GSC
GAMBLING

AML/CFT Guidance for Virtual Assets/Goods

V1.3 (April 2024)

Contents

This version of the guidance is effective from April 2024

Version Control

Version	Date Published	Comments
1.0	11/01/2018	Supplementary AML/CFT guidance for virtual currencies and virtual goods
1.1	N/A	Draft changes circulated to AML Forum for comments 25/11/2020
1.2	Dec 2020	Replaces the 2018 supplementary guidance, including references to - GSC's AML/CFT Guidance - Latest FATF Guidance - Blockchain analysis tools
1.3	April 2024	Formatting and general updates in line with new branding and stakeholder consultation feedback

1.0 GENERAL

1.1 Abbreviations and Definitions

AML/CFT	Anti-money laundering and Countering the Financing of Terrorism (also incorporates countering proliferation financing)
AML Guidance	AML/CFT Guidance for Gambling Operators
FATF	The Financial Action Task Force
Fiat currency	"Real currency", "real money" or "national currency" is the coin and paper money of a country that is designated as legal tender.
FT	Financing of Terrorism
GSC	The Gambling Supervision Commission which includes the Board of Commissioners and the Inspectorate
IOM	Isle of Man
IOMFSA	Isle of Man Financial Services Authority
ML	Money Laundering
MONEYVAL	The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
Operator	A holder of a licence issued under the Isle of Man Online Gambling Act
Peel Chains	A method of moving stolen crypto funds where typically a wallet with a large amount of currency is "peeled" into smaller and smaller amounts over many wallets.
PF	Proliferation Financing – providing funds or financial services that in some way assist the manufacture, acquisition, possession, development, transport, export etc of nuclear, chemical, biological or radiological weapons
The Code	The Gambling (Anti-Money Laundering and Countering the Financing of Terrorism Code 2019
Virtual Asset (VA)	Digital methods of payment or investment for instance Crypto-currency e.g. Bitcoin, Ethereum. Previously referred to as convertible virtual currency.
Virtual Goods (VG)	Includes virtual goods on the blockchain that are collectibles such as NFTs that do not meet the definition of a VA and also non-blockchain goods such as digital "skins" or in game currencies. Previously referred to as non-convertible virtual currency.
Virtual asset account	Means an account held in the name of one or more customers which is or may be used for storing, sending or receiving virtual assets
Virtual Asset Service Provider activity (VASP)	Means any natural or legal person who **by way of business** conducts exchange, transfer, safekeeping or administration or financial services in relation to sales of VA of VG.

1.2 About This Document

This document has been prepared by the Gambling Supervision Commission (GSC) and is intended to be read alongside the existing Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Guidance found here.

This document provides guidance on AML/CFT matters relating to virtual assets and goods only and does not cover other matters such as fund protection or problem gambling. The guidance is intended to provide licence holders with an overview of the AML/CFT risks in VA and VGs and illustrate areas where further controls can enhance risk based AML/CFT frameworks to ensure that controls are in place to detect and prevent illicit flows of funds and safeguard the reputation of the licence holder, the sector and the licensing regime.

If an operator wishes to accept VA deposits, either directly or facilitated by a PSP or exchange then an operator is required to notify the GSC to seek permission. An operator that facilitates VA deposits will be issued with an additional licence condition requiring compliance with policy GSC85. Permitted models of VA and VG use are outlined in Section 3.4 in this document, the GSC do not permit exchange between VA and Fiat currencies, or VA and VA.

This guidance applies to licence holders that—

- Accept transactions in any type of either virtual asset or virtual goods
- Utilise blockchain based products and services
- Offer in-house virtual goods such as digital skins or in game items
- **This guidance can also apply to operators that do not accept VA deposits but are aware of a link between a customer and VA use. For instance where VA is provided a source of wealth or is known to be source of funds prior to deposit.**

Throughout this document you will find AML/CFT guidance, models and key messages to assist with applying appropriate risk based AML/CFT controls. The contents of this guidance should not be construed as legal advice.

1.3 About the GSC

The GSC is responsible for regulatory oversight of the gambling sector including licence holders' compliance with legislation such as the Gambling Acts and the Code. The GSC is an independent statutory board of Tynwald and comprises the Inspectorate and the board of the Commission.

The board of the Commission consists of several independent members drawn from various professions and backgrounds. The board of the Commission conduct monthly hearings into all matters that pertain to gambling in the IOM supported by the Inspectorate.

A list of the current Commission Members and Meeting Dates can be found here.

The Inspectorate is managed by the Chief Executive of the GSC. The Inspectorate supervises compliance through a combination of self-assessments and on-site reviews that make up an inspection and this allows the GSC to assess a licence holder's policy framework and processes.

The Commission also participates in national initiatives to continually assess the risk of ML and terrorist financing within the gambling sector as well as evaluation exercises, conducted by

external teams of assessors, which check the IOM's national commitment and performance against international standards.

The GSC is available 9:00am to 5:00pm Monday to Friday and can be contacted via phone on +44 (0)1624 694331, via e-mail on gscamlinspections@gov.im or at the postal address below—

Ground Floor
St. George's Court
Myrtle Street
Douglas
Isle of Man
IM1 1ED

For more information about the GSC, its structure and its statutory functions, please visit the GSC's website https://www.gov.im/about-the-government/statutory-boards/gambling-supervision-commission/.

1.3.1 Supervision

The GSC has produced guidance on its Supervision Visit Procedures (which includes AML/CFT Supervision) which can be found here.

Supervision is carried out using a risk based approach, all licensed entities are subject to regular inspections, the cycle being informed by both—

- Inherent risks factors that do not changes as often such as type of business model, products offered, customer risks
- Dynamic risks – factors that can change such as compliance history.

Inspections will primarily focus on the period between either licensing, or the date of the previous inspection where relevant, and the beginning of the current inspection. This guidance provides an overview of the additional factors that may be examined during an inspection where VA or VG use is present.

An AML inspection is split into three distinct stages—

- Desk-top Review – A licence holder will be asked to provide pre-visit documentation which generally includes relevant policies and procedures, training logs etc and a date for an onsite visit will be agreed. The GSC will also review supervisory information provided during the period to be supervised such as quarterly and annual returns.
- During this period licence holders will be required to fill in and return a self-assessment template to establish their AML framework in order to test the framework during the onsite portion of the Inspection. Self-assessment templates are provided upon licensing to allow licence holders time to familiarise themselves with the requirements fully and identify any issues prior to any inspection beginning. Where these have already been provided to the GSC an update will be requested.
- Onsite – The AML/CFT team will, accompanied by the lead general inspector for the licence holder, visit a licence holder's premises in person to look at the effectiveness of the mechanisms reported under the self-assessment and through the pre-visit documents. For Software Suppliers this will be in the form of a business meeting to discuss any points raised in the desk top review. An onsite matrix will be used to ask

standard format questions however these are tailored to the business model and are informed by the desk top review findings.

- Post Onsite Review & Report – following the onsite the AML/CFT team will request any further outstanding documents and issue a report covering both technical findings from the self-assessment and practical findings from the onsite. Following a draft report being issued the AML/CFT team will issue a final report at which point the Inspection is concluded.

Following supervision the results of any compliance findings are fed back into the ongoing risk assessment process to determine the frequency of ongoing inspections. Lower risk and/or more compliant licence holders being visited with less frequency and conversely multiple compliance failings will result in higher risk ratings and more frequent inspections.

Where the outcomes of any inspection includes remedial actions these will be monitored for completion and follow up visits may be more targeted to these areas. Compliance failings that meet the criteria for enforcement, for instance they are widespread, deliberate, material in nature, repeated etc will result in an escalation to the Enforcement Team for consideration and more information can be found in the Enforcement Strategy outlined on page 5 of the GSC Guidance on the Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Act 2018.

Note: the IOMFSA oversees AML/CFT compliance for businesses that are classed as Virtual Asset Service Providers (VASPs) the GSC does not dual supervise these types of business. Guidance on VASPs can be found on the IOMFSA website, https://www.iomfsa.im/media/2688/sector-guidance-virtual-assets.pdf.

2.0 Background

2.1 Regulatory Changes to Allow Acceptance of Money's Worth

The Online Gambling (Amendments) Regulations 2016 made changes to the Online Gambling (Registration and Account) Regulations 2008 to allow operators to accept deposits in money or money's worth. This can include VAs and VGs previously defined in guidance as CVCs and VCs respectively.

In order to provide a flexible approach to the rapid growth and development in the use of VA/VGs and the use of blockchain technology, the GSC's approach to dealing with VA/VGs is set out in policy, guidance and licence conditions which may be changed from time to time as the technology matures.

2.2 Isle of Man National Risk Assessment

The National Risk Assessment (NRA) was first published in 2015 and was updated in 2020, stating that—

"The VA sector is rapidly evolving; it is also complex, the level of regulatory (and investigatory) expertise in the field is limited and it is a challenge to keep up with developments. This inevitably leads to a degree of reliance on industry experts in the IoM as elsewhere, which brings its own advantages and disadvantages. The sector has some risks which are specific and some which are similar to those shared with other DNFBPs."

Risks identified in the NRA are:

- Level of anonymity available which is greater than traditional non-cash methods and difficulty in linking an 'account' to a real identity
- Non face-to-face business relationships; typically traded on the internet
- May permit anonymous funding and anonymous transfers if sender and recipient are not adequately identified
- The opaqueness of activities/transactions
- Cross-border exposure
- VAs facilitate a wide range of financial activities and allow for quick movement of funds
- High level of separation from the mainstream regulated financial sector
- Non-centralised 'accounts' which can be opened without CDD checks
- Potential use of anonymity software such as coin mixers and IP mixers
- Difficulties in establishing source of funds and source of wealth
- Quick and cheap global payments without ability to "chargeback"
- Lack of AML/CFT controls and clarity for VA/VG compliance, oversight and enforcement in many jurisdictions where transactions are segmented across several countries
- The rapidly evolving nature of VA related technologies requires high-level specific knowledge and expertise within the regulatory sector which may potentially be lacking
- The volatility of VA values and limitation of availability may be problematic to VA based businesses. Specifically for the gambling industry, this may be an issue when

it comes to paying out winnings, the value of which having increased significantly from when a bet is first placed. Additionally, it is a requirement for the value of all player funds held on a gambling platform to be matched by the operator, which may be difficult to do should the value of a VA significantly increase or the VA become unavailable.

2.3 Definitions

In order to align with legislative changes this guidance introduces new terminology for virtual assets and virtual goods however the descriptors remain the same. The table below provides an explanation of the changes—

Previous Terminology	Current Terminology	Description
Convertible Virtual Currency (CVC)	Virtual Asset (VA)	• A virtual asset is a digital representation of value that can be traded, transferred and used for payment or investment purposes for instance cryptocurrencies such as Bitcoin or Ethereum. • It is often not unique. • It does not include digital representations of fiat currencies and other financial assets.
Non-Convertible Virtual Currency (VC)	Virtual Goods (VG)	• A virtual good is not **broadly** used as a method of payment however could be traded or sold. • Its primary use is a digital representation of a collectible item or for use within a limited eco-system for instance NFT[1]s, skins, game gold etc • It may have a unique aspect and will not be readily interchangeable with another asset.

Where a virtual token, good or asset does not clearly fit into either definition the GSC reserve the right to determine the status of anything utilised for "money's worth" for the purpose of licensing and supervision.

[1] NFTs may be considered VA where they are deemed fungible and not unique.

3.0 Inherent AML/CFT Risk

3.1 Summary of Inherent AML/CFT risk

The GSC considers that transactions made in VA may represent a higher risk than transactions conducted using traditional non-cash payment methods such as debit card, bank transfer or through regulated payment service providers.

The IOMFSA provides detailed guidance on the AML/CFT risks associated to businesses that provide money service business style products in relation to VA summarised the as follows—

- Non face-to-face business relationships
- Non-centralised "virtual asset accounts" may be opened by anyone without customer due diligence checks
- Difficulty in linking a "virtual asset account" to a real world identity
- Lack of expertise to deal with new and rapidly developing technologies
- Potential use of anonymity software such as coin mixers and IP mixers
- Difficulties in establishing source of funds and source of wealth
- Quick and cheap global payments without ability to "chargeback"
- Lack of AML/CFT controls for virtual assets in most jurisdictions.

FATF has gathered together global case studies to inform a report on red flag indicators of ML/FT/PF that highlights the risks described above. The report should be considered in conjunction with the GSC's AML/CFT Guidance when dealing with virtual assets and VASP activity.

3.2 Examples of AML/CFT Red flags

The list below gives an outline of red flags that may indicate ML/TF/PF. Most will be familiar to AML/CFT professionals however those flags where any type of exchange or facilitating movement of funds should be especially monitored where there is a use of VA/VG.

- Structuring payments to be under the AML/CFT thresholds
- Unusual transaction patterns
- Multiple high value transactions in a short period
- Staggered regular pattern then no transactions for a long time after (ransomware cases)
- Deposit and withdrawal with no or little activity
- Use of new or previously inactive accounts
- Account use not in line with the customer's known profile
- Depositing and transferring to a jurisdiction with low AML/CFT controls
- Wallet addresses linked to fraud or mixer/tumbler use
- Multiple VA use or multiple accounts with no logical reason
- Converting a large amount of Fiat into VAs or a large amount of VAs into other VAs before deposit with no logical reason
- Anonymity and layering behaviour noted privacy coins or wallets (See 3.3 Analytics)
- Analytics shows more than limited exposure to illicit sources (See 3.3 Analytics)

- Transactions that incur unnecessary or very large fees
- Use of unregulated peer to peer exchange mechanisms such as DeFi
- Adverse media showing civil / regulatory proceedings for crime, corruption, misuse of public funds etc
- Sanctions hits on addresses (Sanctions lists are increasingly being updated with cryptocurrency addresses related to sanctioned individuals and entities, screening for these does not negate the need to screen individuals but should be considered as part of a regular screening system where VA or blockchain VG deposits are accepted).

3.3 Analytics

It is recommended that where deposits or exposure to funds from VA are considered a more than minimal percentage of an operator's business then either in house blockchain analytics or paid for tools are utilise to provide an additional layer of oversight of transactions.

Most blockchain activity can be easily traced through the use of blockchain analytics however this will depend on the type of VA/VG and the deposit method. For instance Bitcoin is a type of cryptocurrency that is highly traceable due to its mechanism (UXTO) where each transaction uses the whole of a previous transaction, issuing "change" back to the sender and does not just record a balance on account as with Ethereum and Ethereum based VA/VGs.

Where VA/VGs are deposited from a VASP on behalf of a customer it is unlikely the analytics will show any customer transactional data, instead the analytics will show the activity of the VASPs liquidity pool or will be an address created by the VASP to facilitate a deposit or withdrawal. In this case analytics can still be utilised to determine any red flags or risks relating to the VASP itself providing the source of funds.

Where analytics are used the following considerations should be made—

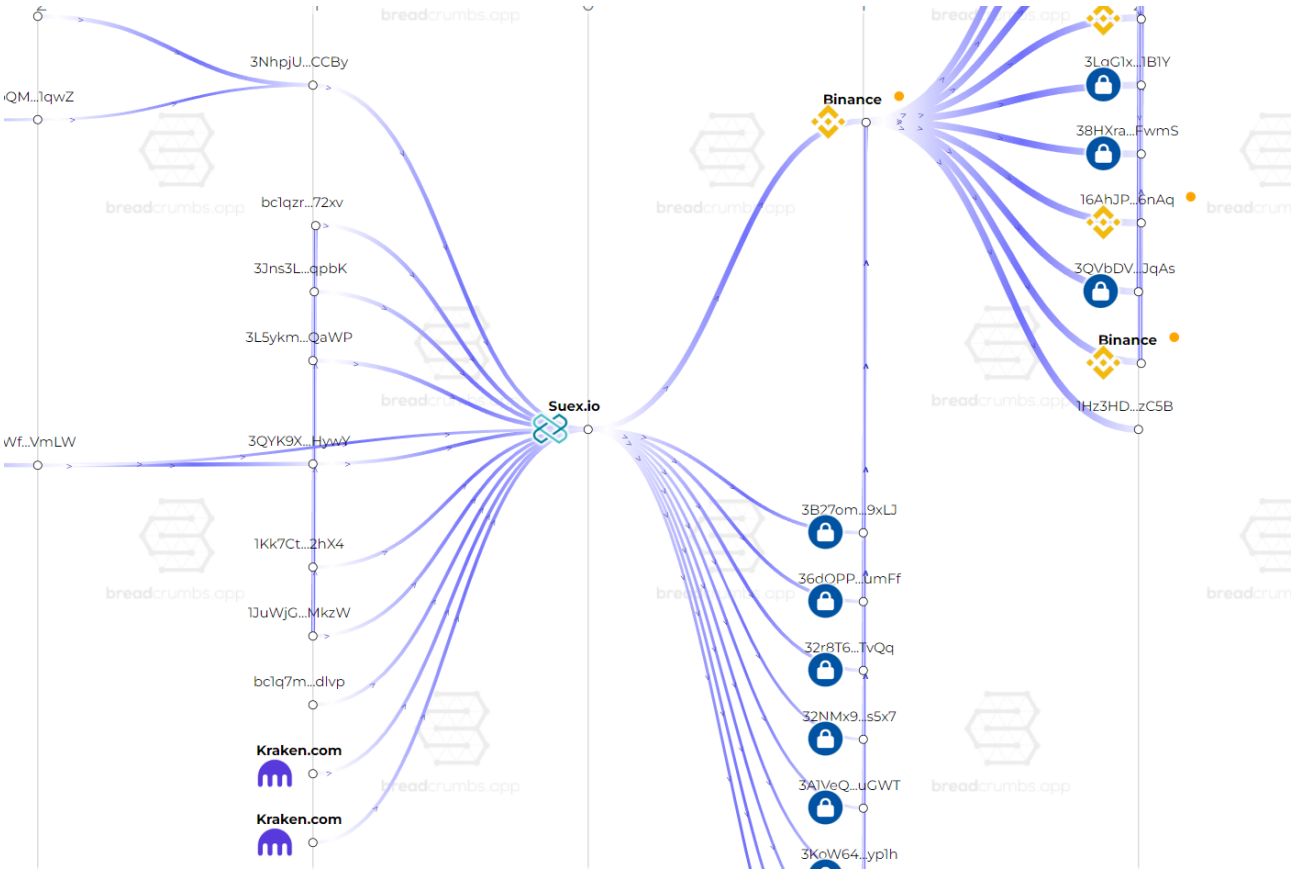
- Business Risk Assessment – the BRA should clearly define the use of analytics is commensurate to the level of risk that the use of VA/VG creates. See 4.2 Business Risk Assessment for further considerations.
- Training – staff should be trained to understand any specific analytics tools and how to identify ML/TF/PF flags. See 4.11 Staff Training on VA/VG.
- Policy – Operators should have clear policies and procedures in place relating to the use of analytics tools outlining risk tolerances around source exposure and hops.

3.3.1 Source Exposure

Analytics will be able to provide attribution (ownership) of VA/VG where they have hit service providers such as exchanges or DeFi platforms, however their pseudonymous nature means it is difficult to attribute ownership for all transactions. An operator should take into consideration the activity of any addresses utilised by the customer including where the majority of funds are being received from as part of the establishing the customer's risk profile. This will be in addition to the requirements of the Code regarding Customer Risk Assessments.

An example is given below of what an analytics graph may look like and shows funds flowing to and from an OFAC sanctioned exchange named SUEX. The transactions senders and recipients are identified where they are exchanges such as Binance and Kraken. However there are more transactions with no attribution so no way of identifying ownership of those transactions. It is important that when using analytics an operator considers this lack of attribution in determining the level of customer risk associated with the VA/VG. In order to do so the levels of source exposure should be defined within an operator's risk tolerance.

For instance if a customer's deposit address and any associated addresses can be linked to multiple illicit sources then that customer has more source exposure which represents a higher risk for ML/TF/PF than where there are one or two links over multiple transactions.



3.3.2 Hops

Each line in the analytics chart above represents a transaction known as a hop so for each hop a transaction has occurred where VA and VG have moved into and out of addresses. As well as source exposure an operator should take into account the amount of hops that have occurred between a customer address and any source exposure. This should not be the only factor when assessing risk as ML typologies such as Peel Chains rely on making hundreds if not thousands of transactions in a short period of time to obfuscate the flow of funds.

3.3.3 Analytics Red Flags

- **Mixing** – where a "mixer" service is used to mix and or/ aggregate virtual currency transactions, sometimes used to hide or break the link between the source of the virtual asset and its destination
- **Chain-hopping** - converting one cryptocurrency into another and moving from one blockchain to another
- **Peel Chain** – A large amount of illicit funds is split rapidly into smaller and smaller chunks creating a large and complex chain to follow where amounts are peeled off into smaller amounts.
- **Labels** – most blockchain explorers label wallets and addresses that have been identified as receiving illicit funds from dark net activity, fraud, hacks and scams.

- **Unregulated/Fraudulent Exchanges** – using unregulated exchanges where there are little or no AML/CFT controls or exchanges that have been involved in fraudulent behaviour.
- **Sanctions** – increasingly sanctions are being extended to both cryptocurrency addresses of individuals and exchanges known to support TF and PF.

Key Messages

Key Messages

- The GSC considers that transactions made in virtual assets may represent a higher risk than transactions conducted using traditional methods and expects an enhanced risk based approach to VA use.
- If accepting VA deposits, either directly or facilitated by a PSP or exchange then an operator is required to notify GSC first to seek permission.

3.4 Permitted Models & AML/CFT Risks

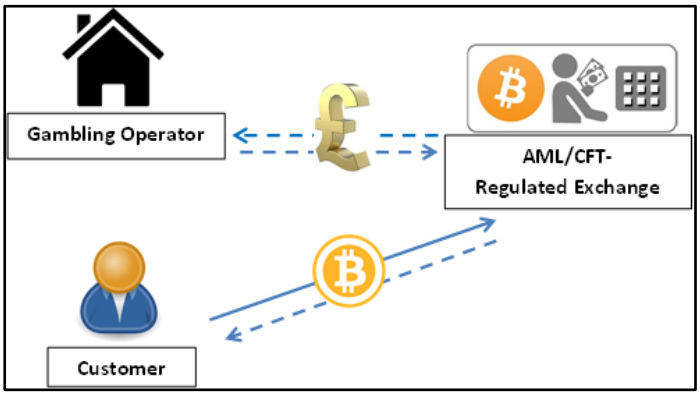
MODEL 1:

VA/VG to fiat conversion prior to play. In this model, the operator uses an exchange mechanism such as a VASP as an interface between players who deposit VA/VG onto its platform. For instance the player deposits with an exchange and the exchange passes the Fiat equivalent to the operator for gambling.

Prior to establishing a business relationship with a VASP, an operator should conduct due diligence. Only VASPs that are subject to an FATF-compliant mandatory regime[2] for reporting suspicions on ML/FT/PF are acceptable.

The AML/CFT framework under which a VASP operates should be considered in the operator's business risk assessment.

Example:



[2] https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

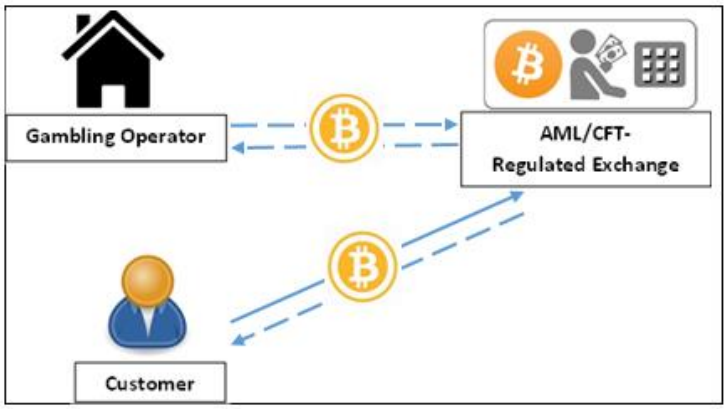
MODEL 2:

VA/VG to exchange prior to play. In this model, the operator uses an exchange mechanism such as a VASP as an interface between players who deposit VA/VG onto its platform. For instance, the player deposits VA/VG with an exchange and the exchange passes the VA/VG to the operator for gambling.

Prior to establishing a business relationship with a VASP, an operator should conduct due diligence. Only VASPs that are subject to an FATF-compliant mandatory regime for reporting suspicions on ML/FT/PF are acceptable.

The AML/CFT framework under which a VASP operates should be considered in the operator's business risk assessment.

Example:



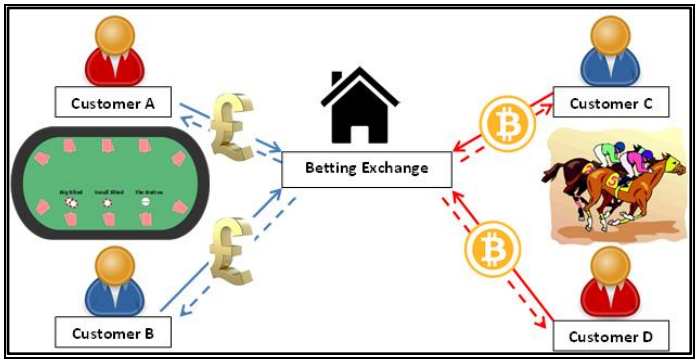
MODEL 3:

VA/VG -in, VA/VG -out, peer-to-peer. In this model, players may deposit VA/VG and use them to play against other players with the same deposit arrangements. Play may be competitive (for example: poker) or passive (for example: pool betting, pari-mutuel).

As with Fiat currency peer to peer gaming, operators should be alert to illogical player strategies, such as—

- Soft play in peer to peer games where players fail to pursue obvious advantages against opponents; and
- Chip dumping, where players seem to deliberately lose to opponents.

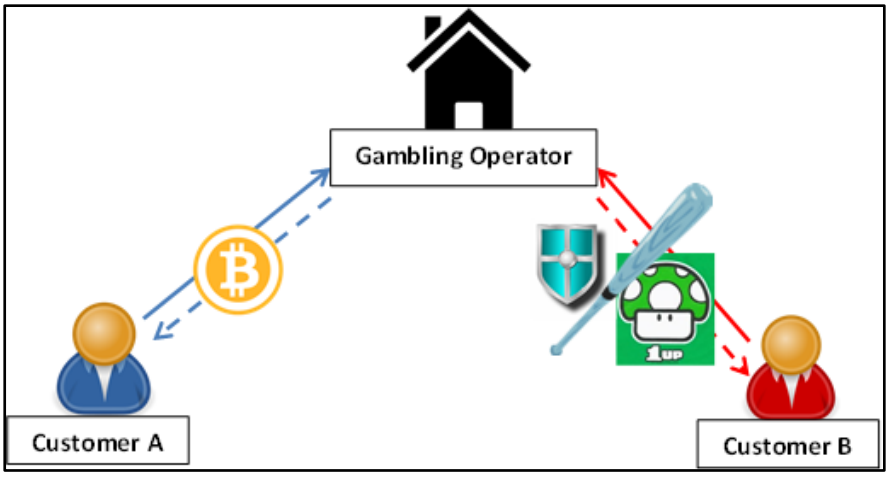
Example:



MODEL 4:

VA/VG -in, VA/VG -out, against the house. In this model, players may deposit or pay for gambling against an operator and winnings are drawn against the operator's funds rather than those of other players. No exchange can occur in this model between different VAs, VGs or Fiat.

Example:

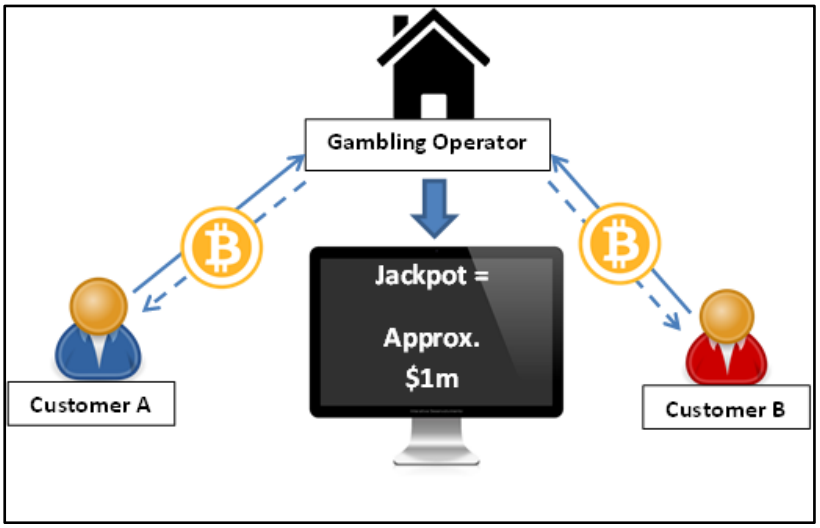


MODEL 5

VA/VG-in, Conversion, VA/VG-out. In this model VA or VG are deposited by the player. Different VA/VGs may have different values and may therefore be converted to a common denomination for the purposes of play using an in-house currency.

This in-house currency is then converted back to the same type of VA or VG as were deposited to supply the prize prior to withdrawal. In this model the conversion is only made by the operator to facilitate gambling and the player does not have access to the converted currency or goods.

Example:



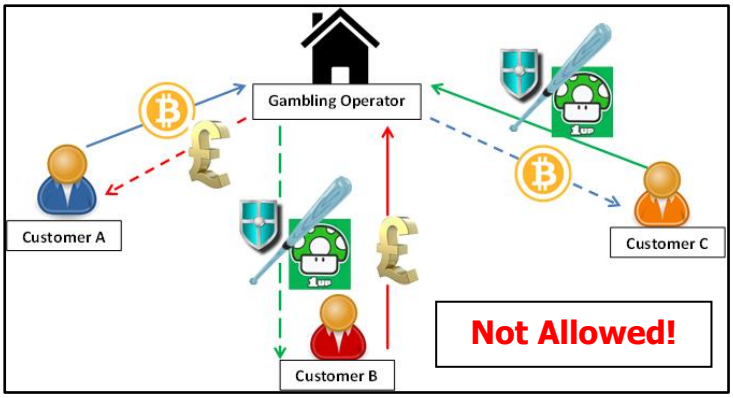
3.5 Non Permitted Models

MODEL 6

VA/VG-X-in, VA/VG-Y-out and **VA/VG-in, Fiat-out** and **Fiat-in VA/VG-out. This model is not permitted due to the AML/CFT risks it creates.** In this model it is possible for players to deposit any Fiat or VA/VG with the operator and choose a different currency (Fiat or VA/VG) as a means of withdrawal, effectively treating the operator as an unregulated exchange.

The GSC recognises that some gambling sites or their partner gaming sites may offer the functionality to exchange VG or provide buy-back services. The GSC may consider these on a case by case basis. Please see 4.8 Transfers and "Buy-back" Functionality for further details.

Example:



Key Messages

Key Messages

- Don't use models that can facilitate money laundering, terrorist financing or proliferation financing e.g. mixers, virtual currencies that promote anonymity.
- Have an effective risk framework that identifies and mitigates the risk associated with virtual currencies.
- Understand the risks associated with virtual currencies.
- Ensure that staff have relevant training when dealing with virtual currencies.
- Ensure that controls are in place for tracing the flow of funds.
- Where needed, ensure source of wealth is proportionate and plausible.
- Use chain analysis tools where possible.
- Non-permitted models - Any permanent conversion between cryptocurrencies, between virtual goods or to fiat facilitated by the operator.

4.0 Application of AML/CFT Requirements

In addition to the requirements of the Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Code 2019 (the Code) and the GSC's AML/CFT Guidance for Gambling Operators, the following also applies:

4.1 Technology Risk Assessment

Technology risk assessments are of particular importance for operators planning to deal with VA/VG. The GSC expects that full and detailed risk assessments should be undertaken for each new VA/VG channel or product used paying particular regard to the privacy/secrecy ambitions of the schema, its history and the ability of law enforcement to obtain access to users' identity. Assessments should be updated to take account of any changes to that channel or product as it develops.

See AML/CFT Guidance which provides further information on the obligations for completing a technology risk assessment and how to conduct one.

Key Messages

Key Messages

- The GSC expects that full and detailed technology risk assessments should be undertaken for each new VA/VG channel or product used paying particular regard to the privacy/secrecy ambitions of the schema, its history and the ability of law enforcement to obtain access to users' identity
- Risk Assessments should be updated to take account of any changes to that channel or product as it develops.

4.2 Business Risk Assessment

The GSC's AML/CFT Guidance for Gambling Operators states that operators should update their business risk assessment at least annually. Due to the rapidly evolving nature of VA/VG's, operators engaging in VA/VG activities are expected to review and/or update their business risk assessments on a more regular basis.

In addition to the typical considerations as detailed in the Guidance for Gambling Operators, the business risk assessment should include reference to the operator's up-to-date technology risk assessments.

For operators engaging in MODEL 1 (see 3.4 Permitted Models & AML/CFT Risks) activities, the assessment should also include details of any exchanges used and consideration of the following:

- The geographical location of the exchange;
- Its AML/CFT obligations;
- The level of regulatory oversight and AML/CFT oversight that it is subject to; and
- Any adverse information about the exchange or its owners and controllers.

See AML/CFT Guidance which provides further information on the obligations for completing a business risk assessment and how to conduct one.

Key Messages

Key Messages

- Due to the rapidly evolving nature of VA/VGs, operators engaging in VA/VG activities are expected to review and/or update their business risk assessments on a more regular basis (i.e. more than once a year).

4.3 Customer Risk Assessment

The GSC considers that VA/VGs as a source of funds represents a higher risk than fiat transactions but this does not necessarily make the customer high risk. All relevant factors should be considered.

The following should be recognised as high risk indicators or "red flags":

- Anonymiser software, IP mixers, coin mixers and anonymity enhanced crypto-currencies;
- IP does not match registration details provided;
- Significant transactions in VA/VG where the value is unusually high or low; and
- Source of wealth is unclear or cannot be verified (see 4.4 Customer Due Diligence for further detail).

See AML/CFT Guidance which provides further information on the obligations for completing a customer risk assessment and how to conduct one.

Key Messages

Key Messages

- Operators to consider VA/VGs as a source of funds may represent a higher risk than fiat transactions and whilst this does not necessarily make the customer high risk, the higher risk should be considered.

4.4 Customer Due Diligence

Unlike traditional payment decentralised VA/VGs can be accessed by anyone anywhere without having to pass any CDD checks. There is no fool-proof way to ensure that a Virtual Asset Account address/account actually belongs to a player. This means that there is a risk that the player could be transacting using someone else's address/account.

In order to mitigate the risks of a player acting as a front man for a person that is a criminal, sanctioned or simply resident in a country where gambling is illegal the GSC recommends that, on a risk based approach, the following additional checks should be considered:

- Matching IP addresses to CDD information supplied;
- Checking the address/account for negative information in the public domain; and
- Use of block chain analysis tools.

Block chain analysis tools in particular can be used to monitor **source of funds** for any VA/VG transaction and can indicate that a wallet address has been exposed to fraudulent behaviour or suspicious sources. Monitoring the address transactions can flag suspicious patterns for instance peel chains or use of tumbling services.

The Code requires an operator to verify a player's identity when the EUR 3,000 threshold is met. (Please see 4.6.2 AML Requirements on Pay-As-You-Go Models for Qualifying Payments for further detail on establishing the EUR equivalent of VA/VG transactions). Due to the risks associated with this new payment technology, the GSC recommends operators to consider implementing a lower than EUR 3,000 threshold and to also apply a deposit threshold over which CDD must be completed.

Enhanced due diligence is required for all high risk customers, including *reasonable measures* to establish the player's source of wealth. The GSC expects operators to apply more stringent measures for VA/VG source of wealth checks, particularly when large values are deposited. An operator should take steps to verify the information provided by a customer. For example, if a VC customer explains that their source of wealth (virtual goods) is from in-game play, the operator should consider how this can be corroborated, perhaps from game logs, game history screens or third party websites showing play history.

See AML/CFT Guidance which provides further information on how to conduct a customer risk assessment.

Key Messages

Key Messages

- Block chain analysis tools in particular can be used to monitor source of funds for any VA/VG transaction and can indicate that a wallet address has been exposed to fraudulent behaviour or suspicious sources.
- Operators to consider implementing a lower than EUR 3,000 threshold and to also apply a deposit threshold over which CDD must be completed.
- Operators are expected to apply more stringent measures for VA/VG source of wealth checks, particularly when large values are deposited.

4.5 Transaction Monitoring

Effective risk based transaction monitoring systems are essential for operators to quickly identify and address any unusual or high risk activities.

The GSC expects the following principles to be followed:

- Transaction monitoring should be conducted on a regular or ideally real-time basis particularly when pay-as-you-go models are in use (see 4.6 Pay-As-You-Go Gambling for further detail);
- Conversion rates must be up-to-date for value-based thresholds/alerts;
- Consideration should be given to setting lower thresholds for VA/VG than for fiat transactions;
- Monitoring should include in-game play, deposit frequencies and transaction patterns rather than focusing only on value in, value out.

4.6 Pay-As-You-Go Gambling

Operators who have satisfied their AML/CFT obligations on account opening may subsequently offer pay-as-you-go arrangements to players due to the quick and cheap nature of VC transactions, that is: players purchase a stake in an individual game of chance directly rather than depositing currency in a wallet and drawing from it.

For example, a player plays crypto-slots with an operator. Every time he selects the spin button, a payment of virtual currency is made to the operator's address. Whenever he wins a prize, it is sent to his address. After a twenty minute session, he stops playing and his balance with the operator is zero.

The GSC considers that the potential speed in which multiple transaction may be carried out poses increases risks relating to AML/CFT and also fraud.

4.6.1 Requirement to Detect Unusual Activity

An operator offering a pay-as-you-go model must be able to detect unusual activity in real time and suspend the account automatically. The GSC's experience of third party software written to mimic human players (bots) suggests that similar applications could be created to make automatic virtual currency payments (for whatever reason). Such applications could fail and create runaway payment situations.

Equally, player accounts can be hi-jacked and attempts made to drain funds as quickly as possible.

Where unusual activity is detected, the operator's software must be capable of automatically locking the account until a satisfactory explanation can be obtained.

In order to minimise the risks, operators should consider putting into place restrictions on the value and volume of transactions that may be carried out.

4.6.2 AML Requirements on Pay-As-You-Go Models for Qualifying Payments

Operators' software must be capable of applying an automatic lock on withdrawals once the AML/CFT qualifying payment threshold has been met (currently EUR 3,000).

This means that the software must understand and apply the rolling aggregate calculation to the previous 30 day's activity and must calculate the equivalent EUR value of all transactions based on their equivalent value at the time. If multi-channel wallets are held by a single player, the aggregate calculation must operate on the sum of these wallets' activity.

For example: When assessing the value of transactions, the GSC will use the following rule of thumb: a money launderer will withdraw then convert his virtual money into fiat and use it to commit a crime. Therefore the value of funds falling into his hands over a period of time is equal to the convertible value at the times of withdrawal.

A criminal withdraws the following sums during a period of volatile exchange rates:

01/01/2018	*1 altcoin*	*equiv*	*fiat*	*value*	*EUR*	*300*
04/01/2018	*1 altcoin*	*equiv*	*fiat*	*value*	*EUR*	*800*
09/01/2018	*1 altcoin*	*equiv*	*fiat*	*value*	*EUR*	*1*
12/01/2018	*1 altcoin*	*equiv*	*fiat*	*value*	*EUR*	*1900*

The transaction on the 12th January causes the aggregate value of transactions to exceed the EUR 3000 threshold and the account is locked pending AML/CFT checks.

4.7 Withdrawals

All online gambling operators are required (under the Registration and Accounts regulations) to pay funds away either to the same account or facility from which a deposit has previously been made or to an account or financial facility that the operator is satisfied will result in the player exclusively receiving the withdrawal.

Due to the difficulties in connecting addresses with real world identities, the GSC considers that the use of multiple addresses, particularly where withdrawals are made to a different address, is high risk.

The account/address used to deposit a VA/VG should be the account/address used for withdrawal transactions.

Requests to send a withdrawal to a second or subsequent address, even if the player supplies a credible reason why a second address should be used, should be considered as higher risk and trigger enhanced due diligence.

For AML/CFT reasons, an operator may not offer a fiat equivalent to make up any shortfall in VA/VG payments to players.

4.8 Transfers and "Buy-back" Functionality

Peer to peer transfer or "buy-back" of convertible virtual currencies (e.g. bitcoin) are not permitted under any circumstances.

The GSC recognises that some gambling operators or their partner gaming sites may wish to provide functionality to allow players to either trade, or sell, unwanted virtual goods (such as "skins" or "game gold").

The GSC recognises that risks arise when virtual currencies are exchanged. However in limited circumstances, in relation only to virtual goods that are non-convertible currencies, this may be permitted. Such functionality would be considered on a case-by-case basis with consideration where the exchange is incidental to the operator's main business (i.e. gambling) given to the following factors:

- The value of the virtual goods;
- Whether trades are with the operator, a third party company or with other players;
- Controls in place;

- Whether such a service could lead the operator being considered as providing activities that are required to be licenced or registered with the IOMFSA.

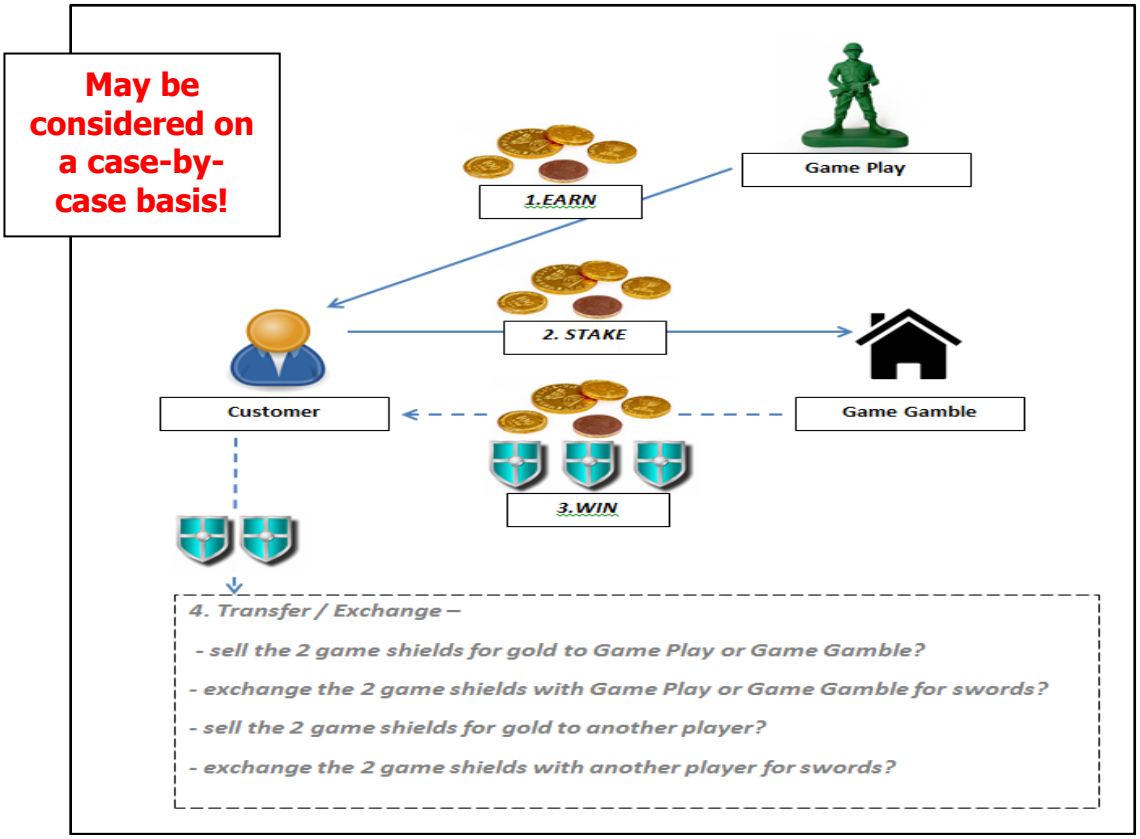
For example –

A customer may play on gaming site "Game Play". During play, the customer earns 5 pieces of "Game Gold". The customer can use the "Game Gold" to buy "Game Goods" such as swords and shields to assist in their gameplay.

The gambling operator "Game Gamble" allows the player to deposit and stake the game gold for a chance of winning more game gold or various game goods.

Neither the gold nor the goods can be used outside of "Game Play" or "Game Gamble" meaning that it is non-convertible virtual currency.

The customer wins their bet and receives back their staked gold plus three shields but the customer only needs one shield. The GSC may consider whether the unwanted game goods could be sold for game gold or exchanged for different game goods:



4.9 Blocking and Freezing of Accounts

Operators must be able to manually lock accounts so that they can prevent payments being made to people that are subject to financial sanctions or AML/CFT investigation.

If a player's risk rating changes and becomes higher (perhaps as a result of an unusual step up in transaction value, a change in the country from which play occurs or a change in political exposure) then the system must be able to lock the account to prevent the withdrawal of funds until the AML/CFT requirements in the Code have been satisfied.

4.10 Record Keeping and GSC Information Requests

4.10.1 Conversion rates

When examining transaction records the GSC will require equivalent EUR values to be supplied so it will be helpful if operators can record against each transaction the EUR equivalent or the exchange rate at the time of the transaction.

Operators may be asked to demonstrate to the GSC which exchange rate or basket of exchange rates they track. Once an exchange rate or basket of rates has been selected, the GSC expects that this source will be used consistently.

4.10.2 Separation of Channels for Quarterly Reports

The financial data supplied on quarterly returns for fiat activity and virtual activity must be separated by channel. If an operator offers poker, casino games, a sports book, poker, altcoin slots and virtual goods gambling for Diablo III artefacts and CS:GO skins then it will be required to report financial data relating to fiat gambling, altcoin gambling and virtual goods gambling separately.

4.10.3 Thematic Checks

As the GSC moves compliance to a risk-based approach, it is likely that it will seek to understand virtual currency and virtual goods gambling more quickly than other developments.

For this reason, operators which offer these products may be asked to participate in additional activity designed to help the GSC understand the practicalities of the technology and to identify any potential typologies for example are operators noticing that a larger than normal proportion of VA/VG customers are also considered as politically exposed persons.

4.11 Staff Training on VA/VG

The GSC recognises that VA/VGs are a rapidly evolving area and as such, operators may find it difficult to ensure that staff members have sufficient training. The GSC expects that staff dealing with VA/VG transactions should have a moderate level of understanding about the VA/VGs that they are dealing with.

A more detailed technical knowledge is required for assessing technological development and business risks. For this reason, operators that do not have the appropriate level of understanding or experience in dealing with VA/VGs internally should seek input from a reliable and independent expert.

Key Messages

Key Messages

- Effective risk based transaction monitoring systems are essential for operators to quickly identify and address any unusual or high risk activities.
- An operator offering a pay-as-you-go model must be able to detect unusual activity in real time and suspend the account automatically.
- Operators' software must be capable of applying an automatic lock on withdrawals once the AML/CFT qualifying payment threshold has been met (currently EUR 3000).
- All online gambling operators are required (under the Registration and Accounts regulations) to pay funds away either to the same account or facility from which a deposit has previously been made or to an account or financial facility that the operator is satisfied will result in the player exclusively receiving the withdrawal.
- Peer to peer transfer or "buy-back" of convertible virtual currencies (e.g. bitcoin) are not permitted under any circumstances.
- Operators must be able to manually lock accounts so that they can prevent payments being made to people that are subject to financial sanctions or AML/CFT investigation.
- It is helpful if operators can record against each transaction the EUR equivalent or the exchange rate at the time of the transaction.
- The financial data supplied on quarterly returns for fiat activity and virtual activity must be separated by channel.
- The GSC expects that staff dealing with VA/VG transactions should have a moderate level of understanding about the VA/VGs that they are dealing with

5.0 Further Guidance

This document is not the only source of information on AML/CFT. Other sources include:

IOM National Risk Assessment

IOM GSC - Home Page

IOM GSC - Legislation

IOM GSC - Anti-Money Laundering Guidance

FATF

IOM Government - FATF and MONEYVAL

IOM - Sanctions and Export Control

FATF - Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing Financial and Non-Financial Sectors

FATF - 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers

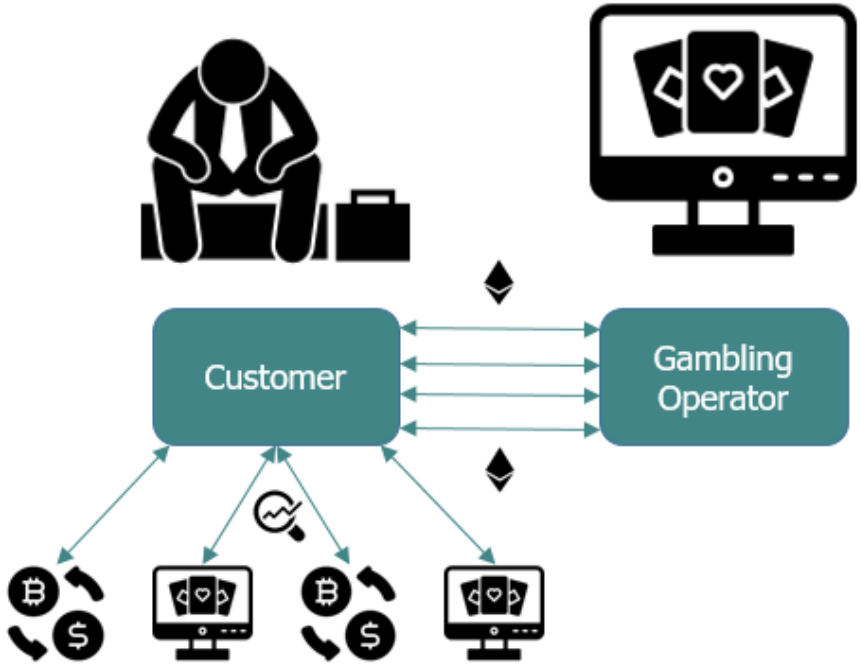
FATF - Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing

FATF – Guidance for a Risk-Based Approach – Virtual Assets and Virtual Asset Service Providers

FATF – Virtual Currencies – Key Definitions and Potential AML/CFT Risks

Appendix One – Typologies[3]

Case Study 1 – Money Mules



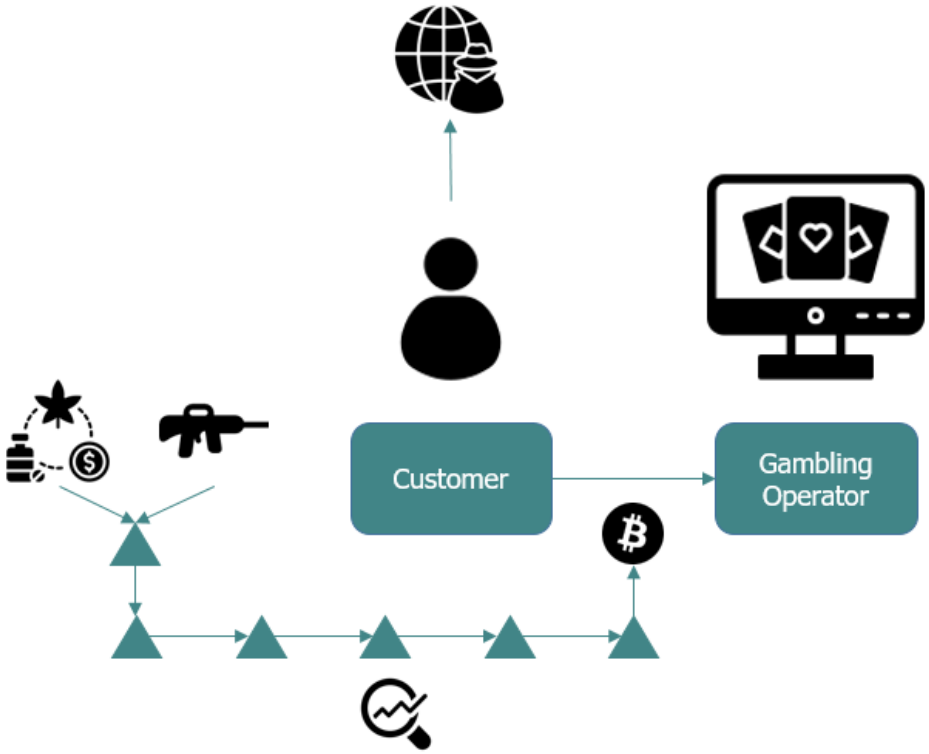
In this example, a customer with low income is approached to earn money by moving funds for someone else or allowing someone else to use their established account. The account receives regular deposits of Ethereum.

Red flags may be –

- An uptick in activity on a previously low turnover or dormant account
- Multiple addresses used to deposit and withdraw
- Minimal gameplay, or gameplay more likely to provide a return
- Reluctance to provide updated CDD/EDD documents and declare SOW
- Spending that is not commensurate to known SOW and customer profile
- Attempts to change IP address or use of a VPN and frequent changes in personal details
- Customer profile indicates they may be vulnerable members of society such as the unemployed, immigrants etc
- Analysis shows links to illicit sources or that funds are rapidly moved in and out of other gambling platforms or exchanges

[3] The case studies presented are fictional and presented to provide an indication of where those looking to move illicit proceeds of engage in TF or PF may attempt to circumvent AML/CFT controls. They are provided as non-exhaustive or exclusive but rather for guidance to create awareness.

Case Study 2 – Source Exposure

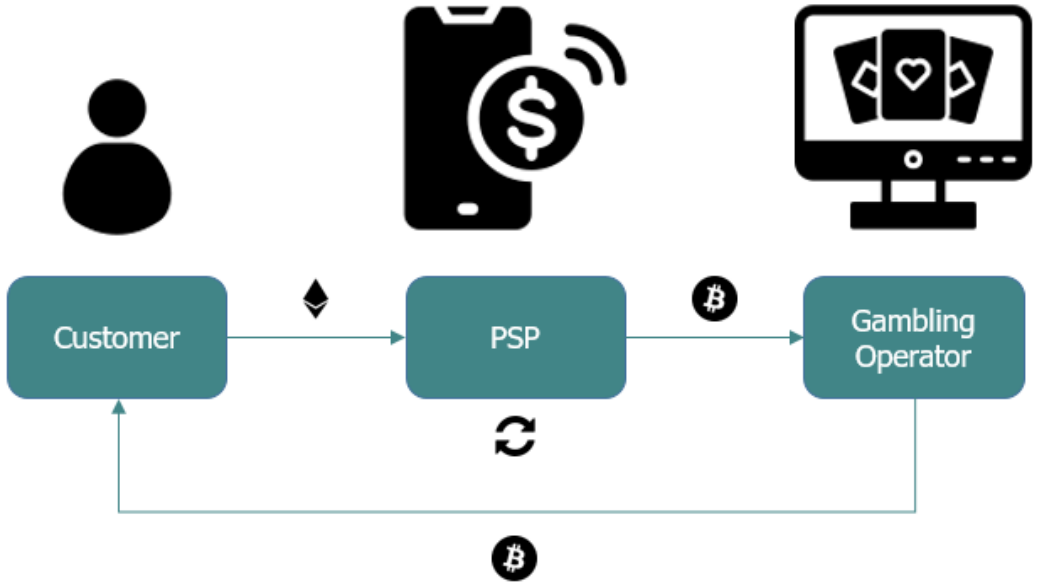


In this example, analytics conducted by an operator flag a Bitcoin deposit from a customer for dark web exposure, however it also reveals the exposure to illicit activity was over 100 hops away. The source of the exposure originated from a website associated with the illegal sale of drugs and firearms but isn't necessarily linked to the customer. Further analytics shows that a large proportion of funds in addresses associated with the customer's address also have dark web exposure coming from illicit sources linked to terrorism financing.

Red flags may be –

- Analytics show a more than minimal exposure from the customer's addresses to other illicit addresses
- Use of multiple addresses for deposit and withdrawal
- Adverse media relating to the customer or the risks in the customer's jurisdiction
- Reluctance or refusal to provide updated CDD/EDD documents or SOW
- Customer profile shows links to sanctioned countries, entities or individuals
- Activity processed by cryptocurrency mixing services linked to sanctions

Case Study 3 – VA Conversion

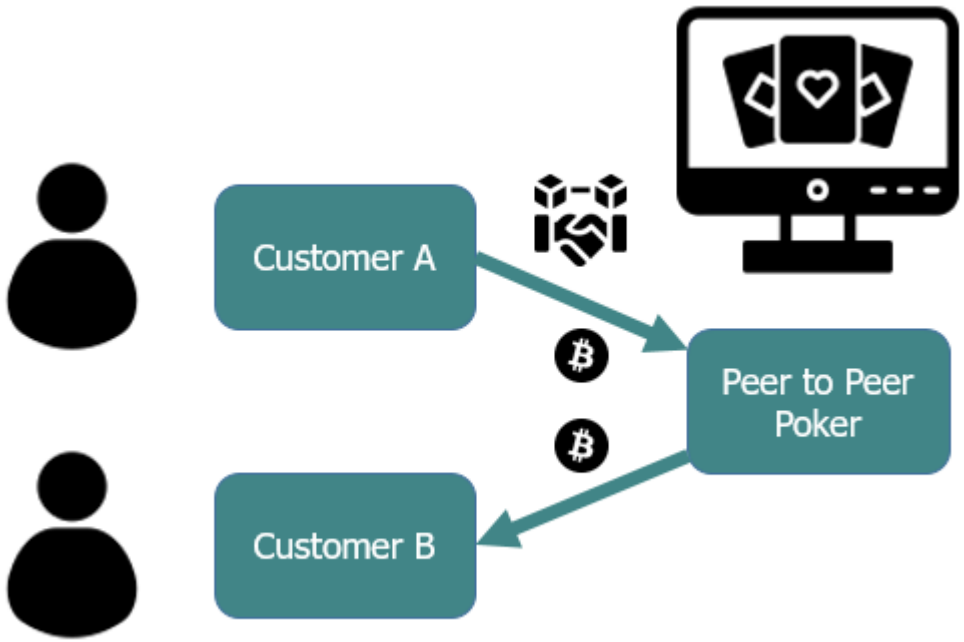


In this example, a customer deposits cryptocurrency into a PSP, is able to convert these funds into another cryptocurrency and then deposit these funds with an operator. The customer has minimal game play or does not want to play through the deposit and requests a withdrawal in that cryptocurrency to a non-custodial wallet address that they have never previously used converting funds thus trying to circumvent the GSC's permissible models and AML/CFT controls.

Red flags may be:

- Conversion of funds prior to play with no rationale
- Conversion of multiple types of VAs prior to play with no rational
- Activity processed by cryptocurrency mixing services linked to sanctions
- Use of unregulated payment providers
- Open loop withdrawals not being returned to additional deposit method

Case Study 4 – Peer to Peer Transfers



In this example, a customer deposits cryptocurrency onto a peer to peer poker website through a smart contract. They regularly lose a similar amount to the same customer where the betting activity does not make sense. It is quite evident that the two customers are colluding in order to transfer funds from one account to another through legitimate activity.

Red flags may be:

- Large bets placed with questionable rationale that lead to the same winner
- Similar residential addresses, locations and IP to accompany signs of collusion
- Interactions over operator chat portals or social areas that would indicate collusion
- Indications that a money mule is being used as the depositor