FATF

Red Flag Risk Indicators

Risks of Gaming and Gambling

September 2026

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2026), *Risks of Gaming and Gambling, Paris, France*,
https://www.fatf-gafi.org/en/publications/Methodsandtrends/risks-of-gaming-and-gambling.html

Photo credits cover photo ©Shutterstock

Key findings

1. The gaming and gambling industries have changed significantly over recent years and continue to evolve through the expansion of online, cross-border, multi-product and multi-payment platforms. Gaming and gambling establishments and platforms are now part of a broader interconnected value-transfer ecosystem with numerous actors, some of which fall outside national anti-money laundering/counter-terrorist financing (AML/CFT) regulatory frameworks. These factors, as well as the varying scope among jurisdictions in AML/CFT regulation of gambling or understanding of gaming risk-exposed activity, have led to developments in the money laundering (ML), terrorist financing (TF) and, to a somewhat lesser extent, proliferation financing (PF) risks associated with the sector. The FATF does not have a strict definition of "casinos", but in the context of the risk-based approach, it is up to jurisdictions to assess the risks and implement proportionate measures to mitigating the risks they identify.

Background

2. This work offers an updated analysis[1] of the ML/TF/PF risks posed by the casino sector as well as risks posed by the broader gambling sector and gaming sector. The FATF has examined the scope of gaming and gambling activity offered globally including online and brick-and-mortar casinos, sports and novelty betting, other non-casino gambling (including scratch cards, arcades, bingo, lotteries and slot machines outside of casinos) and online video/mobile gaming, and risks derived from illegal operators. The FATF has also examined the business models and delivery channels used in gaming and gambling, the interaction of gaming and gambling services with the financial system and the intersection of gaming and gambling activity with other platforms such as social media.

3. Questionnaire responses from 80 jurisdictions from across the FATF Global Network, written comments from 29 jurisdictions and targeted consultation with industry bodies, researchers and private sector stakeholders supported the development of this work, and numerous case studies provided by jurisdictions supported the findings.

4. In response to the findings, several recommendations and operational mitigation measures for jurisdictional and FATF consideration are suggested, and red-flag indicators of the misuse of the gaming and gambling sectors for ML/TF/PF are also shared.

Global gaming and gambling sector

5. The FATF's analysis considered the most common gaming and gambling verticals across jurisdictions, divided into casinos, sports and novelty betting, other non-casino gambling, and online video/mobile gaming. Overall, the findings indicate an increase in market size globally, a rise in the proliferation

[1] Financial Action Task Force (FATF) and Asia-Pacific Group on ML's (APG) previous work on casinos in 2009.

and the use of online platforms, and an overlap of services and payment mechanisms (e.g. cash, card, bank transfer, virtual assets, mobile money, third-party intermediaries and money or value transfer services).

6. However, the level and types of ML risks differed depending on the use or combination of payment methods and/or service offered and whether the gambling or gaming operator was land-based or online.

Money laundering, terrorist financing and proliferation financing risks identified in gaming and gambling

7. The project found that ML through gambling is an established risk across many jurisdictions. Generally, brick-and-mortar and online casinos and sports betting are considered to be particularly exposed to ML risks. Lotteries, scratch cards and certain other non-casino forms of gambling may be considered less exposed to ML risks by some jurisdictions.

8. While gaming and gambling platforms share a number of structural similarities (e.g. cross-border customer bases and flow of funds), based on currently available evidence, ML through gaming appears to take place on a smaller scale, or with less sophistication and frequency, than through gambling.

9. TF risks and typologies related to gambling remain limited and less frequently reported compared to the online gaming space which demonstrated more observable and documented TF related misuse influenced by social and technological factors. Although the vulnerability may exist, the risks of PF in the context of both gaming and gambling remain very limited.

10. Findings indicate that certain payment methods associated with gaming and gambling activity, such as cash, e-wallets, mobile money and virtual assets are vulnerable to a range of ML risks. The variety of payment methods accepted by online gaming and gambling operators increasingly allows rapid, anonymous, cross-border transactions, and the conversion of value into different forms.

11. Online gaming and gambling platforms are also increasingly interlinked with social media and other digital platforms which can increase ML/TF/PF risks. Social media can be used to communicate and co-ordinate illicit activity such as competition manipulation, advertise illegal or unlicensed gambling, recruitment of money mules, dissemination of terrorist propaganda and fundraising for TF.

12. The abuse of gambling operators for illicit finance is linked with other crimes such as corruption, cyber-enabled fraud, professional ML networks and organised crime.

13. Illegal and unlicensed offshore gambling is cited as a significant risk. The illegal gambling market rivals or even exceeds the legal market in some countries and continues to proliferate, attracting players through promotions and greater levels of confidentiality.

14. Although on the decline and subject to increasingly strict regulations, junkets are still considered to pose risks relating to the anonymity of players and obscured beneficial ownership of the junket operator.

Challenges in addressing illicit finance risks in gaming and gambling

15. The FATF has explored the regulatory landscape for combatting ML/TF/PF in gaming and gambling, finding that the scope of AML/CFT supervision and the distribution of oversight responsibilities, licensing regimes and market entry controls differed across jurisdictions.

16. Challenges faced by supervisors, law enforcement authorities and operators/reporting entities in the sector include responding to regulatory framework differences across jurisdictions enabling regulatory arbitrage by gambling operators, limitations in information sharing between private and public sector, difficulties in international co-operation, and tackling illegal gambling activity and the speed of technological evolution.

How jurisdictions can better mitigate illicit finance risks from gaming and gambling

17. Some best practices shared by jurisdictions to address these challenges are set out below, noting that many of these practices relate to the gambling sector given the differing levels of understanding and reporting of risk outlined above.

Recommendations

18. A number of recommendations to jurisdictions to strengthen their response to the ML/TF/PF risks of gaming and gambling are suggested. These include:

- Improving risk awareness and understanding given the evolving and technologically integrated nature of the sector, and applying a risk-based approach in line with Recommendation 1 of the FATF Standards to mitigate the risks identified.
- Strengthening licensing and registration requirements to prevent criminals controlling gambling operators
- Raising awareness of risks to service providers and to the general public, particularly on illegal and unlicensed offshore gambling.
- Strengthening formal and informal international co-operation between agencies, especially in relation to online, illegal and cross-border gambling activities.
- Considering developing or strengthening public-private partnerships to enhance information sharing and enable quick responses to emerging and evolving risks.

Red-flag risk indicators

1. The indicators below were provided by countries through the project questionnaire and have been elaborated using open-source research and information from work by other international organisations. This is not an exhaustive list. A single risk indicator alone is not necessarily a clear indication of money laundering, terrorist financing or proliferation financing (ML/TF/PF) activity, but it can prompt further monitoring and examination as appropriate. The existence of several indicators in relation to a customer or transaction warrants further examination. Some indicators may also be indicators of problem gambling behaviours, rather than intentional attempts to engage in illicit conduct. In some cases, indicators and risks of both illicit activity and problem gambling may co-exist.
2. Operators and platforms are varied in nature and the risk indicators provided below may not be relevant to all operators and platforms. Most risk indicators that were shared are related to land-based and online casinos, and to a lesser extent betting. Risk indicators for video games were not common, but since they have commonalities with online casinos and betting platforms, some of the risk indicators provided are also applicable to them. The categories are divided into online and land-based where appropriate, as it was found that land-based operators have similar indicators, as do online platforms.

Customer behaviour and profile

Brick-and-mortar

- Attempts to influence or bribe venue staff to ignore their activity or bypass thorough customer due diligence (CDD) checks, including offering tips/other incentives.
- Frequently deals with only one staff member and avoids other staff.
- Uses third parties to place cash funds into cash redemption terminals, purchase gaming chips or place bets in an attempt to anonymise gambling.
- Requests winnings to be paid in cash up to the threshold amount and never returns to collect the balance.
- Purchases or attempts to purchase winning claim instruments (e.g. lottery ticket, betting slip, ticket-in-ticket-out (TITO) voucher, prize coupon) from another customer and then presents them as their own.
- Player attempts to present a casino value instrument (e.g. chip) from an unknown source.
- Behaving in an unusual way on the premises (e.g. acting suspiciously or out of character for a regular customer).
- Players appearing to act on behalf of a third party (e.g. taking instructions from mobile phones, or other customers on the premises).

Online

- Deliberate attempts at concealment of identity such as repeated virtual private network (VPN) use, multiple device use and discrepancies between the customer's claimed residence and their detected location.
- Customer tries to open multiple accounts under the same name or a fake name.
- Online betting account details do not match the account details of the payment method for deposits and withdrawals.
- Internet Protocol (IP) address and stated location do not match.
- IP address shows multiple players at the same address or using the same internet service provider.
- The customer is based in a country where gambling is illegal.
- Reluctance or refusal to appear on video call to verify identity.
- Attempts to re-open or re-register a previously suspicious / closed account (where operator has previously investigated and taken action against the account).
- Customer account has images, videos or symbols that promote or endorse terrorism or violent extremism.

Both

- Customer is reluctant or refuses to provide up-to-date identification documents or inconsistencies in personal information provided. Customer attempts to bypass other CDD measures.
- Frequent changes in account details (e.g. phone number, address, linked bank accounts or payment mechanisms).
- Bank details registered to the account do not match player details and/or there are inconsistencies in information (e.g. player address location does not match proof of address documents provided).
- Customer provides unclear or doctored documents which are difficult to authenticate.
- Customer has wealth or funds are inconsistent with their profile or that cannot be easily explained.
- Customer is reluctant to provide evidence of their source of wealth/source of funds.
- Source of wealth checks show that the customer earns money through the international trade of dual-use goods with sanctioned states (e.g. washing machines, cars or medical equipment).
- Customer's address is a post office box or business address, rather than a residential property.
- Customer is matched through screening against a national or international sanctions list.
- Customer is associated with a sanctioned state, group or individual.

- Open-source information indicates customer is a known terrorist or has links with terrorist organisations, has extremist ideologies, links to violent extremist social media accounts or is identified in adverse media.
- Customer onboarding documents, email addresses or usernames suggest the customer supports or has sympathy with a particular terrorist group or cause.
- Customer discloses that they are a member of a terrorist organisation.
- Customer is located in a higher risk jurisdiction.
- Customer enquires about moving funds to a high-risk jurisdiction.
- Customer is a foreign national (especially from a high-risk country) with no clear connection to the jurisdiction in which the gambling operator or activity is taking place.
- Customer is identified as a Politically Exposed Person (PEP).
- Customer enquires about whether the platform or operator reports to government authorities or about transaction limits. Customer shows unusual interest in internal controls and processes.
- Customers with no known or apparent relationship share funds.
- Customer is linked to criminal activity or their gambling activity is subject to law enforcement enquiries.
- Customer is active in multiple venues/platforms simultaneously with no apparent genuine gaming or gambling purpose.
- Customer says extreme or unusual things in the venue or platform, such as voicing intent to harm others.

Online accounts

- Unusual activity signalling ML such as frequent transfers, deposit of funds and distribution of payments to or from numerous individuals.
- Significant changes in how the account is used (e.g. amount of money added/withdrawn, amount of money wagered, use of multiple payment mechanisms).
- Frequent deposits to an account via methods where it is difficult to determine the source of funds.
- An inactive player account is suddenly funded with a large deposit inconsistent with the account's history.
- Account has a high rate of failed deposit attempts.
- Account profile is inconsistent with declared source of funds or source of wealth.
- Account has activity linked to unlicensed online operators or organised crime groups.
- Several accounts under different names are opened using the same IP address or device.

- Multiple accounts share the same physical address or contact details.
- Customer details (e.g. telephone number or postal code) do not correspond to the declared country of residence.
- Use of VPN to access the platform. IP address changes to different locations with each login.
- New IP address which is inconsistent with the account's previous IP history, which may be indicative of account take-over.

Betting patterns

- Spending patterns are inconsistent with the customer's profile including their known income and background (e.g. job profile or residence).
- Sudden changes in the customer's gaming/betting patterns (e.g. sudden increases in amounts staked or in frequency of betting activity).
- Co-ordinated or unusual betting activity, including hedged bets, betting on all outcomes and consistent losses to other player(s) in peer-to-peer (P2P) settings.
- Structuring of deposits into smaller amounts to fall under reporting thresholds.
- Use of short-odds bets and other low-risk mechanisms to justify withdrawals.
- Withdrawals from the account are not commensurate with the conduct of the account, (e.g. the player makes numerous large withdrawals without engaging in significant gambling activity).
- Customers appear to play frequently together, with one always winning and the other always losing. Suspected collusion in gambling activities, including gambling on both likely outcomes of certain games (e.g. one person betting on red and the other on black in roulette).
- Customer tries to circumvent note insertion limits by playing multiple machines simultaneously.
- Customer frequently plays games with low returns but with lower risks and a higher chance of winning.
- Customer repeatedly collects winnings just below a customer identification threshold.
- Bets appear to be placed automatically, or robotically.
- Placing of bets by customers who are related to or identified as being involved in the sport on which they are placing bets (e.g. as a game, match or competition official including referee/umpire, staff member of an organisation or club involved in the sport or body that oversees the sport, player or competitor or coach).
- Betting on an outcome which is later determined to be the result of competition manipulation
- Non-genuine play patterns – wagers are low while large sums are deposited and withdrawn.

- Large bets on low probability outcomes or immediate cash outs.
- P2P anomalies (e.g. chip dumping).
- Consistently betting on all possible outcomes (e.g. on red and black in roulette, on both teams to win a match).
- Highly improbable, sustained winning streak indicative of collusion, insider information or corruption.
- Player places unusually large or co-ordinated bets (in timing, market selection or amount) on specific events that have been flagged by integrity bodies or monitoring services for potential match/result fixing.

Payment methods/transactions

- Heavy use of cash (especially higher-denomination notes) in physical venues.
- Cash loading of digital accounts (e.g. through a betting shop which is also linked to a remote account from the same operator).
- Numerous daily cash deposits within short timeframes (even seconds apart).
- Preferential use of higher-risk payment methods such as virtual assets (VA), prepaid cards, vouchers and e-wallets.
- Multiple payment methods in different names linked to a player's account.
- Unusual use of payment methods (e.g. using multiple credit cards, combining fiat and VA).
- Withdrawal of funds internationally, in foreign currency or VA, which differs from players stated geographic location.
- Attempts to withdraw funds to an account different to the source of the funds.
- Deposits followed by withdrawals with minimal or no play in between.
- Banking anomalies including mule accounts, high-velocity transfers and transactions connected with higher-risk jurisdictions.
- Movement of funds to or from sanctioned or high-risk jurisdictions.
- Multiple individuals aggregate or pool deposits in a platform or operator's bank account, followed by a single transfer to a single customer's account.
- Depositing funds from numerous international bank accounts.
- Deposits made by third parties that are not clearly related to the account holder.
- Multiple small deposits from different sources are consolidated into larger withdrawals.
- Rapid withdrawals to different accounts or beneficiaries.
- Frequent attempts to bypass responsible gambling limits imposed by the venue, platform or jurisdiction (e.g. time limits, deposit caps, spending caps, self-exclusion).
- Deposits frequently reach daily limits.

- Frequent failed payment attempts.
- E-wallets used are held by foreign payment institutions.
- VA wallets are used on unlicensed platforms.
- Use of unlicensed or unregistered remittance providers to make deposits into play account of platform bank account.
- Player co-mingle casino value instruments with cash.
- Leaving large sums of money dormant in account for periods of time (e.g. to hide/store illicit funds)
- Chargebacks against multiple cards.
- Payment method details do not match customer registration details.
- Multiple customers are identified as sharing the same bank account or payment method from which deposits or withdrawals are made.

Product and platform features

- Remote gambling environments which enable rapid transactions and facilitate relatively easy account creation without face-to-face checks.
- Unregulated or unmonitored chat spaces and functions.
- Variations in CDD quality, weak ongoing monitoring and inadequate thresholds, insufficient staffing, limited training and gaps in record-keeping.
- Complex (and often cross-border) ownership structures that obscure beneficial ownership and control, and which may conceal criminal elements during the licensing process.
- Use of numerous and/or complex legal arrangements (e.g. nominees, trusts, foundations) in ownership structures.
- Structuring beneficial ownership shareholding in a way which aims to bypass/avoid thresholds for regulatory checks, especially when AML/CFT controls and anti-corruption frameworks are weak.
- Dependence on third-party providers or white-label arrangements without robust oversight.
- Third-party contracts and business arrangements with intangible service providers (e.g. software provision, marketing, consultancy or technology services) that appear to lack economic or commercial sense.
- Open-source information indicates that beneficial owners may be linked to organised crime groups, bribery, corruption, fraud (including cyber-enabled fraud (CEF)), modern slavery, competition manipulation or other criminal activity.
- Platform is based in a high-risk jurisdiction or a jurisdiction with weak anti-money laundering/counter terrorist financing (AML/CFT) measures.
- Ownership/control by individuals in high-risk jurisdictions for ML/TF/PF or regions with high instances of corruption, fraud (including CEF), and/or transnational organised crime.

- Rapid financial growth or unexplained profitability, sudden spikes in revenue or customer activity that do not appear to be in line with the business profile of the operator/platform.
- Significant business-to-business cross-border financial flows which are unrelated to regulated gambling activity.
- Operators engaging in rapid business expansion into other digital-led services (e.g. virtual asset service providers, payment service providers or digital marketing).
- Limited online presence and/or unsophisticated websites that lack functionality.
- Citizenship by investment nationals or dual nationals are beneficial owners of gambling operators, particularly from jurisdictions with weaker AML/CFT measures.
- Frequent changes of platform URLs /website addresses or company/brand name.
- Obtaining a gambling licence followed by prolonged period of operational inactivity
- Commercially questionable transfers of beneficial ownership (e.g. beneficial owners giving away ownership rights of their financially successful gambling businesses to third parties or purchasing under-performing gambling businesses at inflated prices).
- Platforms/operators accept new customers through introducers/agents.
- Commercial business-to-business transactions using VA.
- Remote service provision or use of agents.
- Online platform advertises in jurisdictions where gambling is illegal.
- Junket arrangements pertain to players from high-risk jurisdictions.
- Abuse of merchant identity (also known as “sham merchants”), where illicit operators disguise themselves as legitimate domestic businesses to process gambling-related transactions that appear as ordinary retail payments.
- Deliberate publication of images, videos or symbols that promote or endorse terrorism or violent extremism.

September 2026

www.fatf-gafi.org