GAMBLING

Money Laundering Red Flags

For Gambling Operators

Updated May 2026

Gambling Supervision Commission
Ground Floor, St George's Court
Myrtle Street
Douglas
Isle of Man
IM1 1ED

Red Flag Indicators - Terrestrial

1.

Changing Notes

Scottish/English/Northern Irish banknotes – customers using large amounts of these banknotes to then withdraw quickly/in large amounts of Manx notes, helping disguise the origin of the funds. Or currency conversion – launderers might wish to use this service to convert cash obtained from a predicate offence into cash of a different currency to complicate tracking of the source of funds.

2.

Minimal Play

Minimal play with large/quick transaction – both on FOBT machines and in the casino on slots/tables.

3.

Avoids Verification

Circumventing CDD - customer who wishes to cash out a value in excess of the threshold amount, who then upon request of CDD verification reduce the cashout amount to circumvent the CDD requirement. Or transacting slightly below the verification threshold consistently – i.e. £100s per visit – attempting to avoid the verification requirement.

4.

Unusual Bets

Unusual betting patterns – e.g. betting red and black on roulette, both with and against the bank in baccarat, both sides of the same event for sporting events – to try and ensure a win and 'legitimate' cash with minimal losses.

5.

Fake IDs

Use or attempted use of fake IDs (invalid/uncommon documents) or IDs that don't belong to the individual presenting the document.

6.

Third-Party Betting

Third-party betting – use of third parties/agents to disguise source or ownership of money. This may not be obvious and the customer may not declare they are acting as a third-party so it is something to be vigilant for, e.g. customers acting suspicious/mysterious.

7.

Odd Behaviour

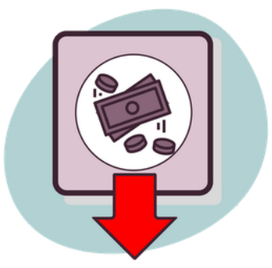
Customer's behaviour acting mysterious/suspicious i.e. 'shifty' – or out of character for a regular customer – could be using stolen money, fake ID, been coerced into placing a bet.

8.

Dormant Funds

Customer leaving large amount of funds on their account for a long period of time – e.g. use of Casino account as a 'savings account' to hide/store criminal money.

9.



Smurfing

Smurfing – placing frequent smaller bets across different betting accounts (collusion) or different betting shops to avoid the threshold.

10.

Lots of Cash

Mainly cash businesses so common to see cash – but large amounts of cash being transacted, well above a customer's means could be identified as unusual activity.

11.

Bribery

Customers attempting to bribe, influence, or conspire an employee to avoid requesting CDD or further verification documentation.

12.

Transferring Funds

Customers transferring funds - chips (Casino) or a betting slip (bookmaker/LBO) to another individual for them to cash out.

13.

Higher Risk Jurisdictions

Customers from higher-risk jurisdictions spending large amounts of cash.

NOTE.

Regularly check adverse media and typology reports, such as UNODC reports, highlighting emerging risks. The latest NRA is available on the counteringfinancialcrime.im website.

GSC GAMBLING

Red Flag Indicators - OGRA

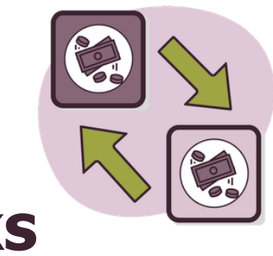
1. Many Cards

Unusual numbers of cards or payment types being used against one account.

2. Different GEOs

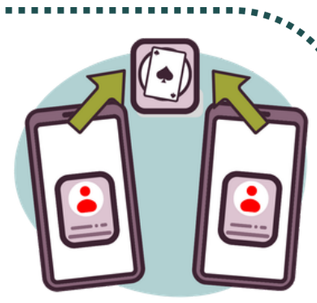
Accounts being accessed from different geo-locations for different payment types.

3. Chargebacks



Chargebacks against multiple cards.

4. Playing together



Players 'always playing' together and one person always winning.

5. Same IPs

IP address checks show players at the same address or using the same Internet Service Provider.

6. Bad Key Words

Chat board monitoring by the e-gaming company picking up key words and evidence of groups conspiring.

7. Mismatched Details

Information provided by the player contains a number of mismatches (e.g. email domain, telephone or postcode details do not correspond to the country). And/or the registered credit card or bank account details do not match the player's registration details.

8. Sanctions

The player is situated in a higher-risk jurisdiction or is identified as being listed on a sanctions list.

9. It's a PEP

The player is identified as a politically exposed person.

10. Multiple Accounts

The player seeks to open multiple accounts under the same name OR the player opens several accounts under different names using the same IP address.

11. Strange Login

The customer logs on to the account from multiple countries.

12. Big Deposit

The player deposits large amounts of funds into his online gambling account.

13. Withdrawals

The withdrawals from the account are not commensurate with the conduct of the account, such as for instance where the player makes numerous withdrawals without engaging in significant gambling activity.

14. Inactive Funds

A deposit of substantial funds followed by very limited activity.

15. Suspicious SOFs

The source of funds being deposited into the account appears to be suspicious and it is not possible to verify the origin of the funds.

16. Re-opened

The player has links to previously investigated accounts.

17. Shared Bank Details

Different players are identified as sharing bank accounts from which deposits or withdrawals are made.

Red Flag Indicators

For a full list of typologies, flags and controls please read the Gambling sectoral NRA (2026)

18. AI-Assisted ML 1

Multiple gambling accounts showing identical playing patterns, timing intervals or transaction signatures.

19. AI-Assisted ML 2

Synthetic IDs that pass initial digital Know Your Customer ('KYC') checks but exhibit repeated anomalies during live or follow-up authentication.

20. AI-Assisted ML 3

Gameplay that is statistically improbable for a human – extremely consistent reaction speeds, highly uniform betting patterns, or instantly adaptive wagering.

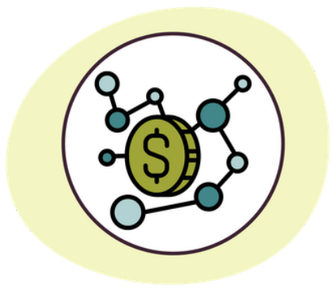
21. Straw account 1

Mules claiming to work for online companies that do not exist.

22. Straw account 2

Verification calls or live video checks where the individual's image shows unnatural lighting, audio that doesn't match the environment, or biometric desynchronisation consistent with deepfake use.

23. B2B VA Payments



Use of virtual assets for B2B settlement or other payments, particularly where wallet provenance cannot be established, may indicate attempts to obscure the flow of funds. (Note: may also overlap with straw man ownership and concealed-control typologies.)

24. B2B Businesses (front company)

Company was recently incorporated with minimal operating history; the registered office may be a virtual office or shared office space. Minimal company information available online and the company may operate over multiple jurisdictions with poor transparency.
Business plans are unrealistic or vague, income isn't commensurate with activity, or the business is unprofitable and is being subsidised with no evidence of growth or restructuring in order to grow profits. Minimal or no genuine business operations.

25. Ownership /control

Owners and/or management appear not to exercise genuine control over key decisions within the business.

A lack of effective control, particularly where decision-making authority is unclear, delegated in unusual ways, or inconsistent with the stated ownership structure, may indicate that another party is exerting influence behind the scenes.

26. Complex Structure

The use of trusts, foundations, shell companies, or nominee arrangements without a credible business rationale, particularly where there is reluctance or refusal to disclose the individuals who ultimately own or control the entity, may indicate attempts to obscure beneficial ownership.

NOTE.

- Regularly check adverse media and typology reports, such as UNODC reports, highlighting emerging risks.
- The latest NRA is available on the counteringfinancialcrime.im website.
- The Isle of Man FIU also produced monthly typologies on thier website.

GSC GAMBLING