ISLE OF MAN

Proliferation Financing 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.

Avoids Verification

Circumventing CDD - a 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.

2.

Minimal Play

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

3.

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.

4.

Unusual Bets

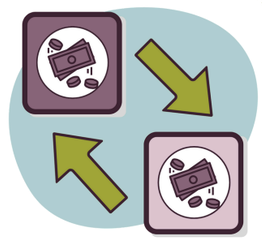
Unusual betting patterns – e.g. betting red and black on roulette, both with and against the bank in baccarat, both sides of the same event for sporting events – to try and ensure a win and 'legitimate' cash with minimal losses.

5.

Strange 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.

6.



Transferring Funds

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

7.

Higher Risk Jurisdictions

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

8.

PF Jurisdictions

Links to countries associated with Proliferation (Iran, DPRK, Russia).

9.

PF Crypto Links

Cyptocurrency address linked to bad state actors such as the Lazarus group (APT- 45).

GSC
ISLE OF MAN

Red Flag Indicators - OGRA

1.

Same IPs

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

2.

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.

3.

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.

4.

Sanctions

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

5.

Shared Bank Details

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

6.

It's a PEP

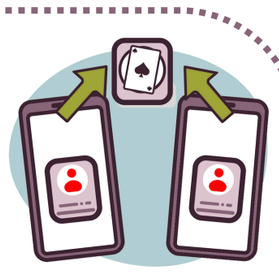
The player is identified as a politically exposed person.

7.

Strange Login

The customer logs on to the account from multiple countries.

8.



Re-opened

The player has links to previously investigated accounts.

9.

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.

10.

PF Crypto

Cypto address linked to bad state actors such as Lazarus group (APT- 45).

11.

Higher-Risk Industries

Links to industry associated with Proliferation Financing, such as manufacturing, health, etc.

12.

PF Jurisdictions

Links to countries associated with Proliferation (Iran, DPRK, Russia).

ISLE OF MAN

NOTE.

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