



Human Trafficking Red Flags

For Gambling Operators

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

Red Flag Indicators - Terrestrial

1.

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

2.

Fake IDs

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



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.

Lots of Cash

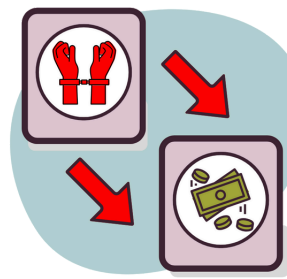
Mainly cash businesses so common to see cash – but large amounts of cash being transacted, well above a customer's means could be identified as unusual activity



5.

Bribery

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



7.

Higher Risk Jurisdictions

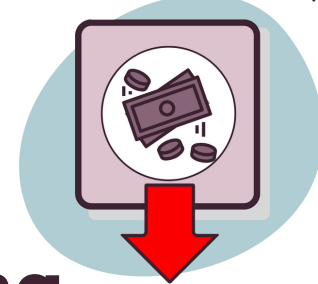
Customers from higher-risk jurisdictions spending large amounts of cash.



8.

Smurfing

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



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

Red Flag Indicators - OGRA

1.

Many Cards



Unusual numbers of cards or payment types being used against one account. All in different names.

2.

Same IPs

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

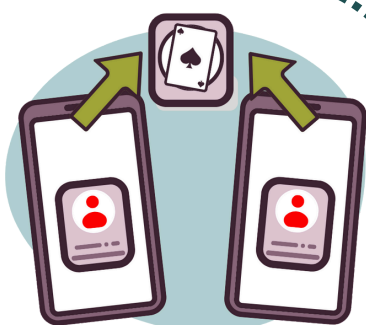
3.

Bad Key Words

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

4.

Playing together



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

5.

Sanctions



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

6.

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.

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.

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.

9.

Shared Bank Details



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

10.

Isolation



Staff members from higher risk jurisdictions seem coerced, controlled or isolated.

NOTE.

Regularly check adverse media and typology reports, such as UNODC reports, highlighting emerging risks.