ISLE OF MAN
GAMBLING
SUPERVISION
COMMISSION

AML/CFT Guidance for Virtual Currencies 2020

V2.0 - 12/2020

Contents

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
2.0	Dec 2020	Replaces the 2018 supplementary guidance, including references to - GSC's 2020 AML/CFT Guidance - Latest FATF Guidance - Blockchain analysis tools

1. Introduction

1.1 About this document

This document has been prepared by the Gambling Supervision Commission (GSC) and is intended to sit alongside the existing Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Guidance Notes. The document provides guidance on AML/CFT matters only and does not cover other matters such as fund protection or problem gambling.

This document applies to operators that accept transactions in any type of virtual currency.

The contents of this guidance should not be construed as legal advice.

1.2 The Gambling Supervision Commission

The application of the gambling legislation to the industry falls to the GSC. The GSC is an independent statutory board of Tynwald and comprises the Inspectorate and the Commission.

The Commission consists of six independent members drawn from various professions and backgrounds. The Commission members conduct monthly hearings into all matters that pertain to gambling in the Isle of Man and are supported by their Inspectorate.

The Inspectorate is managed by the Chief Executive of the GSC.

The GSC is available 9:00am to 5:00pm Monday to Friday
It can be contacted via phone on +44 (0)1624 694331
It can be contacted via e-mail on gaming@gov.im

The address is:
Ground Floor,
St. George's Court,
Myrtle Street,
Douglas
IM1 1ED

2. Background

2.1 Regulatory changes to allow acceptance of money's worth

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 includes convertible virtual currencies (CVCs) and non-convertible virtual currencies (VCs).

The GSC's initial approach to dealing with CVCs and VCs are set out in policies, guidance and licence conditions which may be changed over time as the technology matures.

2.2 Terminology

Fiat currency a.k.a. "real currency", "real money" or "national currency" is the coin and paper money of a country that is designated as legal tender.

Digital currency refers to any electronic representation of a fiat currency and this can include representations of virtual currency.

Virtual currency is a narrower asset and is a digital representation of value which can be traded digitally. The nature of a virtual currency means that it does not need to be (but may be) centrally controlled or administered. Virtual currency can be either convertible or non-convertible.

Convertible virtual currencies (CVCs) include crypto-currency e.g. bitcoin and ether. CVC's can be bought and sold through independent exchanges for fiat currency.

For a currency to be convertible, there does not need to be set rate or an established benchmark, merely that a recognised third party market exists and the ownership rights can be transferred from one person to another(whether for consideration or not). CVCs can be used as a method of payment as an alternative to using fiat currency

Non-convertible virtual currencies (VCs) include virtual goods, such as digital "skins" for avatars or items such as weapons within video games. VC's also include currencies that exist within the context of a specific game for the purpose of buying in-game items etc. VCs differ to CVCs in that they are not used in the same way as fiat currency and are not broadly used as a method of payment.

Whilst the GSC does not define such items as convertible it is aware that sites exist where they can be exchanged such as uncontrolled or black markets. This however does not affect the GSC's view that the items are not convertible in the traditional sense.

Note: the Isle of Man Financial Services Authority (FSA) oversees AML/CFT compliance for businesses that provide money service business style products in relation to convertible virtual currencies. The FSA does not oversee businesses dealing with non-convertible virtual currencies. The GSC regulates gambling activities relating to both convertible and non-convertible virtual currencies.

3. Inherent AML/CFT Risk

3.1 Summary of inherent AML/CFT risk

The GSC considers that transactions made in CVC/VC 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 IOM Financial Services Authority guidance[1] provides detailed guidance on the AML/CFT risks associated businesses that provide money service business style products in relation to convertible virtual currencies. The GSC would summarise the risks as follows:

- non face-to-face business relationships;
- non-centralised "accounts" may be opened by anyone without customer due diligence checks;
- difficulty in linking an "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 CVC/VC in most jurisdictions.

The Financial Actions Task Force (FATF) has gathered together global case studies to inform a report[2] on red flag indicators of money laundering and terrorist financing that highlights the risks described above. The report should be considered in conjunction with the FATF's guidance[3] on a risk based approach when dealing with virtual assets and service providers.

[1] https://www.iomfsa.im/media/2688/sector-guidance-virtual-assets.pdf
[2] http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html
[3] http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

3.2 AML/CFT Risk profile by business model

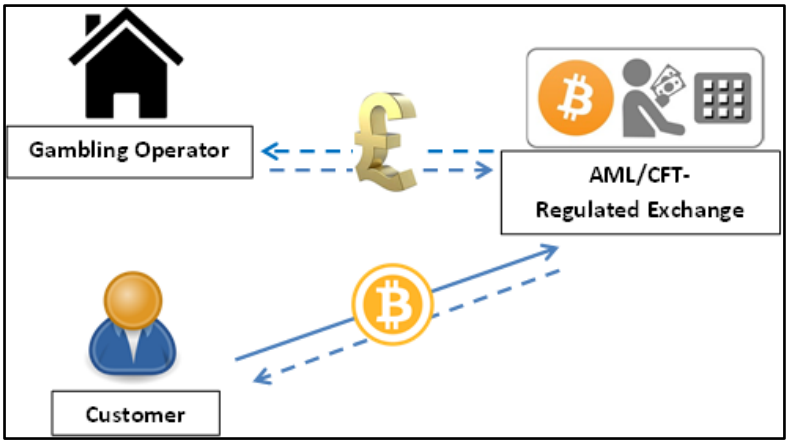
MODEL 1:

☑**CVC/VC to fiat conversion prior to play**. In this model, the operator uses an exchange as an interface between players who deposit CVC/VCs and its platform. The player deposits with the exchange and the exchange passes the fiat equivalent to the operator for gambling.

Prior to establishing a business relationship with a CVC/VC exchange, an operator should conduct due diligence on that exchange. Only exchanges that are subject to an FATF-compliant[4] mandatory regime for reporting suspicions on money laundering and terrorist financing are acceptable.

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

Example, model 1:



[4] http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

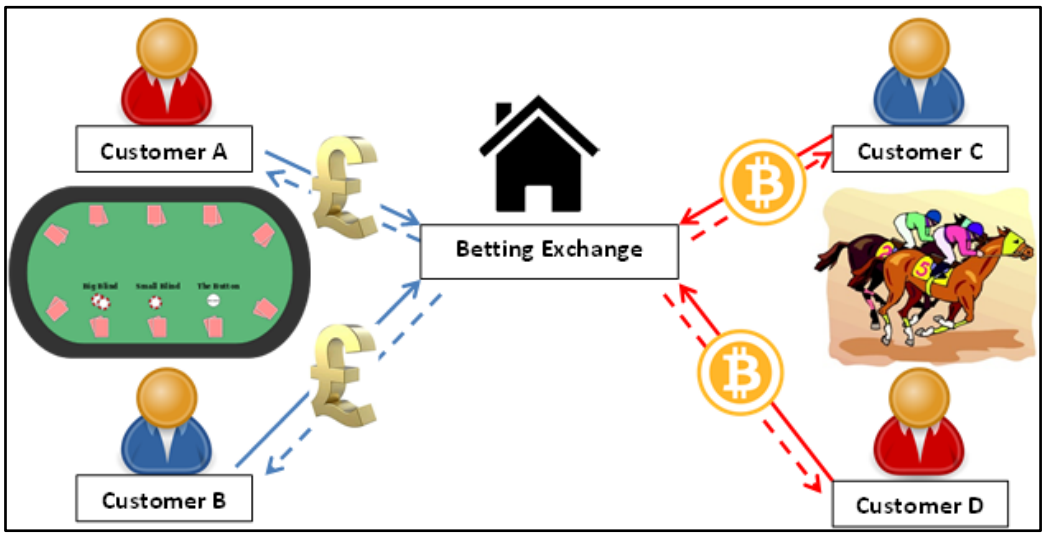
MODEL 2:

☑ **CVC/VC -in, CVC/VC -out, peer-to-peer**. In this model, players may deposit CVC/VCs 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 2:

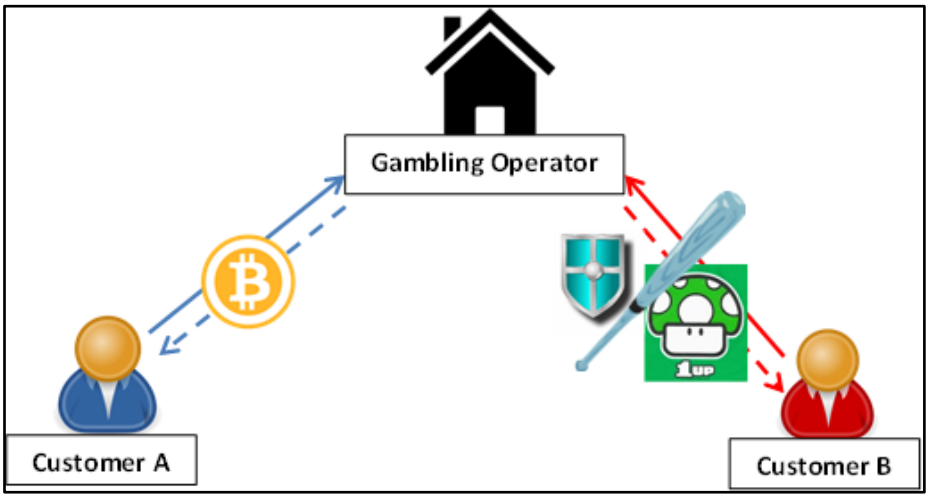


MODEL 3:

☑ CVC/VC -in, CVC/VC -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.

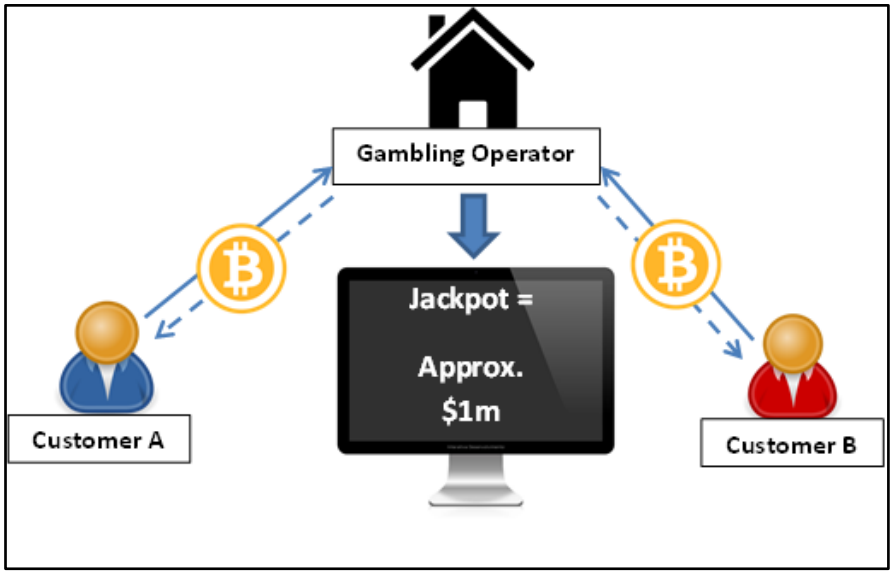
Example, model 3:



MODEL 4:

☑ **CVC/VC-in, Conversion, CVC/VC-out**. In this model virtual goods are deposited by the player. Different virtual goods 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 virtual currency or goods as were deposited to supply the prize prior to withdrawal. In this model the conversion is only made by the operator to facilitate the gambling and the player does not have access to the converted currency or goods. Therefore this model is not considered to represent any additional money laundering or terrorist financing risks to the models described above.

Example, model 4:

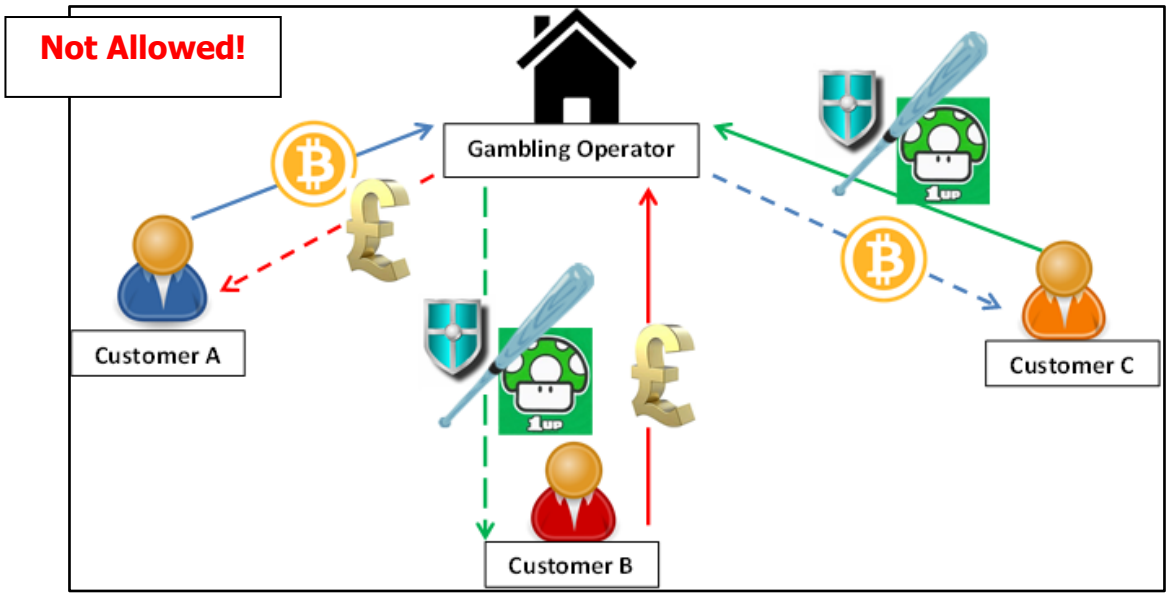


MODEL 5:

☒ **CVC/VC-X-in, CVC/VC-Y-out** and ☒ **CVC/VC-in, Fiat-out** ☒ **Fiat-in CVC/VC-Out.** In this model it is possible for players to deposit any fiat or CVC with the operator and choose a different currency (fiat or CVC) as a means of withdrawal, effectively treating the operator as an exchange. The GSC is not willing to permit this model.

The GSC recognises that some gambling sites or their partner gaming sites may offer the functionality to exchange virtual goods or provide buy-back services. The GSC may consider these on a case by case basis. Please see section 4.8 for further detail.

Example, model 5:



4. Application of AML/CFT Requirements

In addition to the requirements of the Gambling (Anti-Money Laundering and Countering the Financing of Terrorism) Code 2019[5] (the Code) and the GSC's AML/CFT Guidance for Gambling Operators 2020[6], the following also applies:

4.1 Technology Risk Assessment

Technology risk assessments are of particular importance for operators planning to deal with CVC/VC. The GSC expects that full and detailed risk assessments should be undertaken for each new CVC/VC 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.

4.2 Business Risk Assessment

The GSC's AML/CFT Guidance for Gambling Operators 2020 states that operators should update their business risk assessment at least annually. Due to the rapidly evolving nature of CVC/VCs, operators engaging in CVC/VC 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 2020, the business risk assessment should include reference to the operator's up-to-date technology risk assessments.

For operators engaging in MODEL 1 (see section 3.2) 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.

4.3 Customer Risk Assessment

The GSC considers that CVC/VCs 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 CVC/VC where the value is unusually high or low; and
- source of wealth is unclear or cannot be verified (see part 4.4 for further detail).

[5] https://www.tynwald.org.im/business/opqp/sittings/20182021/2019-SD-0219.pdf
[6] link needed

4.4 Customer Due Diligence

Unlike traditional payment decentralised CVC/VCs can be accessed by anyone anywhere without having to pass any CDD checks. There is no fool-proof way to ensure that a CVC/VC 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 CVC/VC 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.[7]

The Code requires an operator to verify a player's identity when the EUR3,000 threshold is met. (Please see 4.6.2 for further detail on establishing the EUR equivalent of CVC/VC transactions). Due to the risks associated with this new payment technology, the GSC recommends operators to consider implementing a lower than EUR3,000 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 CVC/VC 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.

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 for further detail);
- conversion rates must be up-to-date for value-based thresholds/alerts;
- consideration should be given to setting lower thresholds for CVC/VC than for fiat transactions;
- monitoring should include in-game play, deposit frequencies and transaction patterns rather than focusing only on value in, value out.

[7] A peel chain is 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.

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 EUR3000).

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 EURO 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*	*EUR300*
04/01/2018	*1 altcoin*	*equiv*	*fiat*	*value*	*EUR800*
09/01/2018	*1 altcoin*	*equiv*	*fiat*	*value*	*EUR1*
12/01/2018	*1 altcoin*	*equiv*	*fiat*	*value*	*EUR1900*

The transaction on the 12th January causes the aggregate value of transactions to exceed the EUR3000 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 CVC/VC 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 CVC/VC 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 FSA.

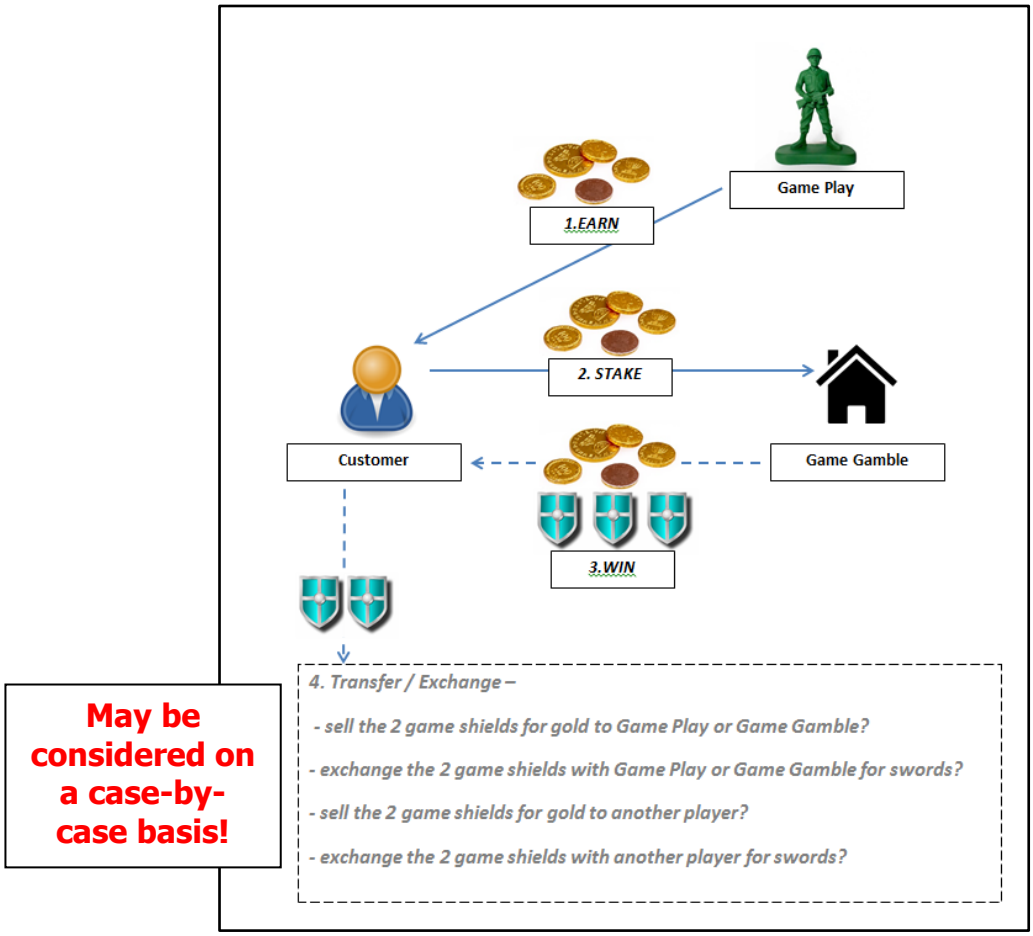
For example –

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 until the AML/CFT requirements in the Code have been satisfied.

4.10 Record keeping and GSC Information Requests

❖ **Conversion rates**

When examining transaction records the GSC will require equivalent EURO values to be supplied so it will be helpful if operators can record against each transaction the EURO 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.

- **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.

- **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 CVC/VC customers are also considered as politically exposed persons?

4.11 Staff Training on CVC/VC

The GSC recognises that CVC/VCs 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 CVC/VC transactions should have a moderate level of understanding about the CVC/VCs 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 CVC/VCs internally should seek input from a reliable and independent expert.