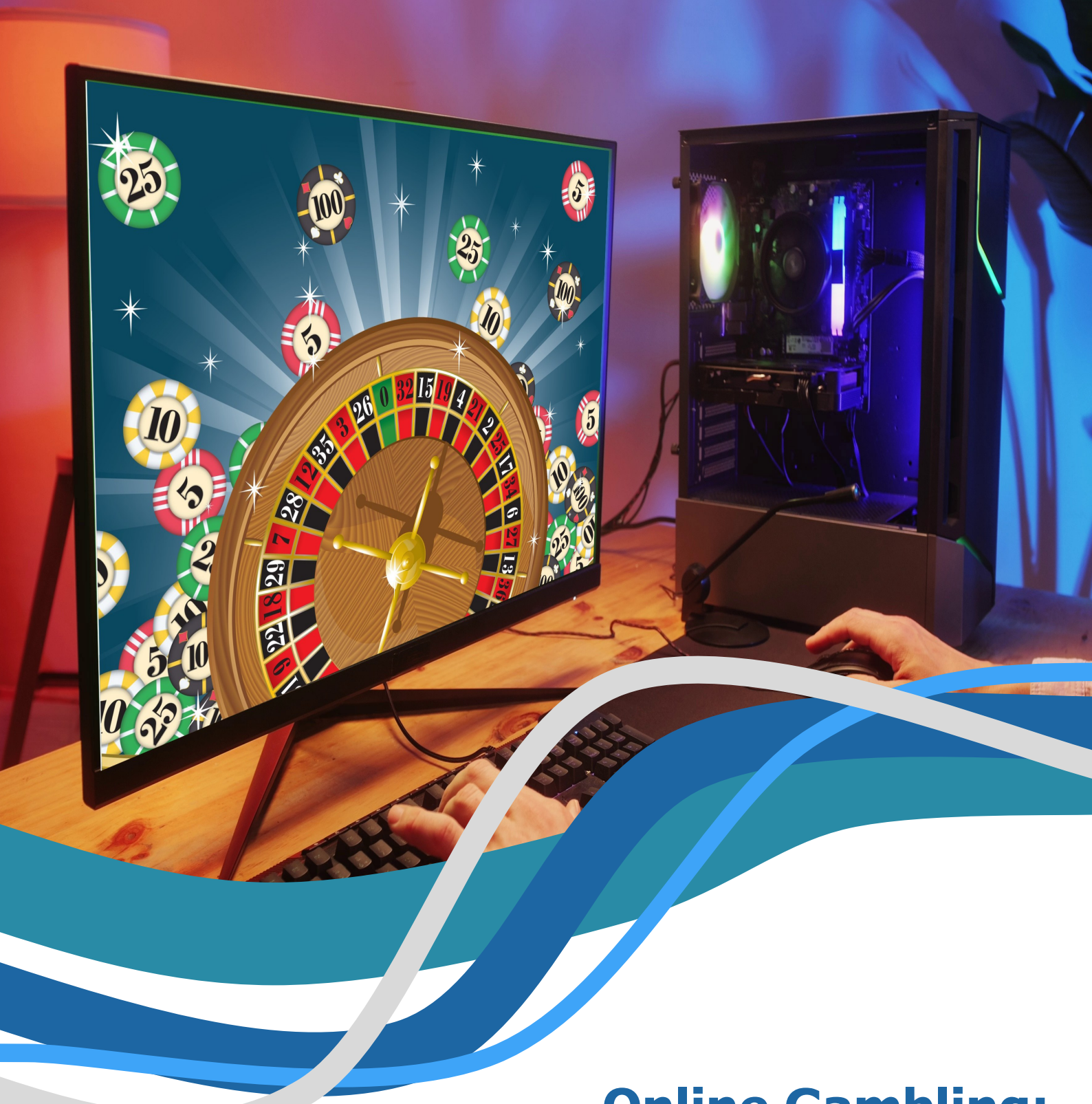


Online Gambling: Red Flags and Typologies for Money Laundering, Terrorist Financing, and Proliferation Financing

May 2025

Isle of Man
Financial Intelligence Unit
Ellan Vannin Unnid Tushtag Argidoil

Contents

Introduction

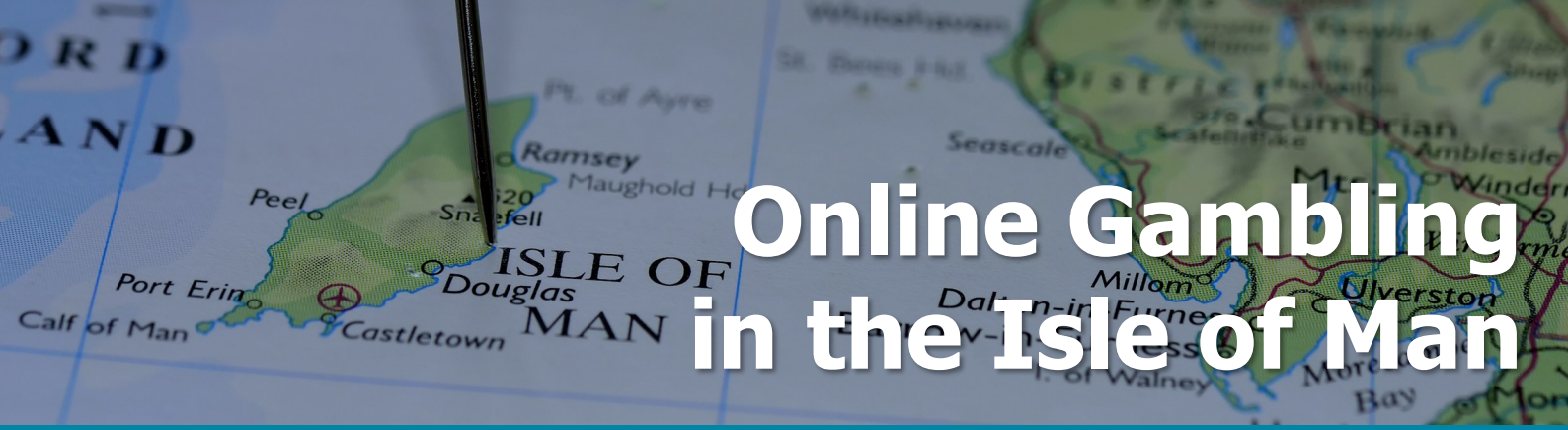
The project undertaken by the Isle of Man Financial Intelligence Unit (FIU) to provide typologies to industry is part of the commitment made to fulfil international obligations under Financial Action Task Force (FATF) Recommendation 29 to identify money laundering and terrorist financing related threats and vulnerabilities and as part of its general powers to provide or assist with the provision of awareness training in relation to financial crime.

The following examples are fictional scenarios, loosely based on the type of information received and analysed by the FIU and follow on from previously issued typologies to assist in highlighting areas and focus information the FIU is receiving relating to suspicions of financial crime relating to the online gambling sector. Whilst some of the activity described can be linked to specific jurisdictional areas of higher risk, understanding and being able to identify the underlying activity itself is crucial, as financial crime is evolutionary in nature and as jurisdictions of higher risk become known, activity is likely to move geographically to evade detection.

The increasing success and popularity of the online gambling industry has brought an increasing risk of businesses in this sector being used to facilitate financial crime.

This document is intended to assist professionals across a range of reporting sectors to identify signs of potential money laundering (ML), terrorist financing (TF), and proliferation financing (PF) associated with online gambling. We anticipate that this document will be useful for a wide variety of professionals working across different sectors, including online gambling and e-gaming, banking, money services businesses, corporate services, accountancy, virtual asset service providers, legal services, and conveyancing.

“A typology is the study or systematic classification of types that have several characteristics or traits in common”
-ECOFEL



Online Gambling in the Isle of Man

The Isle of Man has a well-established online gambling industry which plays a significant role in the local economy, representing around 14% of national income[1]. Businesses in this sector benefit from a mature licensing regime and a strong network of wider professional services, including corporate service providers, information and communication technology (ICT) providers, legal professionals, and accountants.

The Island's gambling regulator, the Gambling Supervision Commission (GSC), offers five types of online gambling licence, which are issued under the Online Gambling Regulation Act 2001 (OGRA): the network licence, full licence, sub-licence, software supplier licence, and token or blockchain-based software supplier licence. Each licence is issued with specific licence conditions, which vary according to the type of activity the GSC has approved the licensee to undertake.

These licences allow holders to engage in various types of activity which sit under two broad categories: business to customer (B2C) activities, and business to business (B2B) activities. B2C activities involve offering games to, striking bets with, and registering players. B2B activities involve providing games or software to other businesses or entering into arrangements which allow other businesses to use one's games, software or servers to conduct their own B2C activities (e.g. sub-licence or network partnership arrangements).

The network licence is the most comprehensive offering because it can permit the widest range of B2C and B2B activities (depending on the specific licence conditions approved by the GSC). At the other end of the scale, the two software supplier licences are elective, meaning businesses are not obliged to be licensed to carry out these activities in the Isle of Man. Operators are only eligible for OGRA licences if they meet certain conditions which include establishing an Isle of Man company, appointing a local designated official or operations manager, and establishing appropriate player protection mechanisms for B2C activities. Whose responsibility it is to register players and conduct customer due diligence varies according to which type of licence or B2B arrangement a firm is operating under.

1. Isle of Man National Income Report 2022/23

Full licence holders must register players and conduct due diligence for their own customers and those of any associated white label providers; sub-licence holders register players and conduct due diligence themselves; and network licence holders can accept customers from network partners (other global operators) without registering them, relying on the due diligence conducted by the network partner.

Online gambling firms that hold network, full, or sub-licences are regulated for compliance with the anti-money laundering (AML) and countering the financing of terrorism (CFT) requirements set out in the Gambling AML/CFT Code 2019. Although firms that hold software licences are not covered by the Gambling AML/CFT Code, they are given licence conditions and guidance relating to AML/CFT. Licence holders are obligated to report suspicious activity to the Financial Intelligence Unit (FIU).

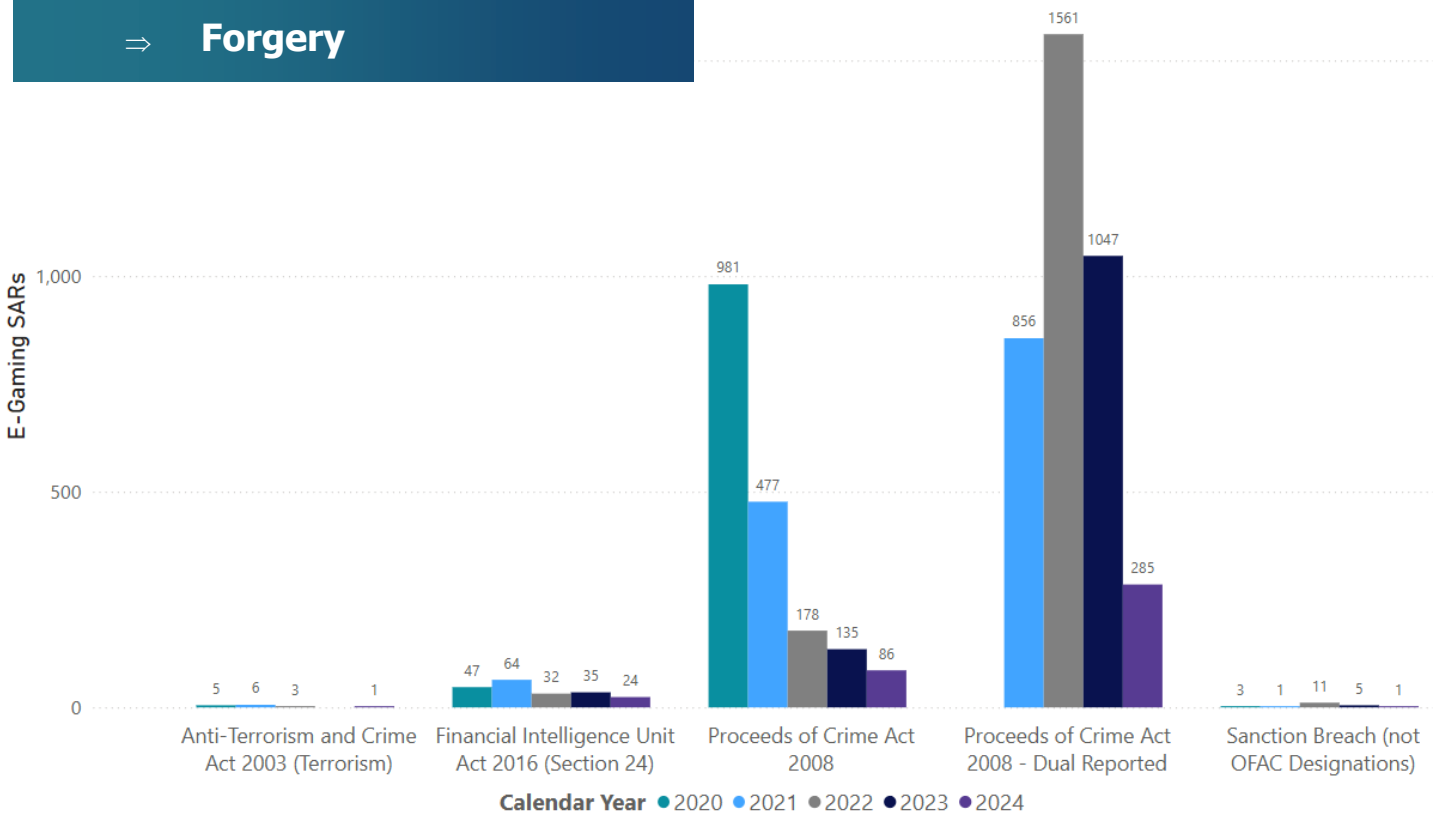
Statistics

Over the last five years 96% of SARs from the online gambling sector were submitted under the Proceeds of Crime Act 2008, 4% under the Financial Intelligence Unit Act 2016, 0.4% under sanctions legislation, and 0.3% under the Anti-Terrorism and Crime Act 2003. Of the SARs submitted under the Proceeds of Crime Act, 56% concerned suspicions about fraud. The second most commonly reported suspicion was drug trafficking (8% of SARs), followed by cybercrime (5%), tax crime (4%), and forgery (2%). It is worth noting that over half of the SARs submitted to the FIU were dual reported (relating to activity occurring in another jurisdiction and also reported to that jurisdiction), and 93% of all SARs submitted by the gambling industry came from a single OGRA licence holder.

Most Frequently Reported Suspected Criminalities

- ⇒ **Fraud**
- ⇒ **Drug Trafficking**
- ⇒ **Cybercrime**
- ⇒ **Tax Crime**
- ⇒ **Forgery**

"In the last 5 years, 93% of all SARs submitted by the gambling industry came from a single OGRA licence holder."



Criminal Misuse of Online Gambling

Since the very beginnings of gambling as an industry it has always been inherently vulnerable to misuse by criminals because games of chance can provide convenient cover stories for accumulations or transfers of illicit funds. Online gambling businesses are particularly vulnerable because:

- ⇒ **They afford a greater degree of anonymity than their face-to-face alternatives,**
- ⇒ **They increasingly support cryptocurrency payment options,**
- ⇒ **Their operations involve a very large volume of high-speed transactions, and**
- ⇒ **They move large volumes of money across international borders.**

These features make online gambling platforms an attractive prospect for criminal actors who want to disguise the origin or destination of illicit funds.

This document outlines some of the methods by which criminals may use online gambling in the course of laundering criminal proceeds, moving money for financing terrorism, or evading sanctions to engage in proliferation financing.

It is important to remember that it may, in practice, be difficult to differentiate between suspicious activity which indicates ML and suspicious activity which indicates either TF or PF. All of the methods described below may be used for ML, but some of them are more suited to TF or PF than others – these will be highlighted as they are described. Also remember that ML, TF, and PF are not mutually exclusive – terrorist organisations and proliferation financiers often make use of proceeds from other criminal sources to help fund their activities. It is essential to be mindful of whether suspicious activity involves persons or jurisdictions of concern when evaluating the risks of TF or PF.

The information below has been compiled from a variety of sources, including Isle of Man FIU databases as well as a range of open-source publications from non-governmental and intergovernmental organisations. All of the examples given to illustrate ML, TF, and PF methods are fictionalised.

These typologies are intended to help professionals understand trends in criminal behaviour and identify patterns in suspicious activity. They are not comprehensive, but they highlight some of the ways in which criminals have used or attempted to use online gambling to facilitate financial crime. It is important to remain alert to new methods and report any suspicious activity to the FIU.

Use of Online Gambling Accounts

Concealing the origin of funds

Cash in, cash out

Criminals can obscure the illicit origins of criminal proceeds by passing them off as gambling winnings. The simplest method for achieving this is known as 'cash in cash out': a criminal introduces illicit funds into an online gambling account, places a few low-risk bets to create the appearance of legitimate gameplay, and then cashes the money out again. They can then point to the money entering their bank account from the online gambling platform and claim the funds represent winnings from bets placed. This simple ML method would only withstand a limited degree of scrutiny, and most gambling platforms have compliance controls which would prevent a player from withdrawing funds before they had played through a significant proportion of their deposit. More sophisticated variations of the cash in cash out method, however, are harder to detect.

Organised criminal groups (OCGs) may split criminal proceeds between a large number of unrelated individuals so that the funds can be passed through multiple online gambling accounts and payment platforms in small volumes (below any reporting thresholds). These large teams of money mules are known as motorcades or points running syndicates, and there are OCGs which specialise in arranging and providing this type of ML service. Advances in computer technology have also allowed some more sophisticated criminal syndicates to automate the process, increasing the speed of processing and eliminating the need to recruit other individuals to act as money mules.

This ML method can be used with either fiat or virtual currency, but the UNODC have reported an increasing trend in the laundering of virtual currencies through online gambling sites. Online gambling accounts can be used alongside crypto mixers, bridges, and peer-to-peer exchanges to obscure the origin of illicit funds and make criminal proceeds very difficult to track. Fluctuations in the value of different virtual currencies also offer criminals a plausible explanation for otherwise unexplained wealth.

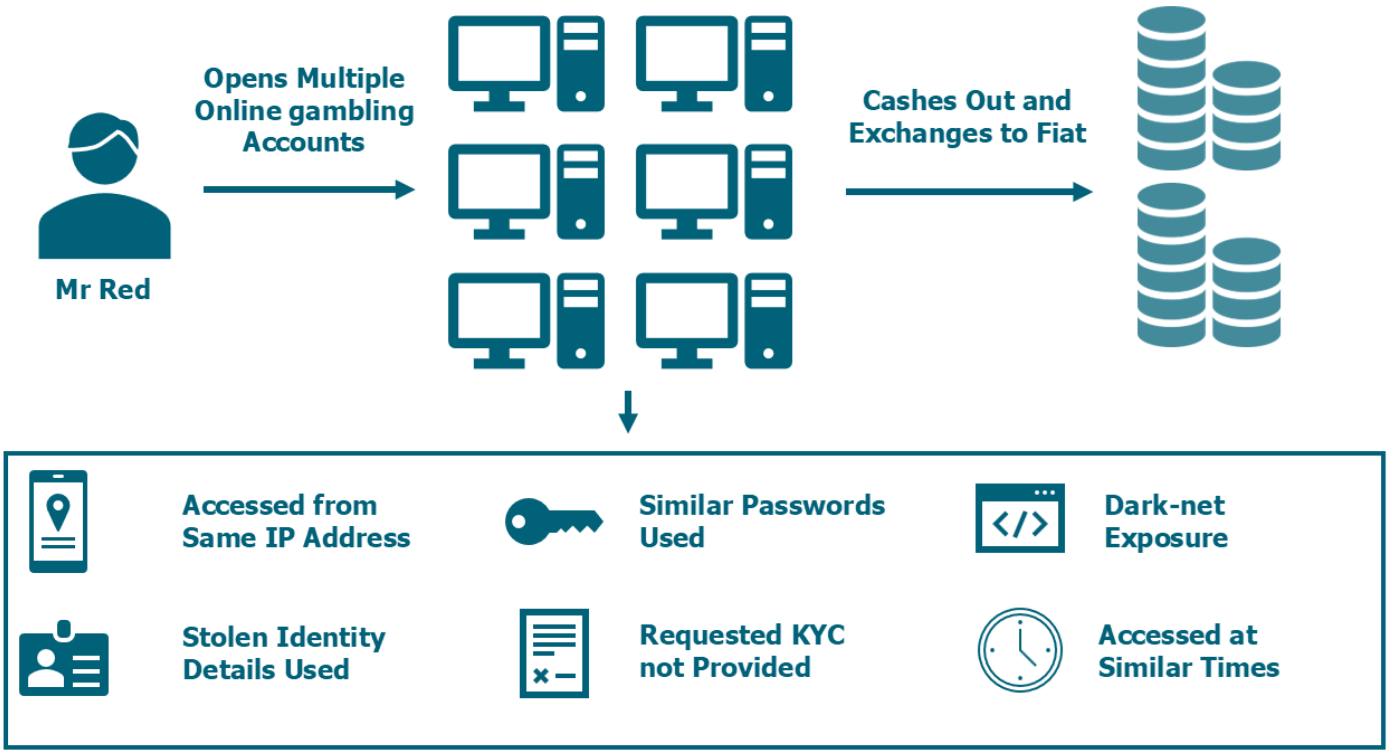
When large volumes of fiat or cryptocurrency are laundered in this way, there is an elevated risk of PF. Cyber-criminals acting on behalf of North Korea (the DPRK) are known to have used the accounts of international junket operators as part of the laundering process for funds stolen during the 2016 Bangladesh Central Bank heist[2].

2. BBC News: The Lazarus heist – How North Korea almost pulled off a billion-dollar hack

Example:

Mr Red is a drug dealer who uses the dark web to sell his products in exchange for cryptocurrency. He used stolen identity details to open a large number of accounts on a variety of online gambling platforms, including 20 different accounts on Isle of Man licensed Platform A. Mr Red deposited illicit cryptocurrency in each of his gambling accounts using different crypto wallet addresses. He would then play through enough of his funds to avoid any withdrawal controls before cashing his funds out and using a payment service provider to exchange the crypto for fiat currency.

Platform A uses crypto investigation software to conduct payment analysis as part of its due diligence regime. When the payments into Mr Red's accounts were analysed, the crypto addresses he had used to fund his accounts were linked to other addresses with dark net market exposure. This prompted the compliance team at Platform A to conduct reviews on each of the accounts opened by Mr Red. Because he had used stolen identity details to open the accounts, Mr Red was unable to provide the additional know your client (KYC) information requested by Platform A's compliance team. It also became apparent on review that each of Mr Red's accounts used very similar passwords and were logged into at similar times and from the same IP address. The compliance team inferred that these 20 accounts may be linked, and they reported their suspicions to the FIU.



Red Flags

Use of multiple sources of funds, Avoidance of withdrawal controls, Dark-Web links, Failure to provide KYC, Multiple accounts with same IP address

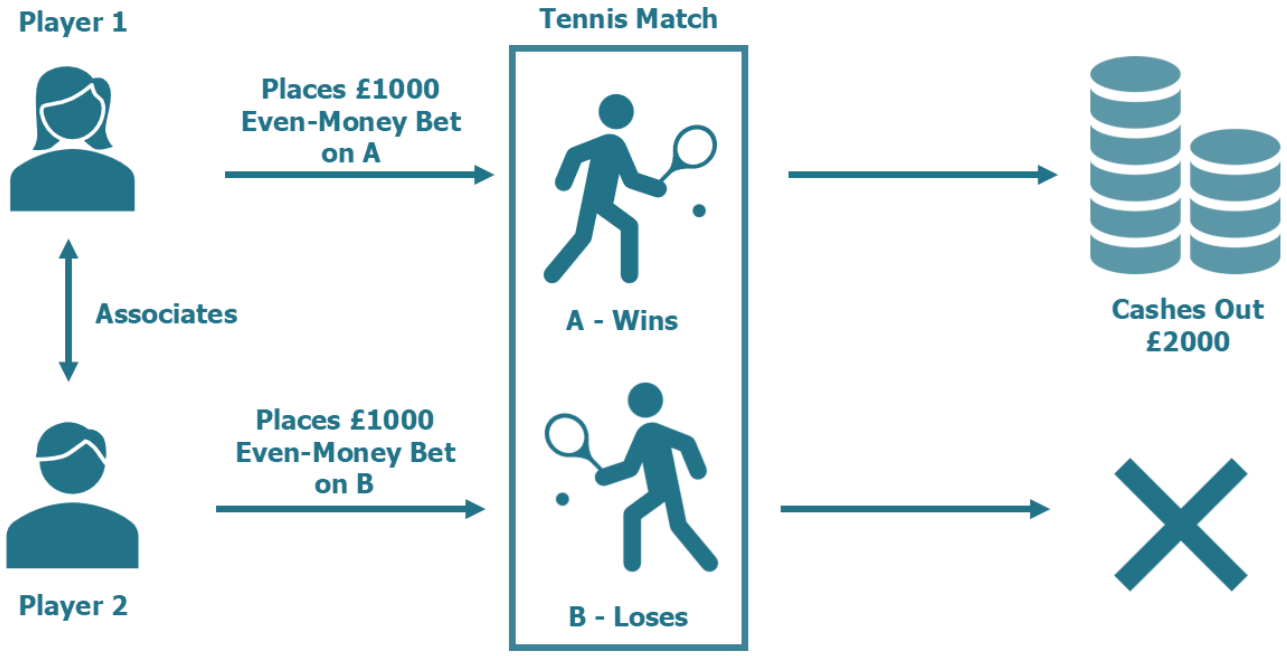
Parallel even-money betting

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. For example, imagine a game of roulette. Criminal A places an even-money bet of £200 on red, meaning that they stand to double their money if they win. At the same time, criminal B, an accomplice of criminal A, places an even-money bet of £200 on black. 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. What was £400 of criminal proceeds is now £400 of legitimate gambling winnings.

Example:

The compliance team at Isle of Man licensed sports betting platform, Platform B, noticed some suspicious activity involving two of its gambling accounts, Account 1 and Account 2. The compliance team had noticed these two accounts repeatedly placing very large bets on tennis matches. Account 1 would bet on one player winning, and Account 2 would always bet on the other player winning.

Although the accounts were in different names, and the account holders were listed as living in different jurisdictions, they had both been opened on the same day. The account holders always logged on to place their bets within hours of each other, and from the same IP addresses. When the compliance team at Platform B requested KYC information from the holders of Accounts 1 and 2, they received no response. They inferred that the accounts may have been used to launder illicit proceeds, and they submitted a SAR to the FIU.



Red Flags

Repeated interaction between accounts, Accounts opened at the same time, Activity repeated between accounts, Multiple accounts with same IP address, Failure to provide KYC

Concealing the destination of funds

Chip dumping

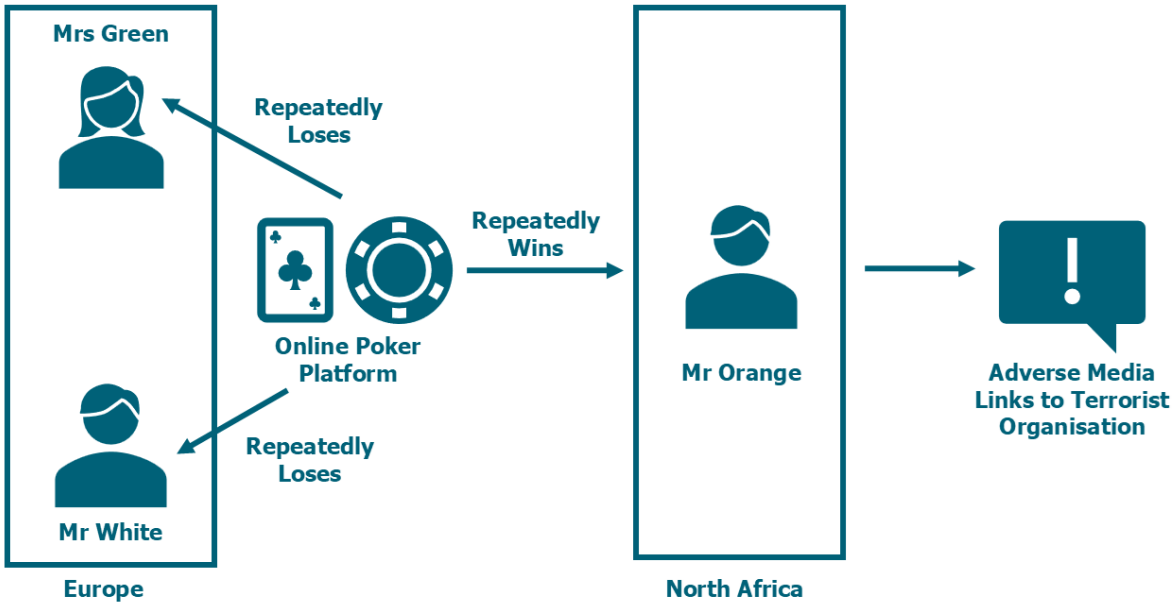
Online gambling accounts can also be used by criminals who want to covertly transfer money to others for illegitimate purposes. Games which allow people to play against each other (peer-to-peer games), like online poker, provide an easy option for criminals who want to directly exchange funds. When two (or more) colluding players enter the same online game, they can coordinate their gameplay so that one player deliberately loses to another, a practice known as 'chip dumping'.

Criminals may engage in this behaviour for various reasons - they may want to settle debts, pay for criminal services, or move money across national borders undetected. Because this method allows people to transfer money between jurisdictions without using the formal financial system it is a particular risk for TF.

Example:

Mrs Green and Mr White, who both reside in Europe, and Mr Orange, who resides in North Africa, all held accounts with an online casino platform licensed in the Isle of Man, Platform C. The compliance team at Platform C were alerted to a suspicious pattern of gameplay involving Mrs Green, Mr White, and Mr Orange. The three players were regularly entering the same online poker games, and their manner of play seemed unusual. Mrs Green and Mr White would often make unwise or irrational decisions during the poker games and would always end the games having lost money to Mr Orange.

Although the amount of money passing from Mrs Green and Mr White to Mr Orange wasn't large, Platform C's compliance team was concerned about the apparently deliberate transfer of funds between the players. Undertaking enhanced due diligence checks, the compliance team found media articles alleging a link between Mr Orange and a sanctioned terrorist organisation active in North Africa. The compliance team suspected the activity on Platform C may have been TF and submitted a SAR to the FIU.

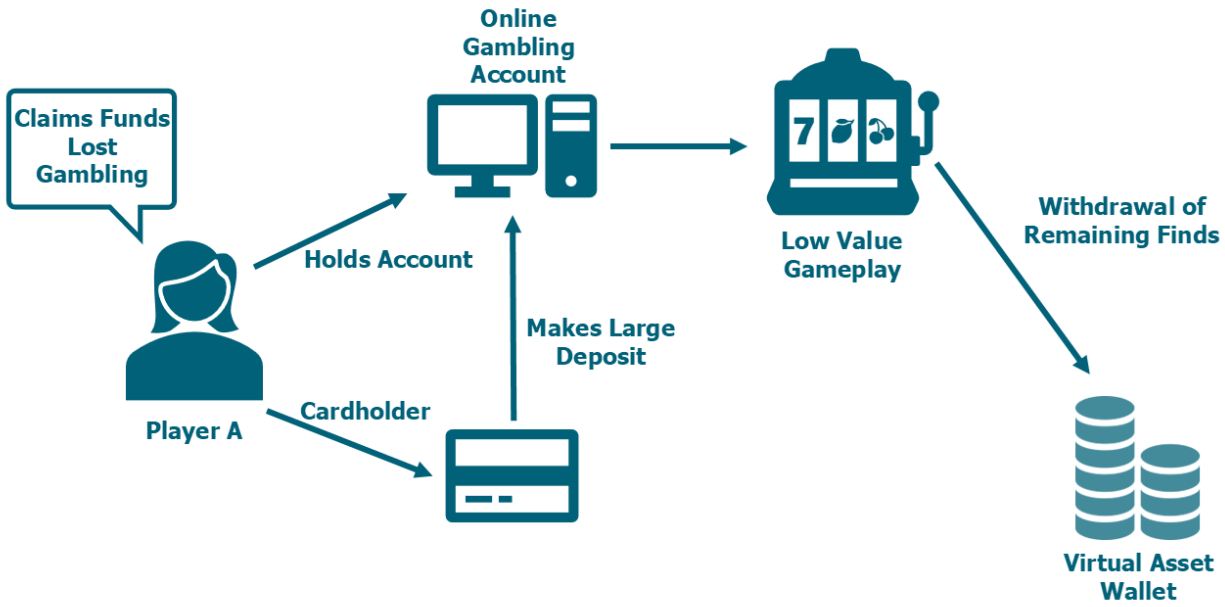


Red Flags

Repeated interaction between accounts, Unusual gameplay activity, Adverse Media, Terrorism links, Sanctioned entity

Disguising illegal spending

If a criminal wants to disguise the fact that they have spent money on an illicit enterprise (for example, paying a bribe), they may try to falsely claim that the money was lost in gambling. This is 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. The difference is that the criminal will seek to cash out their funds into a different bank account or in a different medium (like cryptocurrency). They can then show the money leaving their bank account but not re-entering and claim that the funds were all spent on losing bets.



Example:

Mr Grey had an account with Isle of Man licensed online gambling platform, Platform D. The account had only been used intermittently with low value deposits and low risk gameplay until Mr Grey made an uncharacteristically large deposit. He continued engaging in low-risk gameplay with a small proportion of this deposit, but before long he submitted a request to withdraw his funds. Although the deposit had been made using Mr Grey's debit card, he requested the withdrawn funds be sent to a digital wallet held with a payment service provider.

The support team at Platform D explained to Mr Grey that they were not able to sanction withdrawals via payment methods which differed from the one used to make the original deposit, and Mr Grey became irate in response. Concerned about his behaviour, Platform D's compliance team reviewed Mr Grey's client information, and noticed that his employment was listed as owner of a logging company. Open-source research revealed that Mr Grey's logging company operated primarily in a Southeast Asian country known for its high rate of environmental crime. The compliance team were concerned that Mr Grey may have been intending to use his account with Platform D to disguise bribe payments relating to his business, so they submitted a SAR to the FIU.

Red Flags

Uncharacteristic activity, Request to withdraw to an alternative source, Customer behaviour, Adverse media, High risk jurisdiction

Fraud

Bank card fraud

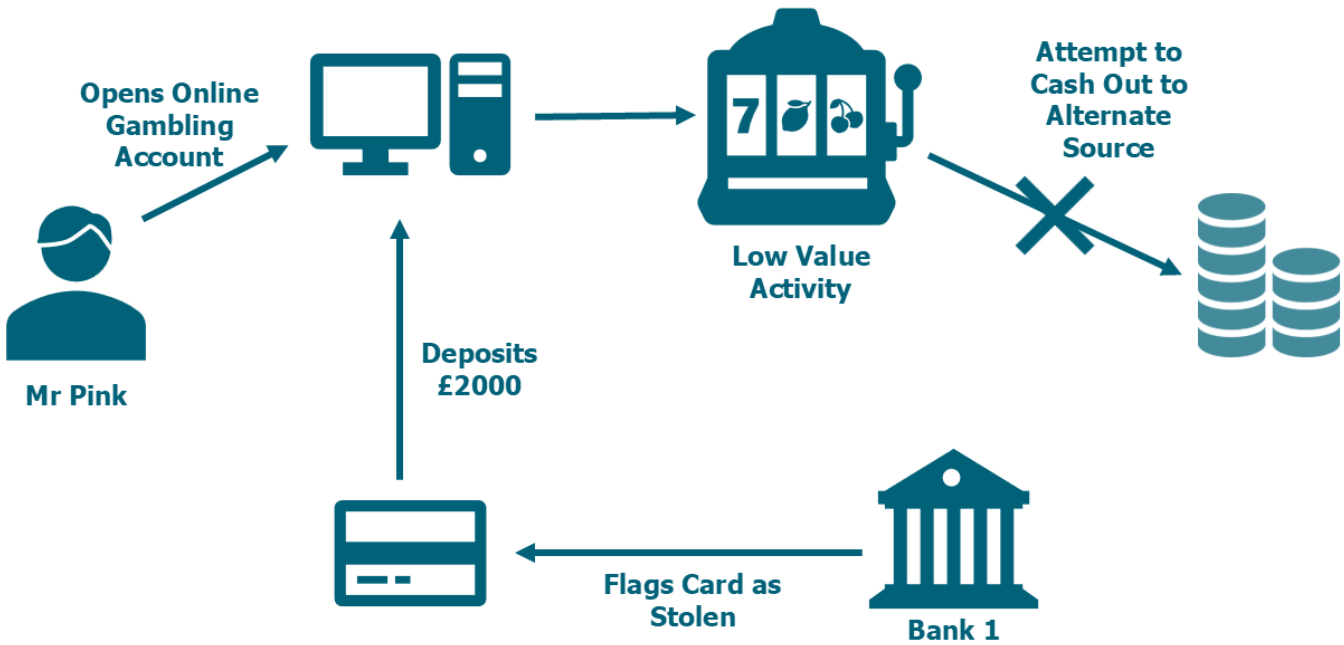
Criminals may use stolen bank cards or card details to credit online gambling accounts and then request that any balance or winnings are cashed out to their own bank account through a different payment method.

Alternatively, they may use their own bank cards to credit online gambling accounts which they have set up under fake or stolen identities. They can then claim to their bank that their card has been fraudulently used by someone else and request a refund from the bank.

Example:

Mr Pink opened an account with Isle of Man licensed online gambling platform, Platform E, and immediately deposited £2000 using a debit card. He placed two low value bets and then requested a funds withdrawal the next day. Mr Pink asked that the funds be sent by wire transfer rather than being returned to the debit card he had used to make the original deposit.

The support team at Platform E asked Mr Pink why he required the funds to be sent through a different payment method, but before they got a response, they were contacted by Bank 1 and told that the debit card used by Mr Pink had been reported as stolen. Platform E's support team immediately suspended Mr Pink's account and submitted a SAR to the FIU.



Red Flags

Withdrawal of deposited funds following minimal gameplay, Request to withdraw to an alternative source, Use of a stolen payment method

Sports fixing

Criminals who engage in sports fixing – rigging the outcome of a competition, like football or horseracing, to ensure a predetermined result – make money by betting on the competition's outcome. Online gambling platforms may be a particularly attractive tool for sports-fixing criminals because they can 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.

Example:

Miss Black, who lives in a North American country, has a cousin who plays professional ice hockey. The two had conspired to fix a game so that they could profit from betting on the outcome. Miss Black used fake names and forged documents to open 5 accounts with Isle of Man licensed sports betting platform, Platform F. Over a period of months, she used all 5 accounts to engage in occasional low value betting to give them an appearance of legitimacy. On the day of the match which she and her cousin had agreed to fix, Miss Black placed high value bets on each of her 5 accounts.

The compliance team at Platform F noticed the out of keeping high-value betting on these accounts. On further inspection, it became apparent that all 5 accounts had been logged onto from the same IP address and had each placed their suspicious bets within minutes of each other. Suspecting the possibility of match fixing, the compliance team submitted a SAR to the FIU.

Red Flags

Use of fake KYC documents, Accounts opened at the same time, Activity repeated between accounts, Multiple accounts with same IP address, Unusual gameplay activity

Use of Online Gambling Accounts: Red Flags and Risk Factors

- ⇒ Falsified identity documents or fake identities
- ⇒ Inconsistent information presented in due diligence checks
- ⇒ Multiple accounts using the same name or similar names, passwords, IP address, or credit cards
- ⇒ Customers in high-risk jurisdictions
- ⇒ Customers who are politically exposed persons (PEPs)
- ⇒ Adverse media concerning a customer
- ⇒ Logging on to the same account from different countries
- ⇒ Deposit values exceed expectations based on declared income, source of wealth, or financial situation
- ⇒ Minimal and low-risk gameplay before cashing out
- ⇒ Requesting withdrawals be sent to different accounts or through different payment methods than the original deposit (e.g. credit card deposit, wire transfer withdrawal)
- ⇒ Excessive deposits relative to the pattern of gambling
- ⇒ Large transfers of balances to other gambling accounts held in different names
- ⇒ Sudden changes in betting activity
- ⇒ Suspicious gameplay (e.g. irrational or potentially deliberate losing in peer-to-peer games)
- ⇒ Multiple deposits or withdrawals below the reporting threshold
- ⇒ Crypto wallets with exposure to both online gambling sites and tumblers, mixers, or darknet markets
- ⇒ Excessive transactions with online gambling sites
- ⇒ Payments into bank account from an online gambling account without any preceding payments out to the site
- ⇒ Bank transfers from unrelated third parties referencing terms related to gambling (e.g. online gambling site names)
- ⇒ Excessive use of prepaid cards
- ⇒ Circular activity in a bank account – money transferred out to online gambling sites, and similar volumes of money deposited back in from them

Beneficial Ownership of Online Gambling Businesses

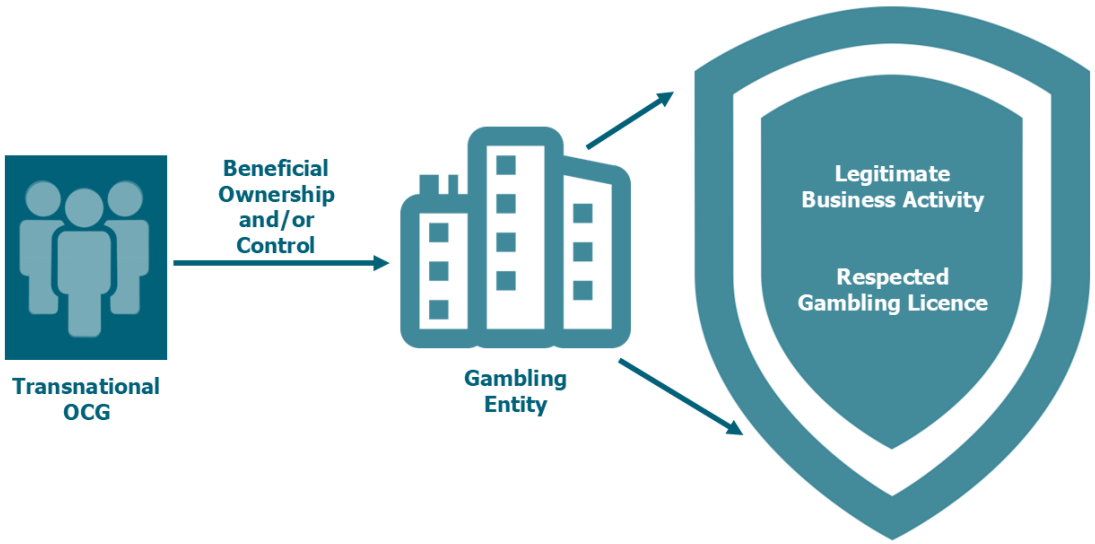
Money laundering as a service

If an online gambling business is under the control of an OCG then it can be operated as a professional ML enterprise.

An OCG which controls an online gambling platform can offer the use of its gambling accounts to other criminals for facilitating ML or underground banking. In exchange for a commission, they may allow criminals to move money freely on and off the platform, between accounts, across jurisdictions, through different payment methods, and between account holders. When the illicit funds are withdrawn from the platform the OCG may offer 'proof' of winnings documentation to increase the appearance of legitimacy and further assist the integration of criminal proceeds into the formal economy. If the client for whom the OCG is performing this ML service is in a jurisdiction where gambling is prohibited, the OCG can change the description in the documentation so that the money appears to be from a different source, e.g. returns from an investment platform.

The prevalence of these operations has risen because of the increasing availability of off-the-shelf gambling technology packages - it has become easier for criminal actors to establish online gambling businesses with very limited technological understanding or industry experience. They are particularly widespread in unregulated or under-regulated Southeast Asian jurisdictions which lack stringent AML/CFT controls for gambling. However, they have also been found in well-regulated jurisdictions. An OCG may choose to trade-off a higher risk of regulatory scrutiny for the advantage of having an offshore license from a reputable jurisdiction like the Isle of Man, because the appearance of legitimacy conferred by a license can make their ML services more effective.

It is important to bear in mind that OCGs running online gambling platforms as professional ML services may cover their tracks by combining their nefarious activities with legitimate business operations. Criminally controlled businesses which also maintain functional online gambling platforms with a legitimate customer base may be very difficult to identify. These operations are able to efficiently launder enormous volumes of illicit funds, as well as helping criminals to circumvent controls preventing TF and sanctions evasion.



Example 1:

An Isle of Man registered company, Blue Company, opened an account with a bank in the Isle of Man. Blue Company owned a newly established online gambling operator which was licensed and operating in South America. Blue Company explained to the bank that the source of funds for the account would be profits generated by the online gambling operator, which went live just a few months ago.

Six months after Blue Company opened the account, the bank noticed that the volume of funds entering the account was far greater than they had anticipated. The bank thought it was suspicious that a newly established online gambling operator would be performing so well within its first year of business, so they submitted a SAR to the FIU. The FIU made enquiries with the South American jurisdiction where the online gambling operator was licensed and discovered that the operator was under investigation for offering ML services to OCGs in the area.

Red Flags

Account activity outside of expectations, Newly established entity and account receiving large volume of funds

Example 2:

An Isle of Man tax adviser was contracted to provide advice to an Isle of Man registered company and OGRA full licence holder, Yellow Firm. Yellow Firm had been active for two years, conducting B2C activities in East Asian markets. When the tax adviser first looked at Yellow Firm's financial statements, she noticed that the business' revenue was very high. The Firm's directors explained that online gambling is extremely popular in the markets they target, and that their marketing tactics were well tailored to recruiting new customers from these regions.

The tax adviser became concerned when she could not find any invoices relating to marketing expenses in the business' accounts. She checked the Firm's online gambling site and saw that it was unsophisticated, lacked functionality, and only offered a very limited range of casino game options. Having recently read an open-source report about criminal misuse of online gambling businesses, the tax adviser knew that this lack of strong online presence was a red flag. The tax adviser had developed a suspicion that Yellow Firm was being used as a front to launder criminal proceeds, and she submitted a SAR to the FIU.

Red Flags

Higher risk jurisdiction, Income outside of expectations, Client contact contradicts accounts, Unsophisticated gaming website with limited functionality

Declaring criminal proceeds as business profits

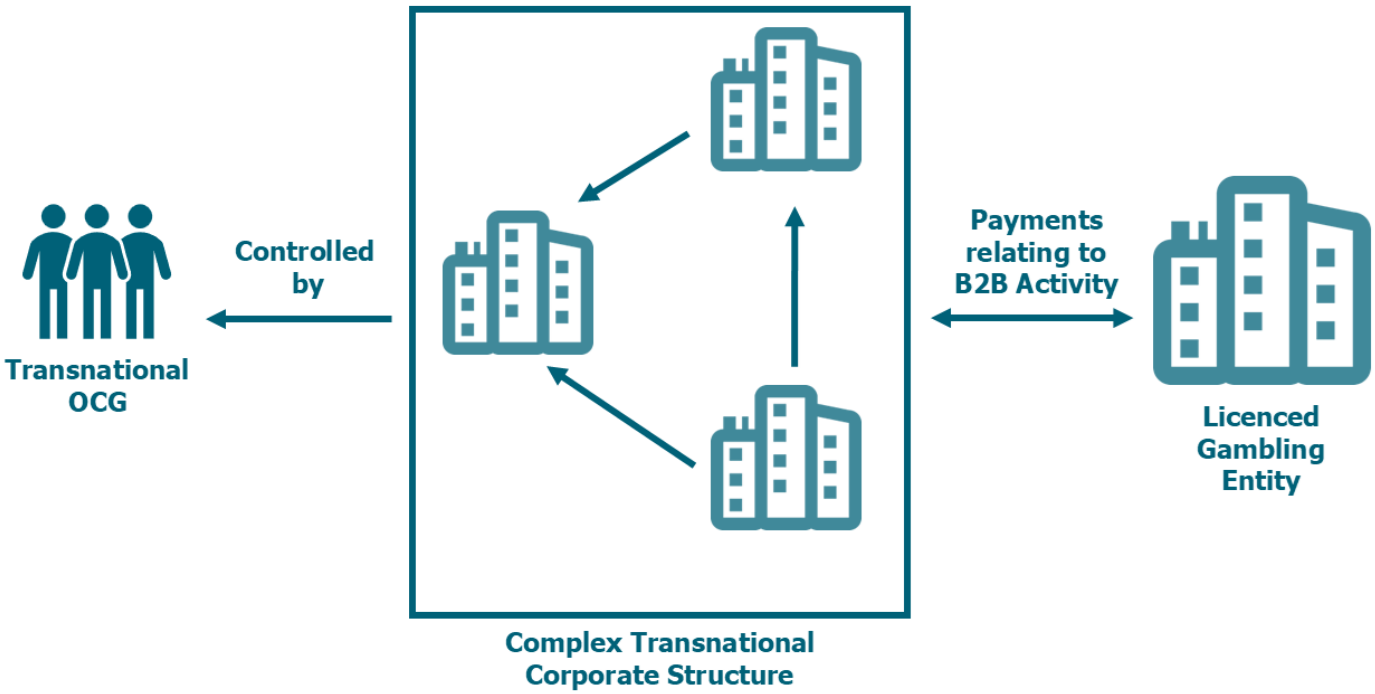
An OCG which owns an online gambling business can launder a very large volume of criminal proceeds by passing the money off as profits of the business itself. Online gambling businesses can generate enormous revenues, and they do so with an intangible product that is consumed internationally. This makes them well placed to provide a convenient explanation for large inflows of money which pass through different jurisdictions.

An OCG may choose to establish their online gambling business in a reputable jurisdiction with a well-regarded licensing regime, because the appearance of legitimacy can make it easier to integrate their criminal proceeds into the formal economy at the end of the laundering process. Once established, they can use the business to disguise illicit funds as legitimate profits in a variety of ways - the most efficient methods involve spurious business-to-business (B2B) arrangements.

Establishing sham business relationships between different criminally controlled corporate entities can legitimise the movement of large sums of money across international borders. These sham relationships might involve any type of B2B activity which can be carried out remotely and justify high-value transfers of money, for example revenue sharing agreements, service arrangements, or software sales and licensing contracts.

Large transnational OCGs may own a range of other corporate entities spread across different jurisdictions, including white label gambling operators, marketing companies, payment service providers, and cryptocurrency exchanges. OCGs can obscure the beneficial ownership of these entities using complex trust and corporate structures, proxies and nominee directors, and layers of ownership which span multiple jurisdictions (particularly jurisdictions which offer greater financial secrecy). Wealthy criminals can further disguise their ownership of assets by exploiting citizenship through investment schemes to obtain second (or 'golden') passports under different names.

The layers of complexity and obfuscation that OCGs introduce into these transnational corporate structures can make the task of client due diligence very challenging. OCGs will go to extensive lengths to obscure the business structure and ultimate beneficial ownership of these criminal enterprises. Each of these criminally controlled corporate entities, including the online gambling business itself, may or may not conduct legitimate business alongside their intended ML purposes.

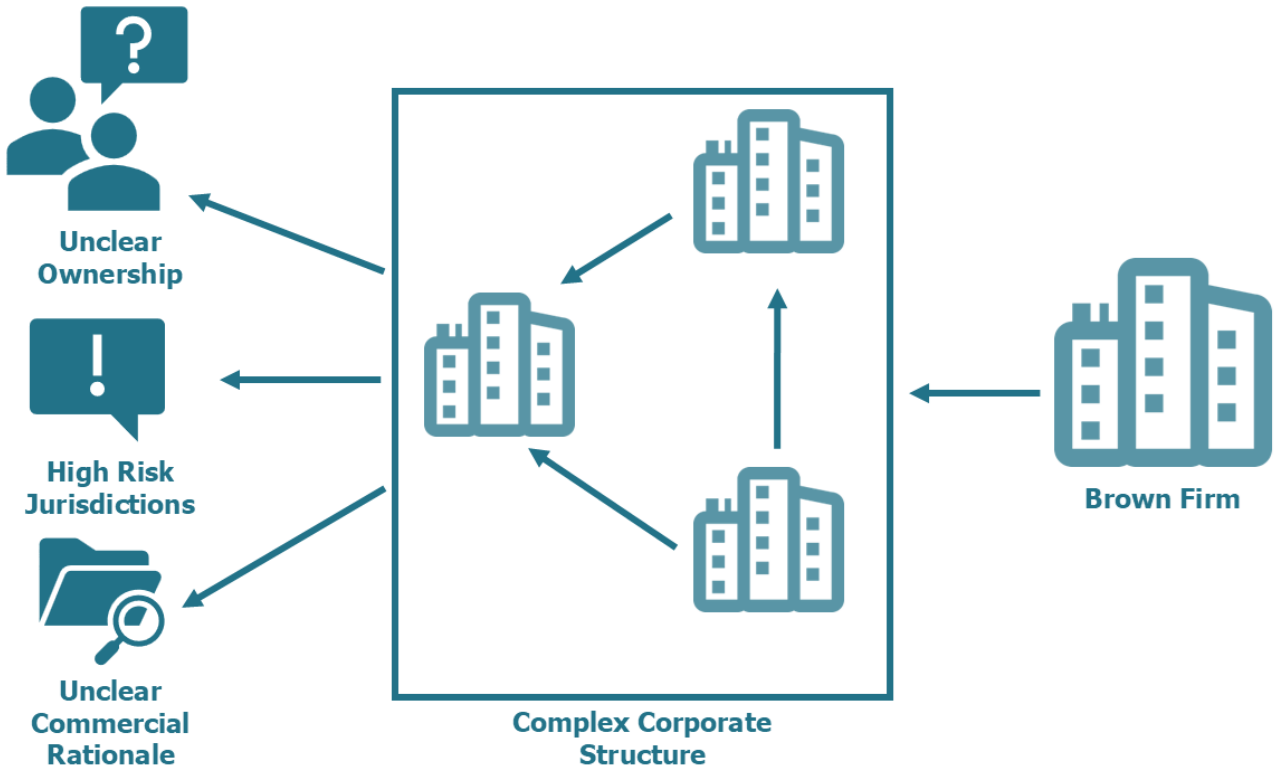


Example 1:

An Isle of Man trust and corporate service provider (TCSP) was approached by Isle of Man registered company, Brown Firm. Brown Firm wanted the TCSP's help in applying for an OGRA software supply licence. In the course of reviewing Brown Firm's business proposal, a number of red flags became apparent to the TCSP.

Brown Firm appeared to be part of a wider group of companies with a complex structure which spanned multiple high-risk jurisdictions. The ownership of the other companies in this group was difficult to determine, and the commercial rationale for the B2B relationships between them was unclear. Furthermore, although Brown Firm described themselves as a cutting-edge gambling software development company, they had a very limited online presence – their website was very simple and lacking in content.

Brown Firm's directors were pushy with the TCSP about the speed of the application process and did not cooperate readily when the TCSPs requested further information to clarify points of concern in their business proposal. The TCSP declined Brown Firm's business and submitted a SAR to the FIU.



Red Flags

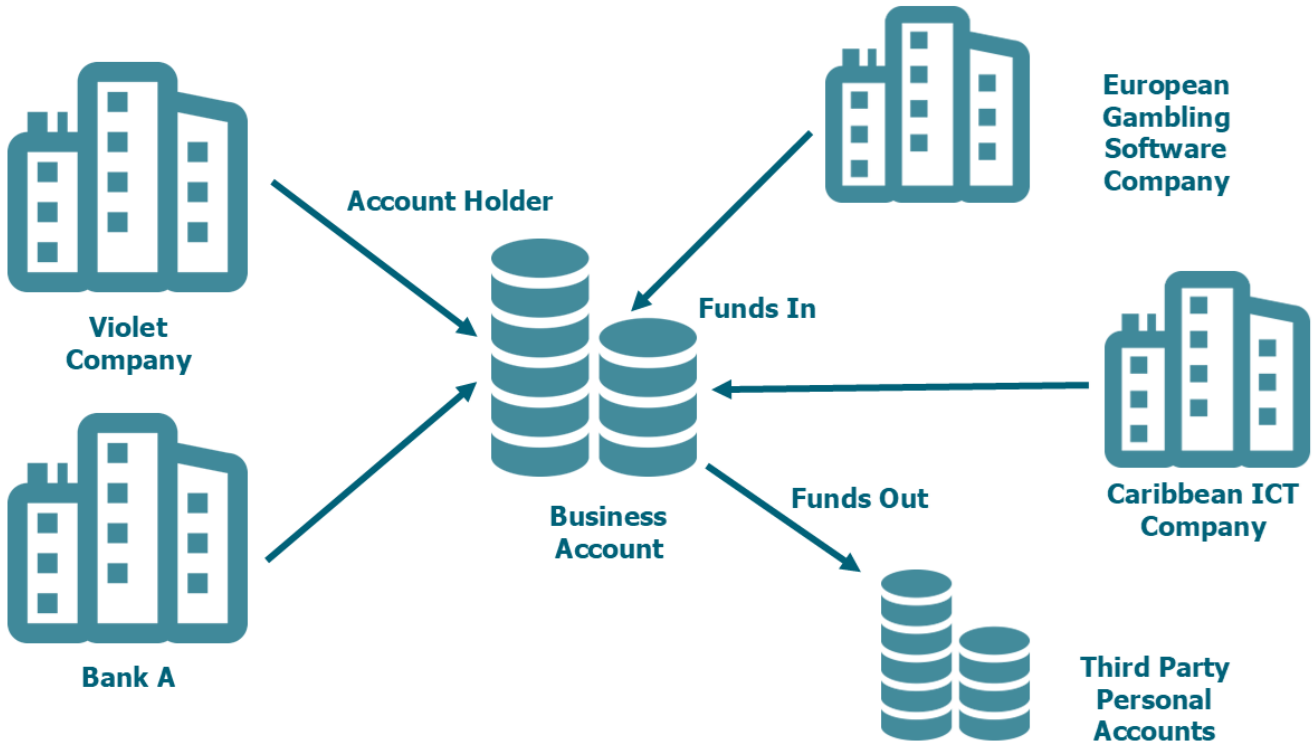
Use of complex structures, High risk jurisdictions, Opaque beneficial ownership, Unclear commercial rationale, Unsophisticated gaming website with limited functionality, Customer behaviour, Reluctance to provide KYC

Example 2:

Violet Company, an Isle of Man registered company operating as a marketing business, held a commercial account with a bank in the Isle of Man. When the account was established, Violet Company had told the bank that they specialised in fashion marketing, and that the account would primarily be used to receive invoice payments from clients.

An internal SAR was raised to the bank's compliance team because Violet Company's account had been receiving incoming payments from a number of companies which were not in keeping with the Violet Company's stated nature of business. These other companies included a gambling software distributor registered in a European jurisdiction, and an ICT consultancy registered in a Caribbean jurisdiction. There had also been several outbound transactions from Violet Company's account to apparently unrelated personal bank accounts in an Australasian jurisdiction.

Concerned that there was no obvious commercial sense to these transactions, the bank's compliance team contacted the directors of Violet Company to request additional information. It took several weeks and a number of chasers before the bank received a response to their query. Violet Company claimed that the company was in the process of changing its business focus to bring in a wider range of clients, but their reply to the bank's compliance team was short and lacking in detail. The compliance team suspected that Violet Company's account was being used to launder the proceeds of organised crime, and they submitted a SAR to the FIU.



Red Flags

Account activity outside of expectations, Unclear commercial rationale, Unexplained payments to third-party personal accounts, Inadequate rationale from customer

Online gambling as a front for cyber-enabled fraud operations

Over recent years, international law enforcement agencies have noticed a growing trend in the use of online gambling businesses as fronts for large cyber-enabled fraud (CEF) operations. Pig-butchering (a combination romance-and-investment scam) has gained a great deal of media attention, but there are many other scam techniques in use including job scams, loan scams, law enforcement impersonation, and dummy gambling platforms which allow fraudsters to control the outcome of bets placed.

Online gambling and CEF have a number of overlapping requirements for technology and human resources – much of the equipment and knowledge needed to operate a successful online gambling platform can also be used to carry out online scamming operations. An online gambling business is a useful front for CEF activities because it provides both a plausible explanation for the infrastructure being used and a way of laundering the proceeds being generated. 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.

This trend began in parts of Southeast Asia where existing online gambling operations, run from casino complexes under the control of OGCs, were repurposed for CEF to supplement criminal revenue during the Coronavirus pandemic lockdowns. Vast scam centres in areas like Myanmar, Cambodia, and Lao rely on victims of human trafficking to conduct online scams and generate enormous volumes of criminal proceeds. There is now increasing evidence that this trend is globalising, and it is important to bear in mind that these CEF fraud operations could be conducted in any jurisdiction.

Example 1:

An Isle of Man TCSP was approached by Mr Beige, the beneficial owner of Isle of Man registered company, Puce Firm. Mr Beige was intending to apply for an OGRA network licence for Puce Firm, and he asked the TCSP to assist with the application process. Mr Beige explained that his business plan for Puce Firm was to form network partnerships with B2C online gambling operators in Southeast Asia. The TCSP had initial concerns about the proposition because Mr Beige's employment history showed no experience in the gambling industry.

On reviewing Mr Beige's proposal, the TCSP developed further concerns about the source of funds to be used in establishing Puce Firm's business. Mr Beige claimed that he had sufficient wealth to fund Puce Firm's initial development, and that he had accrued his wealth from property development projects in an emerging economy. The TCSP noticed that Mr Beige had supplied very little information to corroborate his source of wealth - when they requested more information they were met with resistance.

The TCSP undertook open-source media searches as part of their due diligence process and discovered negative media linking Mr Beige to a prominent member of a well-known East Asian OCG. There were photographs showing Mr Beige with the OCG member at the opening of a casino complex which was widely reported to be hosting a cyber fraud forced labour scam -camp. The TCSP declined Mr Beige's business and submitted a SAR to the FIU.

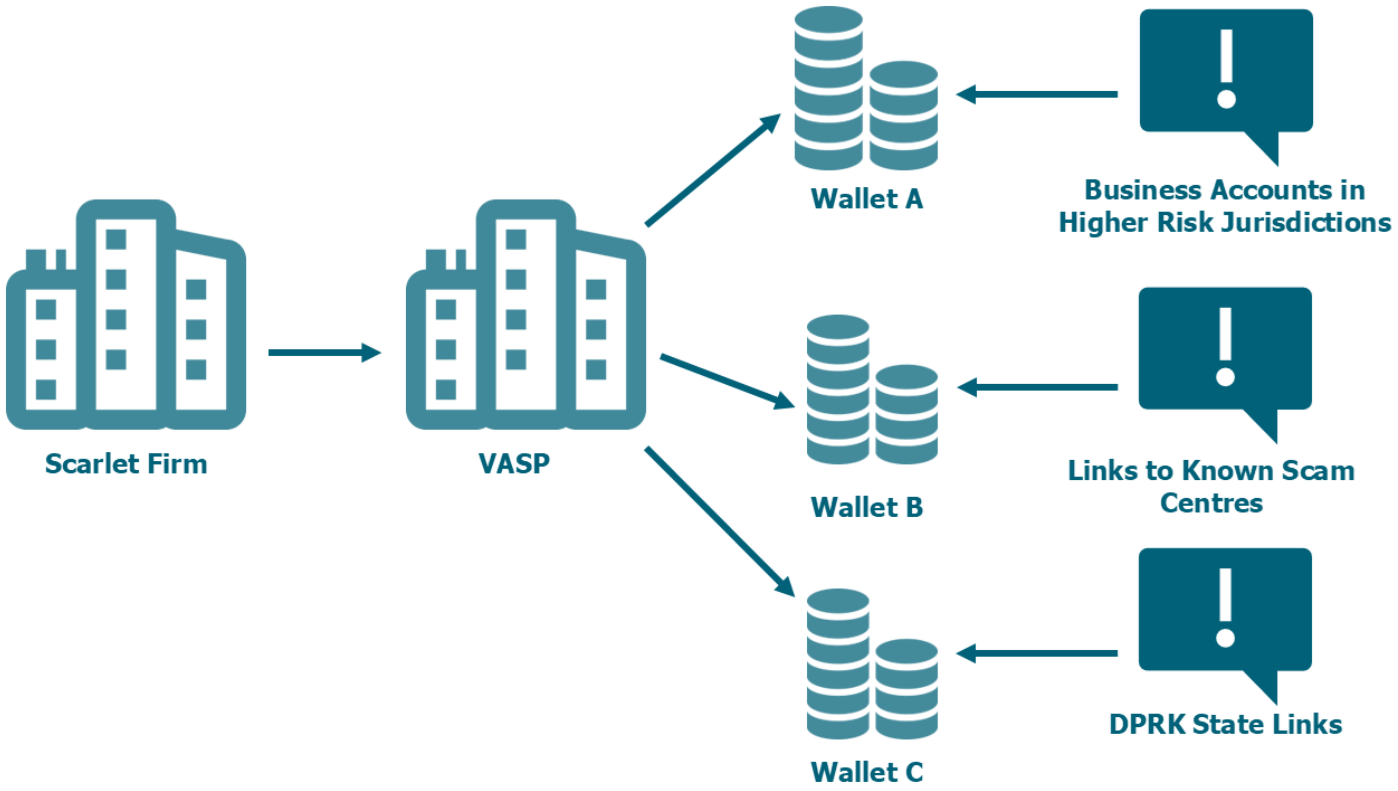
Red Flags

Higher risk jurisdictions, Unclear commercial rationale, Insufficient source of wealth documentation, Adverse media

Example 2:

A virtual asset service provider (VASP) operating in a European jurisdiction acquired another business' customer base, prompting a review of all novated accounts. During this review, the VASP developed concerns about a business account held by Scarlet Firm, a B2C online gambling provider licensed in the Isle of Man.

According to their onboarding documents, Scarlet Firm's account was established to receive funds from customers who were gambling in cryptocurrency. A review of their account activity, however, showed that Scarlet Firm had only been receiving funds from other business accounts. Specifically, Scarlet Firm had been receiving transfers from a cluster of companies spread across Southeast and Central Asia. Because this activity was not in keeping with the declared nature and purpose of the account, the VASP's compliance team undertook a detailed analysis of the account's transaction history. The compliance team's blockchain analysis software flagged several transactions as having links to wallets associated with cyberfraud activities in known scam centres. Even more concerning, another transaction was flagged as having links to an address associated with a DPRK state-sponsored hacking group. Because this transaction had passed through Garantex, an EU sanctioned cryptocurrency exchange, the VASP submitted a SAR to their regional FIU reporting the suspected sanctions breach. They also detailed their wider suspicions about Scarlet Firm laundering criminal proceeds and potentially facilitating PF. The European FIU shared this intelligence with the Isle of Man FIU.



Red Flags

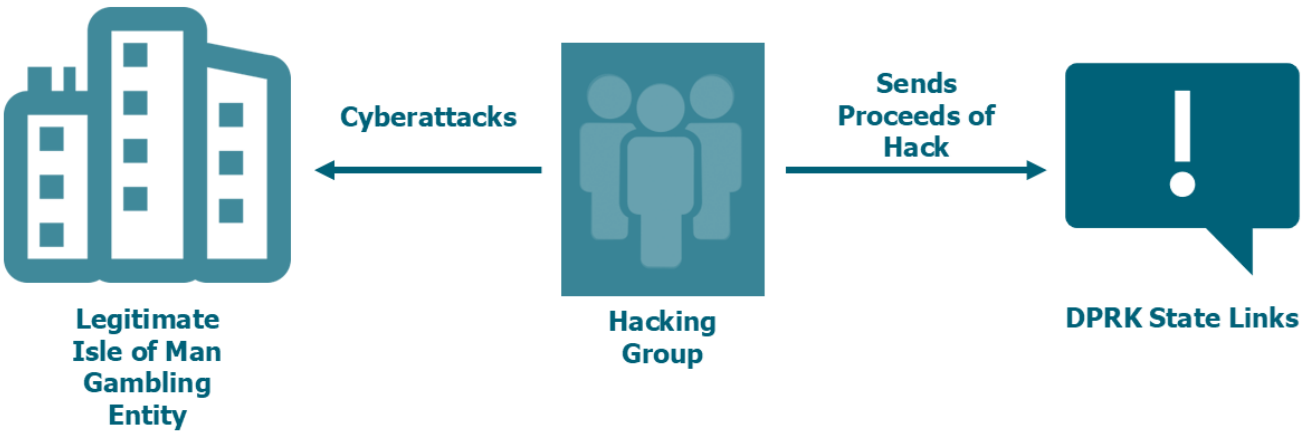
Account activity outside of expectations, Higher risk jurisdictions, Transactions linked to known scam centres, Links to sanctioned jurisdiction, Proliferation financing links

Beneficial Ownership of Online Gambling Businesses: Red Flags and Risk Factors

- ⇒ Business proposals or OGRA licence applications from people with a lack of experience in the industry and/or lack of technical expertise
- ⇒ Golden passports (particularly where the holder's name differs from their original passport)
- ⇒ Opaque or unexplained source of funds or wealth – pushback against attempts to clarify
- ⇒ Using nominees as company directors and trustees
- ⇒ Adverse media
- ⇒ Beneficial owners or business structures linked to countries listed in the Cabinet Office's National Risk Appetite document (published May 2025)
- ⇒ Newly incorporated network partners
- ⇒ Network partners incorporated in jurisdictions listed in the Cabinet Office's National Risk Appetite document (published May 2025), or otherwise known to have poor AML controls
- ⇒ Gambling businesses with limited online presence or unsophisticated websites
- ⇒ Online gambling operators which frequently change URLs
- ⇒ Inconsistencies or unexplained changes in business proposals and licence applications
- ⇒ Business profits out of line with expectations (e.g. new business or unsophisticated platforms generating much higher income than anticipated)
- ⇒ Changes in planned operating models with little planning or notice (e.g. switching from B2C to B2B, or from B2C to software supply)
- ⇒ B2C business reluctant to allow auditors or regulators access to their back-office suite
- ⇒ Complex B2B arrangements and relationships
- ⇒ Complex trust or company structures which cross multiple jurisdictions
- ⇒ B2B relationships which lack a coherent rationale
- ⇒ Commercially questionable business activity (e.g. purchasing other businesses at inflated prices)
- ⇒ B2B relationships with online gambling operators active in un- or under-regulated jurisdictions
- ⇒ B2B payments in cryptocurrency
- ⇒ B2B payments through money transmission services, particularly when doing so is commercially questionable (higher cost than bank-to-bank transfers)
- ⇒ Complex or commercially questionable business banking arrangements

Hacking and Theft

There have been instances of cyber-criminals stealing cryptocurrency from blockchain addresses controlled by online gambling businesses. In at least one instance, the criminals concerned were acting on behalf of the DPRK[3], a regime which has become increasingly reliant on cybercrime to circumvent sanctions and pursue its weapons programme. The threat of direct theft from online gambling platform accounts or blockchain addresses therefore carries an elevated PF risk. It is important for crypto-enabled online gambling businesses to minimise this risk through investment in appropriate ICT security.



3. FBI press release: FBI Identifies Lazarus Group Cyber Actors as Responsible for Theft of $41 Million from Stake.com

Glossary

ML – Money laundering

TF – Terrorism financing

PF – Proliferation financing

AML – Anti money laundering

CFT – Countering the financing of terrorism

GSC – Gambling Supervision Commission

OGRA – Online Gambling Regulation Act (2001)

SAR – Suspicious activity report

OCG – Organised criminal group

CEF - Cyber-enabled fraud

B2B – business-to-business

B2C – business-to-customer

PEP – Politically exposed person

P2P – peer-to-peer

Resources and Links

- ⇒ GSC AML/CFT Guidance
- ⇒ Isle of Man FIU Guidance Documents
- ⇒ MONEYVAL Research Report: The use of online gambling for money laundering and the financing of terrorism purposes
- ⇒ FINTRAC: Special Bulletin on laundering the proceeds of crime through online gambling sites
- ⇒ RUSI Emerging Insights: North Korean Activity in the Casino and Gaming Sector
- ⇒ FATF Report: Vulnerabilities of Casinos and Gaming Sector
- ⇒ UNODC: Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat
- ⇒ UNODC: Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape