Follow-up Committee on Manipulation of Sports competitions
(T-MC)

Council of Europe Convention on the Manipulation of Sports Competitions (CETS No. 215)

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, 3 March 2026 T-MC(2025)5rev

Follow-up Committee on the Manipulation of sports competitions

Council of Europe Convention on the Manipulation of Sports Competitions (CETS No. 215)

Guidelines on combatting money Laundering through sports betting

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Money laundering continues to fuel organised crime

It can support profit-driven criminal activities, can finance terrorism, and is a lucrative activity in itself. It is estimated that between 800 billion and 2 trillion US dollars is laundered worldwide each year (UNODC, 2021).

The European Union has recently strengthened its regulatory framework, but vulnerabilities persist — particularly including within in the sports betting sector.

The betting market presents multiple high-risk characteristics

It is large, fast-moving, and highly fluid. Transactions are rapid, sometimes cross-border, and conducted across numerous platforms.

Certain features of betting accounts, including rapid fund movements, the use of multiple accounts, and diverse payment options, create opportunities to obscure financial flows.

Some operators are based in jurisdictions with limited or uneven supervisory requirements. Criminal groups exploit such gaps, either by misusing existing services or by setting up their own structures to launder illicit funds.

Diversity of betting types facilitates concealment

With a wide range of formats (including in-play betting, fixed-odds, peer-to-peer wagers, spread betting, bets on minor events, etc.), there are many ways to fragment stakes and obscure the trail.

Betting on opposite outcomes (« surebet ») or using multiple accounts can also help simulate losses or spread winnings, making financial flows harder to trace.

Certain payment methods enhance anonymity

Certain payment channels, such as prepaid cards, vouchers, e-wallets, or some crypto-assets, allow funds to be placed or transferred with limited transparency, depending on how verification and due diligence are applied.

Transactions can be carried out quickly, sometimes in small, repeated amounts or across multiple platforms, which complicate the identification of the origin of funds.

Controls remain insufficient

Customer due diligence (CDD)[1] obligations exist in most jurisdictions, but implementation remains uneven. Suspicious activity reports (SARs) are under-reported or delayed, and follow-up investigations remain limited in many jurisdictions.

Limited specialised resources and competing priorities weaken the focus on financial flows, and limited international cooperation also hampers effective action.

Solutions exist to improve prevention and action

The report recommends some national-level measures: enhancing identity checks, regulating payment methods, improving operator oversight, and facilitating information-sharing with financial institutions. It also calls for better detection of unusual behaviours and stricter monitoring of high-risk accounts.

At the international level, it encourages stronger cooperation between financial intelligence units, regulators and law enforcement authorities. The aim is to better identify the misuse of the sector and reduce its attractiveness for laundering money.

---

[1] Customer Due Diligence (CDD): Risk-based checks on customers, including verifying their identity, understanding their profile, and reviewing transactions to detect unusual activity.

INTRODUCTION

1. Money laundering at the heart of organised crime operations

Money laundering is a core activity in facilitating organised crime, terrorist financing, and broader illegal economic activities. It refers to the process by which proceeds of criminal activity are made to appear legitimate (Moneyval)[2]. Once laundered, these funds can be reintegrated into the legal economy through investments in businesses or financial schemes, further obscuring their true source.

This phenomenon is rapidly expanding and increasingly globally with widely cited international estimates placing the global value of money laundering at 2–5% of global GDP, corresponding to a range extending up to USD 2 trillion annually (UNODC)[3]. In response to this threat, the European Union has introduced a new anti-money laundering (AML/CFT)[4] package aimed at strengthening the consistency and effectiveness of the fight against money laundering across Member States.

2. A multifaceted criminal activity

Money laundering is a criminal activity in its own right, constantly evolving. Its complexity and level of sophistication can vary widely, from simple techniques to elaborate schemes involving legal entities, shell companies, or cross-border operations (Organised Crime in Australia, 2017)[5].

Criminals tend to target sectors or mechanisms that maximise the chances of concealment, particularly poorly regulated environments, digital platforms, or anonymous payment systems. They may also exploit differences between national AML/CFT frameworks.

3. A rapidly expanding sports betting market

Over the past thirty years, the global sports betting market — defined as the staking of money in the hope of a financial gain, dependent on the occurrence of a future and uncertain event related to a sports competition[6] — has grown significantly in both scale and nature.

According to the United Nations (UNODC, 2021)[7], the total annual volume of bets could exceed USD 1.4 trillion. The clandestine and illegal nature of part of the activity, the lack of harmonised regulation, and the complexity of operations (such as stake transfers and hedging techniques) make global assessment difficult.

In this context, bettors' accounts display vulnerabilities comparable to those observed in financial accounts subject to limited or unevenly applied supervision.

Recent cases in Australia[8] and the United Kingdom[9] illustrate that vulnerabilities can emerge in any jurisdiction, underscoring the need for consistent implementation of AMF/CFT obligations across all jurisdictions~~.~~

4. A growing priority for European authorities

In 2022, the European Commission (SNRA – Supranational Risk Assessment 2022)[10] published its risk assessment report on money laundering and terrorist financing. The gambling sector, including betting, was classified at the highest risk level. The UK Gambling Commission's 2023 national risk assessment classifies both remote and land-based betting as activities presenting a high level of money-laundering and terrorist-financing risk, placing them among the gambling products that require the strongest safeguards.

---

[2] MONEYVAL in brief (available here), it is the Council of Europe's FATF-style regional body, responsible for assessing compliance with international AML/CFT standards in member States not evaluated directly by the FATF.
[3] MONEYVAL (2023a), Annual Report 2022 (available here); or between 800 billion and 2,000 billion dollars according to UNODC (n.d.), Money Laundering (available here).
[4] AML/CFT (Anti-Money Laundering / Countering the Financing of Terrorism): refers to legal, regulatory and institutional measures aimed at preventing and detecting money laundering and terrorist financing.
[5] Australian Criminal Intelligence Commission (2017), Organised Crime in Australia 2017 (available hesre).
[6] Council of Europe, Convention on the Manipulation of Sports Competitions (Macolin Convention), art. 3.
[7] Annual gross gaming revenue (GGR), a more relevant indicator, is estimated at around €65 billion a year (CK Consulting).
[8] Australian Securities and Investments Commission (2023), Star provides $150m for fines and penalties after ASIC raises concerns (available here); Reuters (2023), Australian court approves $300m money laundering fine for Blackstone's Crown Resorts (available here).
[9] Gambling Commission (2023), £6.1m fine for online operator In Touch Games (available here); Gambling Commission (2022), £9.4m fine for online operator 888 (available here).
[10] European Commission (2022), Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and linked to cross-border activities (available here).

A scientific report by the Transcrime institute (Nazzari and Riccardi, 2024), based on Italian law enforcement data, shows that gambling and betting have become the primary investment sector for Italian mafias in money laundering operations.

5. Link between sports manipulation and money laundering

Despite the close links between the two phenomena, the risks of money laundering through betting continue to receive less political attention than those related to the manipulation of sports competitions. Profits from match-fixing must be laundered, and the funds invested in such schemes often originate from prior illegal activities.

Article 16-3 of the Macolin Convention explicitly requires that the manipulation of competitions be included in anti-money laundering prevention frameworks, with obligations for betting operators regarding due diligence, record-keeping, and reporting.

UNODC[11] reports that the manipulation of sporting events produces criminal proceeds which are commonly integrated into the financial system through betting accounts and other payment structures.

6. Purpose of this document

This document provides an overview of money laundering risks in sports betting, offering a clearer understanding of their nature, scale, and dynamics. It also presents a set of recommendations aimed at strengthening prevention, detection, and investigative capacities.

VULNERABILITY FACTORS OF THE SPORTS BETTING MARKET TO MONEY LAUNDERING

1. A fluid, transnational market: the ideal breeding ground for money laundering

Money launderers favour large, dynamic, and hard-to-regulate markets. The gambling sector has long been used for this purpose (James Banks, 2017) [12].

The global betting market is particularly vulnerable due to its high fluidity — cross-border accessibility, speed of operations, and the proliferation of platforms (Organised Crime in Australia, 2017)[13]. Bettors can place wagers across multiple jurisdictions. The degree of scrutiny applied to betting activity varies significantly, depending on the legal and supervisory framework in place.

The wide range of betting options — in-play, fixed-odds, betting exchanges, spot betting[14], spread betting[15] — increases the opportunities to disguise illicit flows (Gambling Commission, 2020)[16]. Certain techniques, such as betting on opposing outcomes or peer-to-peer betting, facilitate collusion and can complicate the detection of unusual flows.

Technological innovations, including bets linked to NFTs (Non-Fungible Tokens)[17], the Metaverse[18], and Web3[19], further heighten the risks by bypassing traditional regulation (Purbrick, 2023[20]). The use of multiple or VIP accounts, which often lack proper oversight, enables the concealment of fund origins (Moneyval, 2013[21]). Finally, intense competition pushes operators to offer higher return rates to players, thereby lowering the cost of laundering (Precrimbet, 2017[22]).

2. Anonymous payment methods facilitate money laundering

Beyond the features of the market itself, payment methods represent a major vulnerability. It is possible to place large bets anonymously, especially when operators are outside the scope of effective supervision or operate from jurisdictions with limited

[11] UNODC, Global Report on Corruption in Sport (2021), United Nations Office on Drugs and Crime.
[12] James Banks, Gambling, Crime and Society (London: Palgrave Macmillan, 2017).
[13] Australian Criminal Intelligence Commission (2017), Organised Crime in Australia 2017 (available here).
[14] A bet placed on a very specific, isolated event or action during a match (e.g. first corner, next yellow card), often live, which makes it a particularly vulnerable format for manipulation.
[15] A form of betting where the win or loss depends on the difference between the actual result of an event (e.g. number of goals or corners) and a range predefined by the operator, multiplied by the stake per unit of difference.
[16] Gambling Commission (2023), The Money Laundering and Terrorist Financing Risks within the British Gambling Industry (available here).
[17] Unique digital tokens registered on a blockchain, used in certain bets to represent virtual objects or stakes whose value depends on sporting events.
[18] Immersive 3D virtual environments where users can interact, play or bet, often via crypto-currencies, outside of any traditional regulation.
[19] A new generation of decentralised applications based on blockchain, enabling betting via smart contracts without the intervention of a central operator or regulatory control.
[20] Martin Purbrick (2023). The displacement of illegal betting and transnational organised crime. Asian Racing Federation Bulletin Council on Anti-Illegal Betting and Financial Crime, Quarterly Bulletin, Feb. (2023) (available here).
[21] MONEYVAL, The Use of Online Gambling for Money Laundering and the Financing of Terrorism Purposes, Council of Europe, Typologies Research Report, April 2013.
[22] Precrimbet. (2017). Preventing criminal risks linked to the sports betting market (available here).

AML/CFT oversight (Organised Crime in Australia, 2017). These operators often offer high betting limits, especially to VIPs, without applying strict identity verification checks.

Money launderers also use financial mules or intermediaries to conceal the origin and ownership of funds. The use of prepaid cards, vouchers[23], e-wallets, or insufficiently monitored payment platforms further complicates traceability (Moneyval, 2013).

A recent case uncovered the use of payment service providers such as Neteller, Skrill, and Western Union in a cross-border laundering operation where funds moved using false identity documents.

Crypto-currencies such as Monero or Zcash offer high degrees of anonymity by design[24]. Europol (2020)[25] notes that such tools are used to fund betting accounts involved in sports manipulation. Virtual Asset Service Providers (VASPs) are often difficult to monitor, particularly in cross-border flows (Moneyval, 2023). In response, regulators like the UK Gambling Commission have raised the risk level associated with crypto-currencies in their AML/CFT assessments.

While blockchain allows for theoretical traceability, launderers often use crypto exchanges, privacy-focused altcoins[26], or swap services[27] as well as mixing and tumbling services[28], making the origin of funds difficult to identify (Europol, 2021).

Sports betting and crypto-currencies share several characteristics: rapid growth since 2020, widespread use of digital channels, and user profiles than often overlap in online environments. Their speculative and volatile nature increases their appeal but also their vulnerability to misuse (Topps, 2023) [29].

Although crypto-currencies remain marginal in the legal payment processing ecosystem, they are widely used in illegal betting, particularly on the Darknet, where anonymity and circumvention of controls are standard practice (Betmonitalert, 2017).

Illegal operators on the Darknet overwhelmingly accept crypto-currencies. In 2023, one quarter of illegal betting sites used virtual assets, with a strong prevalence of the stablecoin Tether (USDT)[30] (ARF Council, 2024)[31]. These networks operate outside of traditional verification systems and enable large-scale, quasi-anonymous transfers.

3. Regulatory loopholes and uncooperative jurisdictions exploited by certain operators

The very structure of the betting market constitutes a major vulnerability. The coexistence of online and cash-based betting creates pathways that facilitate the concealment of illicit origin of funds. By combining these two channels, criminals can integrate cash from illegal activities into digital circuits, where traceability becomes more difficult. Several investigations have revealed networks simultaneously operating physical betting shops and online platforms controlled by the same criminal groups (Precrimbet, 2017[32]).

Many operators are based in jurisdictions, where AML/CFT requirements are weak and regulatory oversight is limited.

Some licensing arrangements, such as “white-label” models, require clarification, but responsibility for AML/CFT compliance remains legally vested in the licence holder under the UK Gambling Commission’s rules[33].

According to the Australian Criminal Intelligence Commission (2017), bookmakers often favour jurisdictions with limited regulation and poor cooperation with foreign authorities. The lack of harmonised regulation, combined with the transnational nature of online betting, makes this sector a particularly effective channel for laundering and financing criminal activities (ARF Council, 2023). Law enforcement representatives also report a lack of cooperation from certain offshore territories, which frequently ignore legal assistance requests.

---

[23] Voucher: prepaid voucher or code, often purchased in cash, used to credit an online account without using a bank account or a personal card.
[24] Privacy coins: so-called "confidential" crypto-currencies designed to guarantee total or enhanced anonymity of transactions. They use technologies such as address masking or amount encryption, which makes them particularly attractive for illicit uses, such as money laundering.
[25] Europol (2021), The involvement of organised crime groups in sports corruption (available here).
[26] Altcoin: generic term for any crypto-currency other than Bitcoin. Some altcoins, known as "privacy coins", incorporate enhanced privacy features that make it more difficult to trace transactions.
[27] Swap service: a platform for rapidly exchanging one crypto-currency for another, without going through a centralised exchange or creating an account. These services, which are often unregulated, are used to fragment and obscure financial flows for money-laundering operations.
[28] It is important to distinguish between (i) anonymous-by-design virtual assets (such as certain privacy coins) and (ii) anonymity-enhancing tools (such as mixers, tumblers or decentralised swap protocols), as the two categories pose different challenges for regulators and require different mitigation measures in FATF guidance.
[29] Topps, A. (2023), Place your bets: The legal integration of sports betting with crypto-currencies, *UNH Sports Law Review*, *2*(1), 5 (available here).
[30] Tether (USDT): stablecoin, i.e. a crypto-currency whose value is indexed to a fiat currency (in this case the US dollar). It is widely used in crypto transactions because of its relative stability, including on unregulated gambling and betting platforms that operate illegally.
[31] ARF Council (2024), How illegal betting and related money laundering flourished despite the "crypto-currency winter" (available here).
[32] Precrimbet. (2017). Preventing criminal risks linked to the sports betting market (available here).
[33] The UK's 'white-label' system illustrates the loopholes that some regulations can create. It allows holders of licences issued by the UK Gambling Commission to 'lease' them to third-party operators, sometimes located abroad, without these operators being subject to sufficient controls, particularly in terms of the fight against money laundering.

Setting up a betting site for the purpose of laundering money is relatively straightforward in jurisdictions where licensing requirements, CDD (Customer Due Diligence), and AML/CFT controls are minimal or absent. However, third-party operators can also exploit weak controls to conceal illicit financial flows. The presence in offshore jurisdictions makes investigations complex due to opaque structures: shell companies, fragmented bank accounts, foreign servers, and frequent relocation from one jurisdiction to another (Purbrick, 2023[34]).

More broadly, betting sites can be designed specifically for money laundering or used as intermediaries by external launderers. Their high operational flexibility, combined with a lack of transparency regarding beneficial ownership and the ease of bypassing national regulations (forum shopping), makes them attractive to criminal groups. This development illustrates the ability of organised crime to incorporate legal structures into its operations and to continuously adapt its methods to evolving regulatory environments (Europol, 2021).

TYPOLOGIES AND RISK ASSESSMENT

1. Physical betting remains a target for money launderers

Retail betting markets with physical distribution networks are often seen as less exposed to the most sophisticated forms of laundering than casinos or online platforms. However, cash-intensive activity, anonymity in certain transactions and the multiplicity of outlets continue to create vulnerabilities.

The use of cash, the anonymity of transactions, and the possibility of placing multiple low-value bets across different outlets allow for the introduction of criminal proceeds[35].

These risks are particularly relevant in jurisdictions where oversight of outlets is limited or where customer due diligence is inconsistently applied.

Practices such as contactless payments or the use of personal devices (BYOD – Bring Your Own Device)[36] further complicate the detection of illicit flows by fragmenting transactions.

A commonly used technique is smurfing, which involves breaking down stakes or deposits into small, repeated transactions to avoid reporting thresholds or automatic alerts. These operations can be spread across several venues or carried out simultaneously by different individuals, making the flows harder to trace.

The takeover or influence of physical betting outlets by laundering networks may occur in certain jurisdictions, depending on the jurisdiction. Where licensing, inspections and ownership controls are weak, such infiltration enables criminals to operate discreetly and bypass internal due diligence requirements. These features make physical betting markets a preferred channel for discreet yet effective forms of money laundering.

Main typologies:

- **Typology 1 - Laundering criminal funds by buying winning tickets from accomplices**

The launderer sets up a network of compliant bettors who place wagers using clean money. He then buys back their winning tickets using illicit cash and redeems them under his own name. To withdraw the funds discreetly, he may use anonymous services such as Hal Cash[37], which allow cash withdrawals without a traceable bank account.

- **Type 2 - Using stolen bank cards to place bets**

The offender withdraws cash using a stolen card, places a bet, and then then collects the winnings into their own bank account to justify the origin of the funds.

- **Type 3 - Purchasing anonymous winning slips**

---

[34] Martin Purbrick (2023). The displacement of illegal betting and transnational organised crime. Asian Racing Federation Bulletin Council on Anti-Illegal Betting and Financial Crime, Quarterly Bulletin, Feb. (2023) (available here).

[35] Introduction of cash: first stage in money laundering, consisting of injecting cash from illegal activities into the economic or legal financial circuit. In the case of sports betting, this may involve the purchase of tickets or credits or the deposit of cash at a point of sale, with the aim of transforming criminal funds into apparently legitimate winnings.

[36] BYOD (Bring Your Own Device): the practice of allowing customers to place bets at a physical point of sale using their own mobile device, without creating an account or identifying themselves, which makes it difficult to track transactions.

[37] Halcash (How it works): A money transfer service that allows funds to be sent to a mobile phone number, which the recipient can withdraw in cash from an ATM, without the need for a bank account or formal identification. This system can be misused for money laundering purposes by facilitating anonymous withdrawals.

The launderer approaches a winning player (often with the complicity of the retail outlet operator), buys their ticket for cash with a premium, and then claims the winnings as if they were their own. The risk assessment conducted by the GB Gambling Commission (see Annex 1) indicates that land-based markets present a high overall level of risk, notably due to insufficient preventive measures (particularly regarding Customer Due Diligence), vulnerabilities linked to the use of false documents, the anonymity of betting transactions (exacerbated by the predominant use of cash) and the loosely regulated use of multiple payment methods.

Overall, these typologies illustrate that retail betting continues to present clear money-laundering vulnerabilities, particularly due to cash-based transactions, opportunities for anonymity, and the dispersion of activity across multiple outlets. National risk assessments – including that of the UK Gambling Commission – classify land-based betting as high-risk for these reasons.

2. Increased risks on online betting platforms

The absence of in-person interaction has long been recognised as a factor that complicates customer identity verification in online betting (Customer Due Diligence). Earlier assessments, including Moneyval (2013), highlighted this risk, and while technological and regulatory frameworks have evolved in recent years, these vulnerabilities remain relevant in certain environments.

In some jurisdictions, weaknesses such as the absence of closed-loop payment controls, insufficient account verification, or the possibility of using multiple or fictitious accounts increase exposure to misuse.

The technical complexity of these platforms can also enable criminal groups to take direct control and integrate illegal flows.

Recent cases in Australia (Tabcorp, 2017; Star Entertainment, 2022) and in the UK (William Hill, Coral, Ladbrokes, Star Sports) have shown that even licensed operators may have serious weaknesses in their detection mechanisms[38]. These examples demonstrate that weaknesses in customer due diligence and monitoring can occur even where regulatory frameworks are in place. These shortcomings have led to reinforced anti-money laundering measures[39]. Both jurisdictions subsequently reinforced AML/CFT obligations, illustrating how oversight and enforcement play a central role in risk mitigation.

[38] ABCNews (2022), Money laundering watchdog investigates online gambling giants Sportsbet and Bet365 (available here); Racing Post (2023); Star Sports fined £594,000 for anti-money laundering and social responsibility failings (available here).
[39] Casino Guardian. (2023), AUSTRAC orders online sports betting companies to stop accepting bets from unverified customers (available here).

Main typologies:

- **Typology 1 - Depositing illicit funds to withdraw legitimate winnings**

The launderer opens an account on an online betting platform and deposits criminal proceeds, often using anonymous or weekly verified payment methods. Bets are placed on low-risk outcomes (such as favourites), allowing most of the funds to be recovered as winnings. These winnings, appearing to be legitimate, are then transferred to a personal bank account, giving the appearance of legitimate income. The scheme is often repeated across multiple accounts or jurisdictions to further obscure the origin of the funds.

This “minimal play” method is well-documented. Its feasibility is highest in jurisdictions with limited CDD (Customer Due Diligence)/EDD (Enhanced Due Diligence) obligations or permissive verification practices.

- **Typology 2 - Creating a betting platform to channel illicit funds**

A criminal network establishes its own sports betting site, typically based in jurisdiction with limited AML/CFT supervision, with weaknesses in anti-money laundering and counter-terrorist financing (AML/CFT) measures. It then recruits accomplices or “mules” to deposit money into betting accounts and deliberately lose bets on unlikely outcomes. These losses are transferred to bank accounts controlled by the criminal organisation, enabling it to recover the funds with a veneer of legality.

The GB Gambling Commission’s risk assessment (see Appendix 2) confirms that online betting platforms are exposed to high levels of money laundering risk. Key vulnerabilities include the use of open-loop payment channels, weak CDD (Customer Due Diligence) procedures, exposure through VIP accounts, multi-accounting, and a wide range of digital payment methods—some of which allow a high degree of anonymity.

Even when controls exist and are properly applied, the risk level remains high. The speed of transactions, the diversity of betting products, and the ease of moving funds across platforms continue to create opportunities for concealment and misuse.

3. Crypto-assets and money laundering in online betting

Crypto-currencies are increasingly used as tools for money laundering, particularly within the online gambling industry. Their relative anonymity, combined with the technical complexity of tracing transactions, makes investigations more challenging for authorities.

However, regulatory developments in recent years, particularly within the European Union, have significantly reshaped this risk environment. Regulation (EU) 2023/1113 on funds transfer (“travel rule”) now requires crypto-asset service providers to collect and transmit originator and beneficiary information for all transfers, while the new Anti-Money Laundering Regulation (EU) 2024/1624 will prohibit anonymous crypto-asset wallets.

Money launderers typically rely on two main categories of services to manipulate crypto-assets[40] before or after using betting platforms:

- **Intermediary services to obscure transaction trails**

These include unhosted wallets[41] such as Metamask or Trust Wallet, which allow users to hold funds to be stored without relying on a "trusted third party", and notably without any identity verification. Mixers[42], such as Tornado Cash or Sinbad, are used to break transaction links, making funds untraceable. Darknet markets, such as Hydra (shut down in 2022), also facilitate the exchange of crypto-assets for illicit goods or services. These services are sometimes used in combination to convert, move, or fragment funds before injecting them into betting accounts.

- **Gateways to fiat currency for converting cryptos into euros, dollars and other traditional currencies**

This conversion is often carried out via centralised exchanges such as Binance, Kraken or Bitfinex; peer-to-peer (P2P) platforms like Paxful or LocalBitcoins (shut down in 2023); or decentralised exchanges (DEXs) [43] such as Uniswap or PancakeSwap. Once

[40] Crypto-asset: generic term for any digital asset based on a distributed ledger technology (such as blockchain). It includes crypto-currencies (e.g. Bitcoin), stablecoins (e.g. Tether), utility tokens, NFTs and governance tokens. This term is preferred in European and international regulatory texts.
[41] Non-hosted wallet: crypto application managed by the user themselves (e.g. Trust Wallet, Metamask), without going through a centralised platform. It does not require an account or identity verification.
[42] Mixer: service designed to disguise the origin of funds by mixing the crypto-assets of several users. Examples: Tornado Cash (Ethereum), Sinbad (Bitcoin), ChipMixer (closed).
[43] DEX (decentralised exchange): cryptoasset exchange platform operating without a central authority. It allows transactions to be carried out directly between users, without KYC checks. Examples: Uniswap, PancakeSwap.

converted, the funds can be transferred to bank accounts or withdrawn in cash, escaping blockchain traceability. These gateways are sometimes used to inject funds into betting platforms.

An emerging trend involves the use of clandestine services, far more discreet than standard mixers. These are accessible only through private messaging apps (such as Telegram) or the Tor browser and are typically promoted on darknet forums. Such channels allow launderers to fund online betting accounts with pre-anonymised assets, avoiding automated detection.

A UNODC (2024)[44] report highlights that illegal betting platforms, especially in Southeast Asia, increasingly rely on crypto-currencies like Tether (USDT) on the TRON blockchain[45], which has become a central laundering tool. These platforms facilitate the conversion and movement of large volumes of illicit funds, often linked to drug trafficking, fraud, or cybercrime.

Main typologies:

- **Typology 1 - Using junkets[46] to discreetly move funds between jurisdictions**

A player entrusts money to a gambling intermediary (known as a junket) in one country. Rather than transferring the funds abroad, the amount is credited to the junket's internal system. The player can then access this credit in another jurisdiction, for example in a casino or via a connected betting platform. The process relies on internal balancing of credits and losses, without any identifiable international banking transaction

Some junkets even attract deposits by offering high interest rates, effectively operating as unregulated parallel banks.

- **Typology 2 - Using a network of multiple accounts to fragment and transit illicit funds**

Criminal groups recruit individuals to transfer money on their behalf using their personal bank accounts or online betting accounts. These individuals—sometimes referred to as "mobile ants"—repeatedly move small sums of money between different accounts or platforms. They may not always be aware of the illegal origin of the funds but are paid a commission for each transaction.

This system is used to conceal the identity of the ultimate beneficial owners and to make the tracing of money flows more difficult.. It is often linked to illegal gambling, phone-based scams (e.g. fake bank advisers), or organised crime such as drug trafficking or human smuggling.

Overall, crypto-assets continue to present significant ML/TF risks, particularly in opaque environments. In regulated jurisdictions, recent EU reforms reduce anonymity-driven vulnerabilities, but criminal groups still exploit gaps in supervision, cross-border activity, and non-compliant service providers.

LIMITATIONS OF CURRENT ANTI-MONEY LAUNDERING MEASURES IN SPORTS BETTING

1. Regulatory frameworks still insufficient

Despite growing awareness of the risks, current anti-money laundering (AML) frameworks remain inadequate. While most EU Member States require the betting sector to comply with AML directives, the European Commission's assessment of the implementation of the 4th AML Directive revealed significant shortcomings.

In several countries, there are no specific requirements for fit and proper checks[47] or competency assessments for beneficial owners[48] during the licensing application process.

The United Kingdom, for its part, has introduced specific obligations for both online and land-based betting operators through UK Gambling Commission guidelines[49]. However, the effectiveness of this framework largely depends on how well it is implemented by operators, and certain practices, such as the white label system, have been criticised for their lack of oversight.

---

[44] UNODC (January 2024), Casinos, Money Laundering, Underground Banking and Transnational Organised Crime in East and Southeast Asia: A Hidden and Growing Threat (available here).
[45] TRON blockchain: decentralised blockchain network founded in 2017, designed for fast, low-cost transactions. It is widely used for the transfer of stablecoins, notably Tether (USDT), due to its low transaction costs. Its popularity in illicit circles is due to the relative anonymity it offers, combined with high accessibility.
[46] A "junket" is an agreement between a casino and an operator to facilitate the entry and play of high-net-worth players, often as part of VIP programmes. Through their links with casinos, junket operators can offer benefits and incentives to their members or other high-income customers.
[47] Fit and proper checks: administrative or judicial procedures designed to ensure that a natural or legal person does not present risks due to past criminal convictions, links with organised crime or a compromising background. In the gaming sector, they are used to prevent individuals linked to illegal activities from taking control of licensed operators.
[48] Competence of beneficial owners: requirement aimed at ensuring that the persons who effectively own or control a company have the knowledge, experience and integrity necessary to exercise their responsibilities. In the gaming sector, this helps to limit the risks of mismanagement or criminal infiltration.
[49] GB Gambling Commission (2023), Money laundering prevention and combating the financing of terrorism, Gambling Commission guidance for remote and non-remote casinos, Fifth edition, Revision 3, (available here).

Globally, the sector suffers from a lack of harmonised anti-money laundering (AML) standards. The absence of checks on beneficial owners, weak compliance requirements, and insufficient oversight of operators, particularly in certain offshore jurisdictions, make it difficult to detect, investigate, and prosecute money laundering practices through betting.

This regulatory fragmentation creates opportunities for regulatory arbitrage, whereby operators choose jurisdictions offering minimal oversight.

2. The ambiguous role of certain betting operators

Betting operators are on the front line in the prevention of money laundering. They are legally required to adopt a risk-based approach, verify customer identities, implement systems to manage and mitigate these risks, allocate appropriate human and material resources, and report suspicious transactions.

However, the level of engagement among operators varies considerably. While some licensed operators apply AML/CFT measures, others, particularly those operating on the Darknet or under offshore licences, apply little to no control. In some cases, money launderers are even seen as profitable clients, placing large bets and accepting some losses. In such environments, high-spending customers engaged in suspicious activity may be subject to weaker verification processes or limited monitoring, creating situations where commercial incentives can conflict with AML obligations.

3. Weaknesses in the implementation of Customer Due Dilligence (CDD) measures

The effectiveness of CDD (Know Your Customer) systems varies considerably between operators. In some cases, identification procedures are either insufficient or carried out too late, for example at withdrawal rather than at the time of deposit, which reduces their preventive effect.

The GB Gambling Commission's risk assessment highlights that these controls are not consistently applied. This is partly due to the use of forged documents[50], false identities, or "smurfing" techniques (splitting deposits into smaller amounts to avoid detection thresholds).

Moreover, operators typically have only a partial view of a customer's betting activity and are unable to access information about behaviour across other platforms. Finally, the frequent lack of closed-loop payment systems, where the withdrawal method is not verified against the original deposit method, represents a weakness in the traceability of financial flows.

4. Reporting of suspicious transactions remains too rare

In accordance with European anti-money laundering legislation, all regulated providers of gambling services are required to report any transaction suspected of involving money laundering. This Suspicious Activity Report (SAR) must be submitted to the Financial Intelligence Unit (FIU) through the designated officer, known as the MLRO (Money Laundering Reporting Officer).

While this obligation is clearly established at the European level, its implementation remains uneven in practice. Some operators delay submitting reports or fail to do so altogether, which weakens the effectiveness of the prevention framework. This shortfall may stem from a lack of training, limited awareness of risk indicators, or the absence of feedback from the competent authorities.

5. Challenges posed by virtual assets

The FATF (Financial Action Task Force)[51] requires virtual asset service providers (such as crypto-currency platforms) to be registered, licensed and supervised to prevent money laundering and terrorist financing activities.

The 2023 Moneyval report[52] highlights that some countries have introduced targeted controls to limit the misuse of crypto-assets in the gambling sector. These measures include, for example:

- Restricting the types of crypto-assets allowed, so that only certain tokens can be used for deposits or withdrawals;
- Requiring consistency between deposits and withdrawals, to avoid complex transfers between different digital currencies;
- Setting transaction limits to reduce the amount of funds that can be laundered at once;

[50] The GB Gambling Commission adopts the definition of money laundering from the Proceeds of Crime Act 2002, which states that an operator commits an offence if he accepts funds derived from crime. This includes both transactions designed to conceal the origin of funds and the simple use of criminal proceeds for legal purchases, including gambling (available here).
[51] FATF (2021). Virtual assets and virtual asset service providers (available here).
[52] Moneyval (2023b), Money laundering and terrorist financing risks in the world of virtual assets (available here).

- Using blockchain monitoring tools to detect high-risk signals such as the use of mixers (which obfuscate the origin of funds), private chains[53], or complex transfer routes.

However, the very nature of crypto-currencies — including relative anonymity and decentralisation — often conflicts with gambling regulations, which require clear user identification.

This creates two major challenges for the authorities:

- Ensuring effective oversight of legal betting activities, despite the large number of operators and transactions;
- Tackling illegal betting, where offshore or unlicensed operators attract users with better odds, fewer restrictions, and above all, the anonymity provided by crypto-currencies.

6. Too few investigations and prosecutions

According to Moneyval's 2022 annual report (2023a)[54], convictions for money laundering remain infrequent. In addition, parallel financial investigations are not yet conducted systematically in many jurisdictions.

This is also the case in the betting sector, where the number of cases progressing to prosecution remains limited.

Observations reported across some jurisdictions indicate a shortage of human resources and specialised expertise within investigative teams. Tackling money laundering through online betting requires advanced analytical tools and targeted training, which are not yet available everywhere.

Two key factors hinder detection:

- The absence of identifiable victims, which makes cases less visible and less likely to be prioritised;
- The cross-border nature of many operations, which complicates international cooperation.

The lack of structured collaboration between supervisory bodies and law enforcement across jurisdictions further weakens the effectiveness of responses (European Commission, 2024)[55]. This fragmentation limits the overall capacity to identify, trace and dismantle criminal networks involved in laundering through sports betting.

CONCLUSION

1. Strengthening national measures for prevention and detection

- Ensure the effective implementation of the EU anti-money laundering directive within the betting sector (see measures in Annex 3). National authorities should in particular require operators to:
  - ✓ Develop a coherent and rational business risk assessment;
  - ✓ Verify customers' identities using a reliable, independent source, reducing the anonymity made possible by certain payment methods (such as crypto-assets, prepaid cards, Bitcard Secure BTC, etc.);
  - ✓ Record customer data for any transaction or winnings over €2,000;
  - ✓ Apply enhanced due diligence procedures to customers considered high risk;
  - ✓ Pay out winnings only to the original deposit account, to avoid layering and support investigations;
  - ✓ Appoint a dedicated officer for money laundering-related matters;
  - ✓ Increase transparency regarding shareholders and members of the board of directors of licensed operators.
- Adapt the legal betting offer based on identified risks (e.g. types of bets, return-to-player rates), using a risk-based assessment approach.

---

[53] Private blockchains: blockchains to which access is restricted to a group of authorised users. Unlike public blockchains such as Bitcoin or Ethereum, they do not allow everyone to view or validate transactions, which limits transparency and complicates the traceability of financial flows.
[54] Moneyval (2023a); Annual Report 2022 (available here).
[55] Council of the European Union (2024), Commission Staff Working Document accompanying the Report from the Commission to the European Parliament and the Council on the implementation of Directive (EU) 2015/849 (available here).

- Establish clear criteria for reporting suspicious activity, in collaboration with relevant authorities (FIUs, police, regulators, and operators)[56].

  These criteria could include :

  - ✓ Use of multiple betting accounts or payment methods by a single individual;
  - ✓ Suspicious geographical origin of a payment card;
  - ✓ Unusual frequency of deposits, withdrawals, or bets;
  - ✓ High, repeated, or multiplied winnings by the same customer, particularly on low-odds bets.

- Support operators in configuring their IT systems to automatically detect suspicious behaviours.

- Grant regulatory authorities full access to online betting data to better identify high-risk activities.

- Regularly monitor operators' compliance with anti-money laundering regulatory requirements.

- Promote cooperation between gambling regulators and the banking sector, including structured information sharing in compliance with the GDPR[57]. Banks hold valuable data for assessing customer risk profiles.

- Involve financial intermediaries in the implementation of anti-money laundering measures within the betting sector.

2. The importance of international cooperation to strengthen existing frameworks

- Promote cooperation between Financial Intelligence Units (FIUs) [58] on issues related to betting and gambling, notably through the creation of a dedicated working group.

- Strengthen collaboration and expertise among national betting regulators on money laundering, through the exchange of best practices and targeted training.

- Include the prevention, detection, investigation, and sanctioning of betting-related money laundering in the work of the Network of Prosecutors and Judges for Sport (MARS), under the authority of EPAS (Council of Europe).

- Promote the implementation of asset recovery measures in connection with the manipulation of sports competitions.

- Launch an in-depth study on money laundering through sports betting, structured around three key components:

  - ✓ A risk assessment following the three-step FATF (2013) model: identification (threats and vulnerabilities), analysis (nature, sources, frequency, consequences), and evaluation (priorities and strategies);
  - ✓ A typology of money laundering schemes through betting, including concrete examples, based on consultations with the MARS network and other relevant stakeholders;
  - ✓ An analysis of the links between money laundering through betting, laundering via sports structures, and the manipulation of competitions.

- Based on this work, consider the adoption by the Council of Europe of a specific recommendation on the prevention, detection and sanctioning of money laundering in the betting sector.

[56] Council of the European Union (2024), Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing (available here).
[57] GDPR: General Data Protection Regulation (EU 2016/679), which came into force in 2018. It provides a framework for the processing of personal data within the European Union and guarantees people's privacy rights, including in sectors such as gambling.
[58] FIU (Financial Intelligence Unit): national body responsible for receiving, analysing and forwarding suspicious activity reports on money laundering or terrorist financing to the competent authorities. Each country has its own FIU, often attached to a public authority.

APPENDIX 1: RISK ASSESSMENT FOR PHYSICAL MARKETS

The GB Gambling Commission's risk assessment[59] focuses on the UK market but provides a useful insight into how these risks may manifest themselves in other contexts.

Vulnerability	Risk	Likelihood of event occurring	Impact of event occurring	Overall risk
Operator control	Operators failing to comply with prevention of AML legislation/rules	High	High	High
Operator control	Lack of effective customer interaction resulting in failure to prevent/detect ML	Medium	High	High
Operator control	Inadequate/lack of KYC checks resulting in criminals laundering criminal proceeds	High	High	High
Operator control	Third party business relationships and business investors	Medium	High	High
Licensing and integrity	Betting operations being acquired by organised criminals to launder criminally derived funds	Low	High	Medium
Licensing and integrity	Betting employees acting in collusion with organised criminals to launder criminal funds	Medium	High	High
Customer	Unverified customers laundering proceeds of crime through betting	High	High	High
Customer	False or stolen identification used to bypass controls to launder criminally derived funds	Medium	High	High
Customer	Accessibility to multiple premises/operators	High	High	High
Customer	Organised criminal gangs	Low	High	Medium
Means of payments	Cash transactions	High	High	High
Means of payments	Cashless transactions	Medium	High	High
Means of payments	Dyed notes	Low	Medium	Low
Means of payments	Lack of “closed loop” system	Medium	High	High
Means of payments	Multiple methods of payments	Medium	High	High
Product	Self-service betting terminals and Ticket-in-Ticket Out machines used to launder criminal funds	Medium	High	High
Product	Bring your own device (BYOD)	Low	Medium	Low

[59] Adapted from the GB Gambling Commission Risk-Assessment (2023) (available here).

APPENDIX 2: RISK ASSESSMENT FOR ONLINE PLATFORMS

The GB Gambling Commission's risk assessment[60] focuses on the UK market but provides a useful insight into how these risks may manifest themselves in other contexts.

Vulnerability	Risk	Likelihood of event occurring	Impact of event occurring	Overall risk
Operator control	Operators failing to comply with prevention of AML legislation/rules	High	High	High
Operator control	Operators staking and winning directly and indirectly on their own products	Low	Medium	Low
Operator control	Lack of competency of key personnel and licence holders which can then be exploited by criminals seeking to launder the proceeds of crime	Medium	High	High
Operator control	Inadequate/lack of KYC checks resulting in criminals laundering criminal proceeds	High	High	High
Operator control	"High value" customer schemes (VIP Accounts)	Medium	High	High
Operator control	High monetary threshold	High	High	High
Operator control	KYC completed at the point of withdrawal	Medium	High	High
Operator control	Third party business relationships and business investors	Medium	High	High
Licensing and integrity	Gambling operations run or acquired by organised criminals to launder criminally derived funds	Low	High	Medium
Customer	False or stolen identification used to bypass controls to launder criminally derived funds	High	High	High
Customer	Accessibility to multiple remote accounts	Medium	High	High
Customer	Customers from high risk or non-cooperative jurisdictions using remote facilities to launder criminally derived funds	Medium	High	High
Customer	"Smurfing"	High	High	High
Customer	"Mule" betting accounts	High	High	High
Customer	Politically exposed Persons (PEPs)	Medium	High	High
Customer	Business customers (betting exchange)	Medium	High	High
Customer	Use of third parties or agents to obscure the source or ownership of money bet by customers and their identities	High	High	High
Means of payments	E-wallets	High	Medium	Medium
Means of payments	Crypto-asset transactions	Medium	High	High
Means of payment	Pre-paid cards	High	High	High
Means of payment	Lack of "closed loop" system	Medium	High	High
Means of payment	Multiple methods of payments	High	High	High
Product	Peer to peer betting	High	High	High
Product	Unregulated betting events	Medium	High	High

[60] GB Gambling Commission. (2023), Money laundering and terrorist financing risks in the UK gambling industry) (available here).

APPENDIX 3: MEASURES RELATING TO THE 6TH EUROPEAN ANTI-MONEY LAUNDERING DIRECTIVE

- **Risk-based approach:** Entities must assess the risks of money laundering and terrorist financing, and tailor their management and prevention measures according to the level of identified risk.
- **Know Your Customer (KYC): I**nitial process through which an operator verifies a customer's identity and basic information before engaging in a business relationship. KYC focuses primarily on confirming identity documents and ensuring the customer is who they claim to be.
- **Customer Due Diligence (CDD):** Broader, risk-based process that includes KYC identification but also requires assessing the customer's risk profile, understanding the purpose and nature of the relationship, reviewing the source of funds when relevant, and conducting ongoing monitoring of transactions to detect unusual or suspicious behaviour.
- **Enhanced Due Diligence (EDD):** For high-risk customers or transactions, more thorough checks are required, notably with regard to their environment and apparent financial standing.
- **Politically Exposed Persons (PEPs):** Additional measures apply to business relationships involving individuals holding public office or those closely associated with them.
- **Transparency of beneficial ownership**: Entities must identify and verify the beneficial owners (natural persons who control or benefit from a company, trust, etc.).
- **Reporting of suspicious activity**: Any activity or transaction deemed suspicious must be promptly reported to the competent authorities.
- **Record-keeping**: Entities are required to retain relevant documents and information throughout the business relationship and beyond, for a defined period, to facilitate audits and investigations.
- **National supervisory authorities**: Each Member State must have authorities responsible for enforcing anti-money laundering legislation, in coordination with other EU countries.
- **Staff training**: Entities must train their employees to detect warning signs and respond appropriately to suspicious behaviour.