RMG can occur in two primary ways: either operators of illegal platforms engage directly in laundering activities, or users with an intent to channel illicit funds may engage on online game platforms. In the latter case, the risk arises only if operators implement lax KYC practices or have weak compliance measures.

While existing self-regulation and voluntary practices followed by operators offer a degree of mitigation, the sector remains vulnerable due to the absence of regulation and supervisory authority resulting in non-existent enforcement and oversight mechanisms.

Risks is Associated with Payments, Customer, Operators and at the Government Level

The money laundering risks associated with the RMG sector can be categorised at multiple levels, including operators, customers, government oversight, and the diverse payment methods utilised. For operators, risks include inadequate KYC controls, non matching of withdrawal and deposit accounts, absence of policies to prevent player to player collusion and insufficient training of personnel. Customer-related risks involve the use of false or stolen documents to create accounts, access to multiple accounts with a single operator, and methods such as smurfing and the use of mule accounts. On the governmental side, risks arise from the lack of regulation and a dedicated supervisory authority.

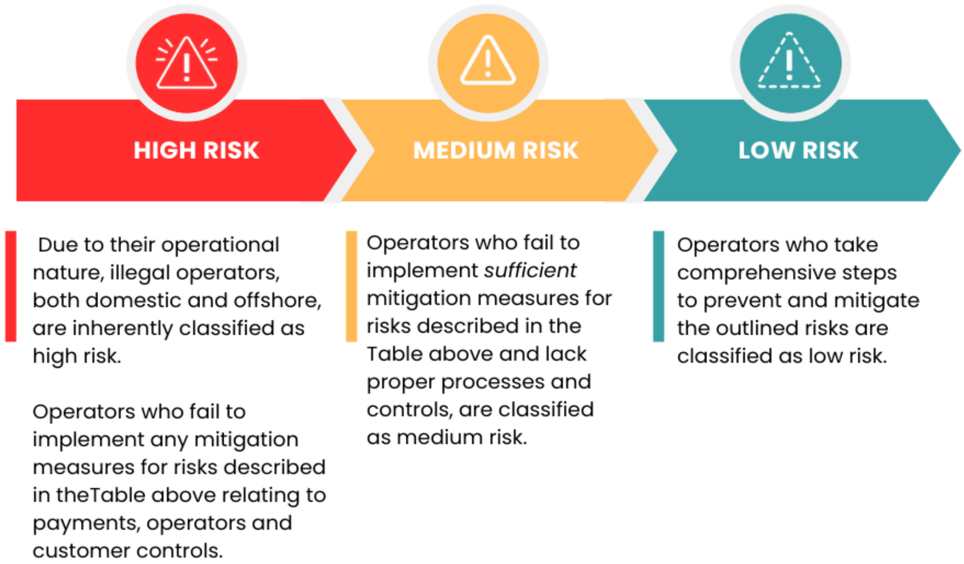
Unwary Users Are Falling Victim To Illegal Operators Due To Their Inability To Distinguish Between Legitimate Online Gaming Providers And Illicit Ones

Illegal gambling and betting platforms often masquerade as skill-based gaming (as discussed in *Part 1*), taking advantage of the absence of a clear and enforceable regulatory framework for online skill gaming. This regulatory void makes it difficult for users to distinguish between legitimate operators and illegal platforms. Additionally, the widespread availability of illegal betting and gambling apps—frequently accessible even after being blocked—via unauthorised channels such as Telegram, websites, and other unofficial platforms, coupled with misleading advertising (often featuring influencers), fuels the growing popularity of these illicit operations. Consequently, unsuspecting users are left vulnerable to money laundering schemes and fraud.

Disparate Mitigation Practices Deployed by RMG Operators

While various federations have established codes of conduct, it is unclear how consistently these are followed. Enforcement efforts appear minimal, except for one federation that conducts audits. However, the outcomes of these audits remain unclear, as no public reports are available, making it difficult to assess their effectiveness. Ultimately, the responsibility for anti-money laundering prevention lies largely with the operators themselves.

Risk Scale:



Why Risk is Low for Operators Who Adhere to the Measures Outlined in the Table

One major factor is **traceability**—while illegal platforms often operate in cash-heavy or anonymous environments (such as extensive use of cryptocurrencies), operators taking comprehensive steps (*as outlined in the table*) typically allow transactions through reporting entities, making it easier to track the flow of funds. These operators usually prohibit cash and cryptocurrency transactions, further reducing the use of untraceable or decentralised currencies for money laundering.

Additionally, the risk of **smurfing** on peer-to-peer ('**P2P**') online gaming platforms registered with GST is low, especially with the recent imposition of a 28% GST on deposits, platform fees of up to 20%, and a 30% TDS. These high costs significantly reduce the financial incentive for money laundering, as the potential costs outweigh the benefits.

Lastly, the **average transaction size** in such gaming platforms is typically small, making these platforms unsuitable for large-scale money laundering. Further, payouts are contingent on winning outcomes, meaning there is no guaranteed return of funds, unlike in traditional laundering schemes—unless the operator itself is involved in laundering, as seen in cases like the Fiewin app.

RECOMMENDATIONS OF PART II

<table>
<tr><th colspan="2">KEY POLICY PROPOSALS</th></tr>
<tr><td>Regulate Online Gaming and Establish a Supervisory Mechanism</td><td>It is imperative that MeitY urgently address the regulation of the online gaming sector, to establish a robust framework for governance, administration, and compliance.

MeitY could achieve this by either operationalising the existing Online Gaming Rules with necessary amendments to address any current gaps or by enacting entirely new regulations as deemed appropriate.</td></tr>
<tr><td rowspan="4">Incorporate Principles of Financial Integrity in Law</td><td>Currently, the Online Gaming Rules do not include provisions (except for KYC requirements) to ensure financial integrity within the sector. Thus, it is recommended that the government incorporate Principles outlined below either,

- by amending the Online Gaming Rules and incorporating these Principles under Rule 4 (relating to additional due diligence) or

- by incorporating these Principles into the new Statute, Regulation or Rules for online gaming as may be notified in future.</td></tr>
<tr><td>Principle 1 - Risk Assessment: Online gaming operators must conduct risk assessment exercises regularly to identify potential financial frauds, money laundering risks and vulnerabilities on their platform.

As part of the risk assessment, online gaming operators must conduct an evaluation of fundamental risk factors, including but not limited to, the types of customers they onboard, particularly those identified as high-risk, the characteristics of the products and services they provide, various transaction types, the financial channels for deposits and withdrawals offered, and the platforms and channels utilised. And building systems to ensure there is no money dumping.</td></tr>
<tr><td>Principle 2 - Internal Controls and Procedures: Informed by the insights obtained from the risk assessment, each operator must develop policies and controls aimed at mitigating financial risks identified:

These may include:

- Operators shall prohibit all their employees, contractors, and any spouse, children, or parents of any employee or contractor from participating in online games that it offers.

- Operators shall contract with a third party to perform an annual independent audit in accordance with generally accepted accounting principles

- As and when the sector is regulated and a supervisory mechanism is prescribed, the operator shall submit the Audit Report to the supervisory authority at the end of the fiscal year.</td></tr>
<tr><td>Principle 3 - Robust KYC Mechanisms: Online gaming operators must verify the identity of every user before accepting any deposits, in accordance with KYC procedures as detailed under RBI Master Directions, Online Gaming Rules, and other relevant regulations.

Additionally, operators should apply customer due diligence measures at appropriate intervals, based on the assessed risk level of each customer.</td></tr>
</table>

	Principle 4 - Prohibition on Multiple Accounts: Online gaming operators must include robust provisions in their terms of service to prevent the creation and use of duplicate accounts. Users should be strictly prohibited from registering or using multiple user IDs. Operators can limits each player to one active account by: - Verifying each player's true identity and location. - Closing each account previously held by a player when a new account is opened by that same player. - Using technologically reasonable measures to detect and prevent the use of a player's account by other players.
	Principle 5 - Legitimate Payment Methods: Online gaming operators should ensure that deposits are strictly limited to those facilitated by registered financial entities, such as banks, credit and debit cards, and other proper channels as may be prescribed, explicitly excluding cash and any other unverified means.
	Principle 6 - Report Suspicious Transactions: Online gaming operators must establish and enforce comprehensive policies and procedures, including an internal system, to effectively identify and report suspicious transactions to: - Supervisory Authority as may be established in future; - Financial institutions (or regulated entities) as maybe applicable from case to case basis; and - Amongst operators themselves.
	Principle 7 - Record Keeping: Online gaming operators must maintain transaction records for a particular duration as may be specified.
Coordinated Efforts	The government may consider establishing a cross-ministerial Comprehensive Screening List that integrates critical watchlists from various ministries such as Home Affairs, Finance, and External Affairs. This list, updated regularly and made accessible via a publicly available Application Programming Interface ('**API**'), would enable online gaming companies to programmatically screen and restrict access to their platforms for individuals or entities flagged for legal or security reasons. Further, financial institutions should collaborate closely with online gaming operators to ensure robust internal financial controls and effective KYC practices.

contact@digitalindiafounaiton.org | www.digitalindiafoundation.org