ISLE OF MAN GAMBLINGSUPERVISION COMMISSION

Barrantee Oaseirys Karrooghys Vannin

Isle of Man Government

Reiltys Ellan Vannin

PRACTICE NOTE: Virtual Currencies

> **OPEN POLICY: This policy is intended to be shared with stakeholders and may be freely distributed.**

Practice note – GSC85

Date established: 1st February 2017
Date reviewed: **15th December 2017**
                             7th November 2018   (**cycling addresses**)
                                                               (**trusted hot wallets**)
                             14th January 2019   (**smart contracts**)
                             9th July 2019   ("**CoinCorner Checkout" model**)
                             17th December 2019   ("**FunFair" model**)
                             19th February 2020   (**Fixed address req't revised**)

Background

It is now possible to open an account with an Isle of Man gambling operator by using anything which has a value in money's worth.

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

Convertible virtual currencies include items such as bitcoins which can be bought and sold through independent exchanges for fiat currency.

Non-convertible virtual currencies include virtual goods such as digital "skins" for avatars and weapons in video games and other digital objects that have functions in video games, as well as in-house game currencies that can be used within the game to buy such objects.

Practice detail.

This practice note outlines the GSC's initial approach to this new form of technology and may be changed over time as the technology matures. For this reason, no regulations will be created until it is clear that the GSC's framework is resilient for consumers and workable for operators. Licence conditions will be used during this period to prescribe the rules and these will be changed as rules need to be strengthened or can be safely relaxed.

1. Permitted models for CVCs and VCs

The GSC has identified five different models which operators could seek to use:

- ☑ **CVC to fiat conversion prior to play**. In this model, the operator uses an exchange as an interface between players who deposit CVCs and its platform. The player deposits with the exchange and the exchange passes the fiat equivalent to the operator for gambling. The GSC is willing to licence this model provided the exchange that is used is subject to FATF-compliant, mandatory reporting requirements for suspicion of money laundering and terrorist financing in a jurisdiction with an effective AML/CFT framework.
    - ○ **The "CoinCorner checkout" style model[1] :** In this model, players who start with crypto can scan a code on the operator's page to deposit an equivalent value of fiat currency. Behind the scenes the exchange handles all of the exchange and conversion mechanics on behalf of the operator. The operator is still obliged to conduct its AML/CFT checks when processing players' funds via the checkout model. An exchange offering this service to operators is still obliged to have an AML/CFT reporting requirement to a competent authority, notwithstanding it does not engage with the player directly.

- ☑ **CVC to operator via exchange (hot wallet)[2]**. In this model, the player deposits money with an exchange and uses it to purchase crypto-currency. The exchange enters into a business-to-business relationship with the licensee and will accept payments from it in crypto-currency that are on behalf of players (much in the same way as a payment service provider that deals with fiat currency). The GSC is willing to licence this model provided the exchange that is used is subject to FATF-compliant, mandatory reporting requirements for suspicion of money laundering and terrorist financing in a jurisdiction with an effective AML/CFT framework and the licensee has complied with the guidance on vetting exchanges. The operator is still obliged to understand who the player is and be able to verify that the funds originate from that player (via the exchange) and not a third party. If player details are passed to the exchange in order to process returns, the operator must have the player's consent to share the data necessary to effect the return. Alternatively, the operator may capture a player-nominated crypto-currency return address provided it can satisfy itself that the address is under the control of the player.

- ☑ **CVC-in, CVC-out, peer-to-peer**. In this model, players may deposit CVCs 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). The GSC is willing to licence this model provided the CVCs cannot be cross-traded, that is: one type of CVC deposited and a different CVC withdrawn. However it is still permitted for multiple channels of CVC and VC to be operated for a player – this concept of multi-channel operations is discussed in (2) below.

---

[1] Added 9th July 2019

[2] Added 7th Nov 2018

- ☑ **CVC-in, CVC-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. The GSC is willing to licence this model provided applicants understand and intend to apply the GSC guidance on CVC/VC gambling.
    - o **The "Funfair" model**: In this model, the games and the software necessary to serve them to players are provided to an operator by a token-based software supplier. The games run on a purpose-created blockchain platform using a "token" as currency. To open a gaming session a smart contract is given a supply of tokens by the player and by the operator, which puts in enough tokens to cover the potential winnings for that session. Once the contract has sufficient tokens from each party, the gaming session takes place and wins and losses accumulate.
    Once a game session has completed, the smart contract pays tokens back to the operator and the players as dictated by the wins and losses accumulated in the game session.
    Players funds are never held in the custody of the operator or Funfair which means that the operator using the platform does not require a player fund protection mechanism. The token-based software supplier may also offer additional functionality with respect to affiliate recognition and payment, as well as utilities to make it easier for players to acquire the token and to supply their AML/CFT credentials.
- ☑ **VC-in, Conversion, 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 goods as were deposited to supply the prize prior to withdrawal. The in-house currency has no application outside the gambling website although the operator may allow it to be purchased separately.
- ☒ **CVC-X-in, CVC-Y-out** and ☒ **CVC-in, Fiat-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 licence this model at present.

2. Player account rules

.AML requirements

Accounts may only be opened if operators can comply with:

- The current AML/CFT Code and guidance for online gambling; and
- The enhanced AML/CFT guidance that the GSC issues in respect of virtual currencies and goods gambling.

.The specific CVC used

Accounts may be opened using CVC/VCs. If an operator wishes to accept a CVC from players directly then its risk assessment for AML/CFT purposes must consider the nature of the CVC 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.

.Multi-channel gambling

A player may deposit and play with more than one CVC/VC but the accounting rules for tracking play must keep each channel separate, as if each currency were a separate wallet.

For example:

A player deposits a bitcoin and a dogecoin with an operator. The bitcoin is gambled and produces a win of another coin. The dogecoin is gambled and produces a win of three extra coins. The maximum withdrawal the player can make is two bitcoins and four dogecoins.

Even if the exchange rate were 1 bitcoin for 1 dogecoin, the bitcoin win could not be converted into dogecoins nor the dogecoin win converted into bitcoins. In the same way the operator could not convert the currencies internally before play or withdrawal. Such crossed transactions will be prevented by the conditions of the licence.

.Requirement to intercept account take-over[3]

There is a general requirement on all operators who handle players' funds to ensure that withdrawals are sent to an instrument that is under the same control as the player who made the deposit. This safeguard is designed to prevent the account takeover typology from succeeding.

In the account takeover typology, an attacker gains access to another player's gambling account (e.g. unattended laptop, misplaced trust in another, hackers, etc) and uses their access to empty the account's funds by specifying a different target (e.g. different credit card number, different crypto address) for the withdrawals.

It is recognised that cryptocurrency applications rarely use the same address twice.

The GSC's inspections will seek to understand how account takeovers are prevented.

If an address is captured at the beginning of the gambling relationship by the operator and that address is the only address that the withdrawals are sent to, that will be considered to mitigate the account takeover risk.

---

[3] Requirement revised 19 Feb 2020

If an address is supplied to the player by the operator and only that address is used, that will be considered to mitigate the account takeover risk.

Operators are not expected to mitigate the risk of an account takeover on the cryptocurrency address itself (i.e. control of the wallet or exchange account) but should consider putting a procedure in place for a player who can prove they once controlled that address and who report that they do not now have control.

3. Protection of players' currencies and goods

If players deposit CVC/VCs with an operator, those deposits may be vulnerable to two types of protection failure.

The first type of failure occurs when insufficient care is taken by the operator to safeguard deposits or winnings held by the operator (for example, the private key of a wallet is shared with temporary staff). The GSC considers it is the operator's responsibility to guard against these types of failure.

The second type of failure is where the underlying platform of a CVC/VC or the infrastructure underpinning CVC/VCs is either withdrawn, insufficiently supported or fails (for example, a company which administrates the virtual goods for a computer game discontinues the game). The GSC does not consider the operator responsible for this type of failure unless it was precipitated by the operator itself.

.requirement to safeguard deposits

Operators must demonstrate to the GSC that they have anticipated threats to the mechanisms used to store players' deposits and winnings and that they have put in place credible measures to mitigate these threats. Mitigations may include:

- Taking surplus currency off the network until it is needed;
- Converting the currency to something more secure until it is needed;
- Using multi-signature applications to protect against withdrawal by a single person;
- Insuring or hedging against loss of currency arising from hacking, accidental loss, deliberate theft (internal or external), and so forth.

If a wallet is held directly by the operator, rather than a trusted third party who executes instructions, then the operator will need to indicate how an internal threat (i.e. from an insider) is managed.

.requirement to explain risk to players

The virtual goods that players obtain in gaming often do not belong to them, but rather remain the property of the software company that created them and which administrates their allocation. Players on the other hand may believe that the virtual goods are theirs because they may have paid for them.

Operators who have not secured the agreement of the company which controls the allocation of virtual goods must make it clear to players that their goods are not protected if an action by that company results in the goods no longer being available.

Operators with formal agreements from software suppliers are not obliged to explain the risk. In this case, if the software supplier breaches the agreement it is only necessary for there to be recourse to legal action (for example, for breach of contract).

4. Volatility rules for player-versus-the-house models

The value of CVC/VCs can change quickly (for example in response to good news and bad news stories). An operator accepting CVC/VCs when the value is low may be faced with a large overhead if a win means they have to source the same currency or goods when the value has increased significantly.

An operator offering betting and other games where it has an exposure to winners in CVCs/VCs must be able to supply those CVCs/VCs if the win occurs.

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

If an insurance arrangement is used to hedge against unpayable wins it must be capable of supplying the CVC/VCs required even during periods where the value of the currency or goods has increased outside of expectations.

5. Player to player transfers - VCs only

If an operator offers ancillary functionality for VCs to be transferred, traded or sold then it must only apply to winnings and it must not be possible for players to set the trade or sale price.

Any transfers must be subject to AML/CFT monitoring and treated as qualifying payments if the EUR3,000 threshold is met.

6. Technology assurance costs

The GSC reserves the right to oblige operators to pay for an independent technology expert to be chosen by the GSC and to assist the GSC with elements of a model that are beyond the GSC's expertise.

The GSC is happy to meet with potential applicants before they pay their application fee in order to discuss models and identify any areas where independent expertise might be required (and where the operator may be requested to fund the expert's fees).

7. Pay-as-you-go gambling

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

For example, a player plays crypto-slots with an operator. Every time he selects the spin button, a payment the CVC 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.

It is recognised that operators automatically paying winnings may elect to retain winnings until the transactions that were used as the stakes have entered the block-chain as trusted transactions.

.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.

Operators will be expected to determine limits which guard against high velocity withdrawals or deposits which appear to be automatic in nature and to lock the accounts where this occurs until the player has been contacted.

.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:

A player with multiple wallets on his account withdraws the following sums during a period of volatile exchange rates:

1/1/2018   1 altcoin   equivalent fiat value EUR300
4/1/2018   1 bitcoin   equivalent fiat value EUR800
9/1/2018   1 altcoin   equivalent fiat value EUR1
12/1/2018   1 altcoin   equivalent fiat value EUR1900

The transaction on the 12th causes the aggregate value of transactions to exceed the EUR3000 threshold and the account is locked pending AML/CFT checks.

.Data that operators can expect the GSC to request

When examining transaction records the GSC will require exchange rate information to be supplied as well so it will be helpful if operators can record against each transaction the exchange rate for fiat (GBP or EURO are acceptable) 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.

.Manual locking of accounts

Operators must be able to manually lock accounts (in other words, prevent further play) so that they can prevent payments being made to people that are:

-   subject to financial sanctions or AML/CFT investigation;
-   suspected of cheating;
-   suspected to be under age; or
-   suspected to have a gambling problem.

.Automatic response to risk factor changes

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.

8. Information requirements

Operators adopting virtual currencies and goods will be subject to two additional requirements for supplying information to the GSC.

.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, altcoin poker, altcoin slots and virtual goods gambling for video games A and B 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 monitor virtual currency and virtual goods gambling more closely.

For this reason, operators which offer these products may be asked to participate in additional reporting.

9. Advertising fiat equivalent values for virtual currency or virtual goods

If an operator suggests in its advertising or on its website/application that CVC/VCs have an equivalent fiat value then the claim must:

- Be correct at the time of the advertising;
- Show how the value has been calculated (i.e. which exchange has been used);
- Must carry a disclaimer that changes in the exchange rate may mean that the prize has a lower value when won; and
- That the prize will, in any case be paid as a CVC/VC despite the fiat equivalent used in the advertisement and that no cash equivalent will ever be paid.

10. Existing operators adding CVCs to their licence

The GSC does not see the addition of a CVC into payment options as a new gambling product. If slots can be played using separate fiat and CVC wallets then it is sufficient for the licence to specify that RNG Games are licensed.

However the GSC will require the licence to be modified so that a schedule with the requirements for CVC use can be added.

11. Existing operators adding virtual goods to their licence

The GSC sees the offering of gambling using VCs as a separate product and licensees seeking to offer this type of gambling will be required to have the new product approved by the GSC and added to their licensed products.

12. Fees and Taxation

The GSC currently accepts only GBP as a payment for its fees.

Operators seeking to offer CVC/VCs in gambling are strongly advised to contact the Isle of Man Treasury's Customs and Excise Division in order to understand how their liabilities will be calculated.

13.Smart contracts

Licensees whose models use smart contracts will be required to demonstrate that the code used in the contracts conforms to the model supplied to the GSC. The GSC requires the opinion of an independent expert which states that the code has been written in a way that conforms to the specification. The GSC will assess the expert report when taking into consideration whether it is satisfied that the smart contracts will behave as predicted.

Appendix A: Summary of permissions and constraints

1. Accounts can be opened using CVC/VCs;
2. Operators can accept CVC/VCs through an exchange or directly from players;
3. Volatility rules apply where play is against the house;
4. CVCs cannot be converted to fiat or other CVCs/VCs at all;
5. Multiple CVC/VCs may be accepted by an operator provided they are kept separate. These cannot be mingled, exchanged or traded. They may be temporarily converted into an in-house currency in order to be compatible with dissimilar currencies in peer to peer play but this in-house currency may only be converted back into the original CVC/VC of the player;
6. The address used for deposits or payments should be the only address that can be used to receive withdrawals unless the operator treats the new address as higher risk and triggers enhanced due diligence.;
7. AML/CFT obligations must be met at all times – equivalent fiat values will need to be calculated to do this;
8. Enhanced AML/CFT rules may be prescribed in licence conditions and additional guidance may be supplied;
9. Value held by the operator for players must be protected against predictable threats but the GSC accepts that loss of value through the failure of a distributed ledger or such like, or the unilateral action of the controller of virtual goods is beyond the operator's control.
10. The GSC may ask operators to pay for technology experts appointed by the GSC but is happy to discuss the likelihood of this before any application fees are paid;
11. Once players have opened accounts, operators may accept payments in real time for gambling rather than require deposits. If this function is offered then ongoing monitoring and account locking must be automatic for certain circumstances and manual account locking must also be possible;
12. The GSC will ask for transaction data to contain exchange rates so operators should consider integrating this into their transaction records;
13. If operators advertise fiat cash-equivalents for CVC/VCs then rules will apply to the calculation and to disclaimers;
14. Cash can never be paid in lieu of virtual winnings;
15. Existing operators seeking to add virtual offerings require additional licence conditions from the GSC and adding VCs requires the product to be added to the licence.;
16. Operators and prospective applicants are advised to contact Customs and Excise to understand the taxation implications of gambling when CVC/VCs are used;
17. The GSC will adapt requirements as this area of technology matures.