Money Laundering Typologies

For Gambling Operators

Updated May 2026

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

Money Laundering

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.

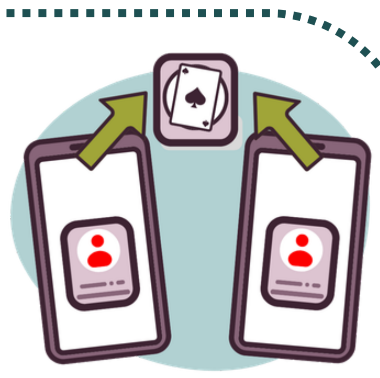
3. Beneficial Owners

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

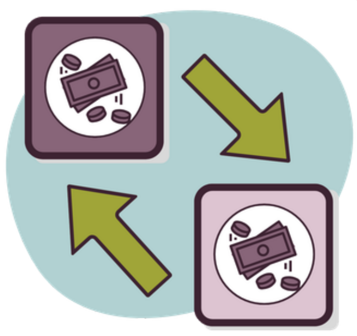


A money launderer colludes with professional gamblers to place illegally obtained funds on online gambling websites. The gamblers keep a commission from any winnings made before transferring the remaining funds to the launderer.

6. Fake ID

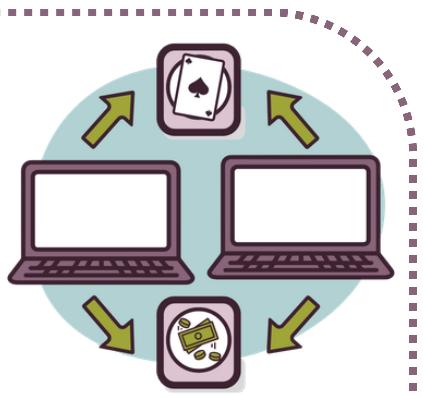
Illegally obtained funds are deposited into an online gambling account using a false identity. The player engages in minimal gambling activity which is sufficient to make the account appear genuine. After incurring minimal losses the funds are then transferred from the gambling account to a legitimate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

GSC GAMBLING

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.

Money Laundering

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 into 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 competitition 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 CDD / EDD verified and using them. FIU Monthly Typology - Jan 2026: Fraudsters take over accounts by impersonating staff of the company holding the users' funds, asking them for login information, including a one-time password, which enables them to take the account over.

16. Vancouver Model

1. A person in Jurisdiction X (who may or may not have been involved in a crime) attempts to transfer substantial funds out of that jurisdiction and may circumvent cash export control laws.
2. The person transfers funds to a criminal group in Jurisdiction X and then travels to Jurisdiction Y.
3. A criminal gang in Jurisdiction X arranges for its associates in Jurisdiction Y to transfer an equivalent amount of the original transfer amount to someone now in Jurisdiction Y (mostly in the form of cash derived from criminal activity which needs to be laundered).
4. The person enters the casino, converts the money into chips, then makes several low value bets and cashes out.
5. This person traded the chips for clean cash or cash checks, and now has both laundered funds for the criminal group through the original transfer and bypassed the cash exit control laws in Jurisdiction X for their own benefit.

GSC GAMBLING

NOTE.

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

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

17.

Straw man ownership

To conceal the true ownership or control of an entity, an individual may be installed as the legal owner, or a corporate vehicle or arrangement may be created to provide nominee ownership. The purpose is to give the business an appearance of legitimacy while enabling the concealment and comingling of illicit proceeds with legitimate funds and/or evasion of regulatory scrutiny.mingling of illicit proceeds with legitimate funds and/or evasion of regulatory scrutiny.

18.

Environmental Crime

Laundering of proceeds of environmental crime, such as habitat destruction/overfishing, through gambling. SoF/SoW from cash jobs with non-verifiable companies that have little/no online presence. Engage in minimal, low-risk play and pull funds back out quickly.

Criminal Ownership Typology Example

Enterprise Global Solutions is a B2C mid-size online casino based in an IFC and holding a legitimate remote gambling licence, which provides access to reputable banking, payment processors and professional services. The licensed entity only represents a small portion of a wider group.

In 2022 EGS gambling business slows and at the same time several new companies are incorporated across the wider group. These entities describe themselves as software developers, digital marketing providers, data analytics companies, turnkey solution providers and crypto payment processers. They rely on intangible cross border service supply that are difficult to verify.

On a quarter-by-quarter basis the wider group funds increases and the bank accounts for the licensed entity see unusually large payments from payment services providers and the affiliated companies purporting to be from gambling, software supply, data hosting and technology services. Service agreements show large revenue agreements which seem disproportionate, and the third parties contracted with all are incorporated around the same time, have similar names and minimal online presence.

Open-source intelligence later reports the links between owners and organised crime groups and opaque structures with allegations of modern slavery, online scams and cyberfraud. The illicit funds being moved through a cluster of shell companies outside of the jurisdiction purporting to be gambling companies, software providers, software resellers, payment gateways giving a plausible explanation to the movement of significant amounts. The regulated status allowed high risk digital service companies within the wider group to justify large cross border payments under the cover of B2B services. This allowed for the large-scale integration of online fraud proceeds into the mainstream financial system through corporate level flows rather than through customers and gambling transactions.

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

Money Laundering

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

19.

Criminal Lifestyle Spend

Individuals that may be known to have criminal associations or to engage directly in criminal behaviour may use their illicit income for leisure activities, especially those with a VIP status. Conversely, problem gambling can create financial stress, which in some cases may increase a person's vulnerability to undue influence or risky behaviour. This does not imply criminality, but financial pressure can occasionally act as a contributing risk factor

20.

AI-assisted ML

Professional ML networks deploy chains of AI agents capable of autonomously performing financial actions across multiple platforms, including online gambling accounts. These agents, often created and orchestrated by a single professional ML actor, can open and operate multiple gambling accounts using synthetic or co-opted identities; and schedule and execute microtransactions (deposits, gameplay, wagers, withdrawals).

21.

AI-facilitated Agent Recruitment & Management

A ML scheme that automates recruitment/management of straw account holders (mules) and executes high volume, microtransactions into hundreds of mule accounts to launder large sums via online gambling platforms. To launder the funds, AI agents automate transactions into hundreds of mules bank accounts used to launder significant sums through online gambling platforms. Perpetrators also bypass digital ID verifications using AI-generated deepfakes

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 their website.

GSC GAMBLING