



Money Laundering Typologies

For Gambling Operators

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

Gambling Typologies

1.



Fake Wins

A money launderer, in collusion with an operator of an offshore gambling website, deposits funds obtained from criminal activities in the gambling account and withdraws such funds as winnings. The website operator keeps a percentage of the proceeds as a commission while the launderer declares the winnings to the tax authorities and then uses the funds for legitimate purposes.

2.



Offshore

A money launderer sets up a company in an offshore jurisdiction through various frontmen. The company then applies for an online gambling licence in the offshore jurisdiction. Funds deriving from criminal activity are then laundered through the online gambling website which is controlled by the launderer.

3.



Beneficial Owners

A criminal colludes with other persons who act as beneficial owners of a company which is used to obtain an online gambling licence. Illegally obtained funds are then co-mingled with the legitimate profits of the company and deposited in a bank account. This can be used by OCGs to offer 'Money Laundering as a service'.

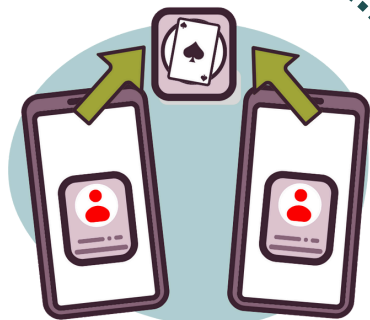
4.



Fake Site

A money launderer sets up an online gambling website without registering the website or obtaining a licence. The website is not made available to the public but is used to place funds obtained from criminal activities which are then distributed as winnings to various frontmen. The website is then disconnected citing failure to make a profit as the primary reason for the disconnection.

5.



Collusion

A money launderer colludes with professional gamblers to place illegally obtained funds on online gambling websites. The gamblers keep a commission from any winnings made before transferring the remaining funds to the launderer.

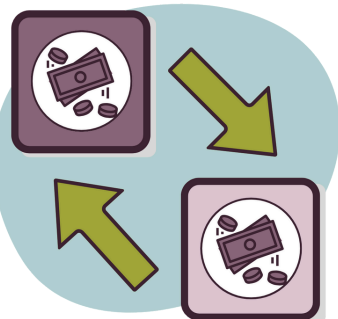
6.



Fake ID

Illegally obtained funds are deposited into an online gambling account using a false identity. The player engages in minimal gambling activity which is sufficient to make the account appear genuine. After incurring minimal losses the funds are then transferred from the gambling account to a legitimate bank account.

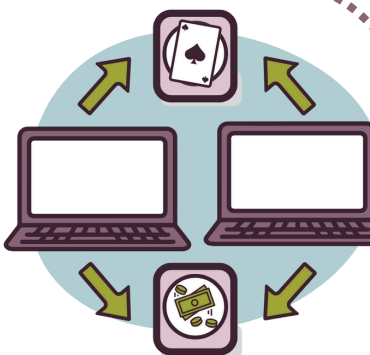
7.



E-Wallet

A money launderer deposits funds derived from criminal activities into an e-wallet through a money service business. The funds are then deposited into an online gambling account by frontmen. The winnings are remitted back to the e-wallet account and used for other legitimate purposes on other websites.

8.



Deliberate Losses

Peer-to-peer games such as e-poker, where value transfers can occur between both electronic and human players as a result of deliberate losses, at a relatively low cost to the players. Players will make large bets on very bad hands expecting to lose to the accomplice. This is generally known as chip-dumping and is considered to mainly pose a risk of FT.

9.



Multiple Cards

A money launderer uses multiple cards to deposit funds derived from criminal activities (either in their own name or someone else's) before withdrawing the funds back out to either one card or to another facility such as an e-wallet.

Gambling Typologies

10.

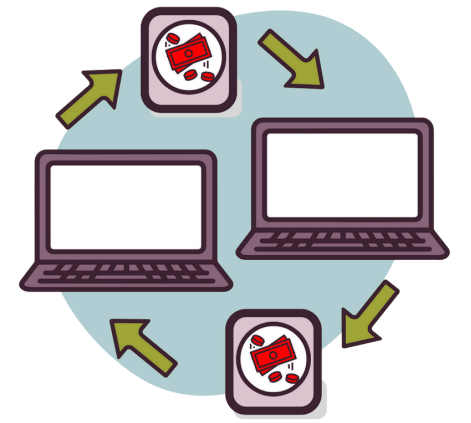
Parallel even-money betting



Two criminals acting in collusion in the same online game can transform illicit funds into gambling winnings by wagering on opposing positions with even odds. It is almost certain that one player will win and the other will lose, but between the two of them they will end up with the same amount of money they started with.

11.

Disguising illegal spending



Similar to the cash in, cash out method – the criminal will introduce funds into an online gambling account and engage in minimal low-risk gameplay before cashing out. But the criminal will seek to cash out their funds into a different bank account or in a different medium (like cryptocurrency).

They then show the money leaving their bank account but not re-entering and claim that the funds were all spent on losing bets.

12.

Bank Card Fraud



Criminals use stolen bank cards or card details to credit online gambling accounts and then request that any balance or winnings are cashed out to their own bank account through a different payment method. Or use their own bank cards to credit online gambling accounts which they have set up under fake or stolen identities.

13.

Sports Fixing



Criminals bet on a competition with a rigged outcome to ensure a win. Using online gambling platforms, criminals set up multiple accounts across a variety of platforms using fake or stolen identity documents, making it possible to place a large number of bets pseudonymously.

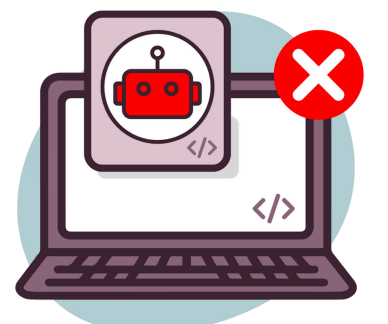
14.

Front for Cyber-enabled Fraud Operation

The illicit funds accumulated through fraud can be laundered through the B2B method described above and may be funnelled through or to offshore jurisdictions for concealment and safekeeping.

15.

Account Takeover



Buying accounts that are already Customer Due Diligence / Enhanced Due Diligence verified and using them.

NOTE.

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