



Code of Practice for the Gambling Industry

Anti Money Laundering Arrangements - v.1.0.2016

Issued by the

Gambling Commissioner

**As approved by the Minister for Gambling,
pursuant to S.6(6)(f) of the Gambling Act
2005.**

Gibraltar Gambling Commissioner

Suite 603
Europort
Gibraltar
Telephone +350 20064145 Fax +350 20064150
www.gibraltar.gov.gi/new/remote-gambling

Version Control

Date	Version/Amendments	Controller	Number
31 Dec 2010	First Release (Feb 2011)	PB	v.1.0.2010
10/10/2012	Removal of GRA references only	PB	v.1.0.2012
27/11/2015	Updated version of SAR Form Updated office address Updated Sanctions list	PF	v.1.0.2015
27/07/2016	Proceeds of Crime Act 2015 references	DW	v.1.0.2016

This document may not be reproduced in whole or in part for commercial purposes without the prior permission of the Gibraltar Gambling Commissioner.
Commercial purposes includes the sale of or subscription to information services.

Contents:

- 1. Introduction – Our Approach**
- 2. Methods of Money Laundering.**
- 3. Key provisions for non remote casino licence holders and all remote gambling licence holders.**
- 4. Additional considerations for remote gambling licence holders**
- 5. Additional considerations for non-remote casino licence holders**
- 6. Contact**

1. Introduction – Our Approach

1.1 Consistent with international guidelines and relevant legislation, for the purposes of this document ‘anti money laundering’ (AML) should be read as ‘anti money laundering and counter terrorist financing’, unless otherwise stated.

1.2 Internationally there is a historic and generally misplaced assumption that gambling facilities may be used by money launderers to ‘clean their cash’. This misconception is widely held by the public, and is amplified by some media and politicians, particularly those indisposed to gambling in general or online gambling in particular. The Gambling Commissioner is aware, and international evidence indicates, that the properly regulated gambling industry’s security processes are highly effective in deterring any attempts to launder money and that the industry is committed to maintaining these high standards. Nevertheless, the Commissioner believes that the gambling industry in Gibraltar should meet its legal obligations in this area in full, and develop AML processes that are visible, credible and resilient, and will assist in overcoming these misconceptions.

1.3 AML arrangements have been prescribed by the European Commission by way of Directives transposed by EU states into domestic legislation. The Government of Gibraltar transposed the most recent Third AML Directive into the Crime (Money Laundering and Proceeds) Act 2007 (CMLP) which has since been repealed and replaced by the Proceeds of Crime Act 2015 (POCA). These are the source documents for this Code. The implementation of AML law in Gibraltar will be overseen by MONEYVAL with the criteria to be met being the 2012 FATF (Financial Action Task Force) Recommendations and the Fourth AML Directive once this has been implemented. This Code meets those recommendations.

1.4 Article 2 of the Third Directive specifically includes all businesses engaged in ‘casino activities’ as a ‘Relevant Financial Business’ that are required to adopt ‘Customer Due Diligence’ procedures. It goes on to refer to casinos in Articles 10, 36 and 37, and to casinos and the internet in the Preamble (paras. 14 and 39). POCA carries these principles forward in SS. 9 and 14.

1.5 The Directive separately, in Article 13(2), and POCA in S.18, define all non face-to-face transactions as ‘Higher Risk’. Higher Risk activities automatically trigger an ‘Enhanced Due Diligence’ requirement for all remote casino depositing customers.

1.6 The Code applies to all financial transactions associated with defined gambling activities undertaken under the authority of a Gibraltar gambling licence. It builds on the existing good practice of the Gibraltar gambling industry, and is consistent with the anti money laundering guidance notes issued by the Financial Services Commission, the Gambling Act, POCA, recommendations from the Financial Action Task Force (FATF) and the International Monetary Fund (IMF), and the risk based approach these bodies recommend. It will be subject to revision based on any comments received and any changes in legislation or regulations.

1.7 The Third Directive, POCA and the Gambling Act effectively identify the Gambling Commissioner as the competent authority for supervising anti money laundering policies and procedures in the Gibraltar gambling industry. It should be understood that this authority is in respect of gambling licence holders’ regulatory liabilities, and only extends into any criminal liability in so far as the Commissioner

may provide formal guidance (this Code) to the industry and the industry may use this Code to demonstrate compliance with POCA. (POCA S.33(2)).

1.8 The Commissioner is mindful that licence holders are also exposed to the anti money laundering arrangements of every country in which their customers are located. Notwithstanding the complexities of investigation and prosecution across international boundaries, we would expect external jurisdictions to look to the Commissioner and/or Gibraltar's law enforcement arrangements were it to be discovered or alleged that a customer had laundered funds from another state through or into a Gibraltar licence holder's gambling facilities.

1.9 This Code is 'interpretive guidance' to the Gibraltar gambling industry in respect of the requirements of the Gambling Act, POCA and the Third Directive. The Code is issued with the consent of the Minister for Gaming and Financial Services and may be taken into account in any proceedings before a court or in any matter to be determined by the Licensing Authority.

1.10 The Commissioner expects gambling licence holders to take reasonable and proportionate steps, consistent with the risk based approach and the terms and conditions of their Licence Agreements, to manage their AML responsibilities. Consequently, the Commissioner can advise that any examination of reported events alleging money laundering would be from the perspective of – "was what the licence holder did, reasonable in the circumstances?" This approach is not intended as a concession, but to put the responsibility for developing and applying adequate and effective AML procedures on the licence holder.

2. Methods of Money Laundering.

2.1 This Code, POCA and the Third Directive are aimed at ensuring that in addition to the general AML liabilities applicable to all companies, organisations and individuals, those sectors undertaking any of the defined 'Relevant Financial Business' activities should also follow, on a risk based approach, measures designed to deter, prevent and avoid facilitating money laundering; but, where money laundering occurs or is suspected, it is appropriately reported, and a substantive audit trail is available that will allow the relevant authorities to investigate and where appropriate use the evidence to prosecute those involved.

2.2 For criminal purposes S.2 POCA creates the primary money laundering offences in respect of all Gibraltar based companies and staff. Not every country in the world has equivalent legislation. For regulatory purposes this Code recognises that acts of money laundering may be initiated in any part of the world where a customer is based at the time of deposit, gambling, withdrawal or money transfer. Consequently, the Commissioner followed the general principles of anti money laundering activities, as set out by the IMF/FATF/OECD/MONEYVAL, and recognised by bodies such as the European Commission, as the framework for the advice and requirements of this Code. Any regulatory action in respect of licence holders or staff will be based on the content and principles of this Code, not on the absence or existence of equivalent legislation in the originating state. Criminal prosecution rests with other authorities.

2.3 In the context of remote and non remote gambling, money laundering includes three methodologies each based on those initiating the actual money laundering (the customers) 'knowing' the funds are illegitimate. From a customer's perspective, these are:

1. The 'conversion' of illegally obtained funds into funds whose source appears legitimate, i.e. conventional 'washing of dirty money';
2. the 'disguise' of illegally obtained funds, i.e. 'misrepresenting dirty money to a recipient';
3. the 'disposal' of illegally obtained funds, i.e. 'spending or receiving dirty money'.

2.4 These are broad descriptions of how customers may launder money. The Commissioner suggests they include, as examples:

1. Where a customer recycles or attempts to recycle illegitimate money or a proportion of such money, even at a substantial loss; or
2. Where a customer misleads a licence holder as to the source of their deposits, where the source is illegitimate, whether or not they claim it is legitimate;
3. Where a customer deposits, loses or wins money where the source of their gambling funds is illegitimate.

2.5 The Gambling Commissioner has found that it needs to be emphasised that the simple spending of 'dirty money', including the depositing, wagering, winning or losing arising from that money, is likely to amount to money laundering by the customer. The discovery of such actions is likely to focus attention on the effectiveness of the licence holder's EDD procedures.

2.6 From the licence holder's perspective, POCA, the Directive and the Crimes Act 2011 (dealing with aiding, abetting criminal offences etc) may create a fourth liability for those who have knowledge, or suspicion, of money laundering, and who are concerned in those arrangements. 'Knowing or suspecting' is a critical element for licence holders as passing this threshold may create a liability for anyone involved in any aspect of known or suspected money laundering.

2.7 'Knowingly', 'suspect' and 'reasonable grounds to suspect' are established legal principles not defined in POCA or the Directive, but for any criminal purposes the law enforcement agencies are likely to apply the established understanding of these terms in the circumstances. For regulatory purposes the Commissioner will apply the civil 'balance of probabilities' test in respect of this Code and seek to establish whether those involved in allowing alleged money laundering to take place should have known or suspected so in the circumstances. This will include considering any persistent overly liberal interpretation of events, any unreasonable delay or any failure to apply recognised safeguards, and any unjustified deferral or ignoring of suspicious circumstances by staff or management.

2.8 Consistent with international practice, licence holders are required to report to the Gibraltar Financial Intelligence Unit (GFIU) and the Gambling Commissioner all circumstances where they know, suspect or have reasonable grounds to suspect that money laundering is being or has been committed or attempted. The format for such reporting will be developed in parallel to this consultation to ensure that reporting is proportionate and commensurate to the seriousness and significance of the circumstances.

3. Key provisions for non remote casino licence holders and all remote gambling licence holders:

3.1 Nominated Officers. The Commissioner requires licence holders to identify and appoint a nominated individual to take responsibility for developing, implementing and overseeing all anti money laundering arrangements for the financial elements of their Gibraltar licensed operations. This will include the development and supervision of internal AML methodologies and policies, liaison with third party suppliers, staff training, the receiving and evaluation of any relevant suspicious activity reports and liaison with the Commissioner and Gibraltar Financial Intelligence Unit (GFIU) as appropriate. This role is widely known as the ‘Nominated Officer’ and is expected to supersede that of Money Laundering Reporting Officer (MLRO). In respect of ‘third party suppliers’, it will also include oversight of any financial management activities outsourced to parties which undertake those activities on behalf of the licence holder (as opposed to in their own right).

3.2 Personal responsibility. The Nominated Officer is likely to be a significant and senior management role and will carry with it considerable personal responsibility. This is most relevant in respect of the effectiveness of AML activities and if any events or substantive suspicious activity reports are carelessly misjudged and/or not appropriately actioned, or if money laundering is found to have taken place due to systemic or obvious failures in the licence holders’ policies and processes. This individual will need to be appropriately located for management, access and control purposes, have access to all relevant data held or managed by or on behalf of the licence holder, and the direct support of the most senior management of the licence holder (Board/Directors) who will hold ultimate responsibility for AML procedures. In the larger, diverse and ‘24/7’ operations a tier of nominated managers may be required to provide the necessary decision making support on behalf of the nominated officer.

3.3 Undertake formal risk assessment of the business. The Nominated Officer will be required to ensure that the licence holder undertakes (or reviews) formal risk assessments in respect of their relevant gambling activities, customers, areas of operation and transaction methods, and their susceptibility to the differing types of money laundering, and review, develop or implement corresponding AML methodologies and policies. The Commissioner is aware that whereas some games, bets, states and transaction methods have already established a reputation as being susceptible to certain lower level money laundering typologies, other elements of gambling have proved less problematic, and licence holders’ policies and systems should reflect these differences. The formal risk assessment and risk reporting process is likely to be a substantial and ongoing responsibility for operators and should include an annual report to the Board/Directors. These risk assessments should be documented and be made available to the Gambling Commissioner.

3.4 Applying due diligence. The Commissioner requires that all new depositing remote gambling customers should be subject to an Enhanced Due Diligence process and record keeping consistent with POCA and the Directive. Non remote gambling customers may be subject to ‘basic’ customer due diligence based on the ‘threshold approach’ to their spending levels. The threshold approach is not directly applicable to the remote sector. All licence holders should be able to demonstrate that they are identifying and differentiating between higher and lower risk customers, transactions and activities, i.e. the minimum measures may be applied in non-

problematic areas, proportionately more measures and responses should be applied in recognised problematic areas.

3.5 **‘Basic’ customer due diligence (BDD).** Without excluding other considerations addressed in this document, the Commissioner believes that ‘basic’ customer due diligence consistent with S.10 POCA is a two stage process of first obtaining the required personal identification details through an effective and reliable customer registration process, and then verifying that identity using ‘reliable and independent’ means, including databases, documents or other supplementary methods of confirming/assuring identity. S.10 POCA and Article 13 of the 3MLD indicate that basic customer due diligence is the start of the due diligence process. It is required for all remote gambling customers but it may be sufficient only for non remote gambling customers (See 3.7).

3.6 **Enhanced customer due diligence (EDD).** The Commissioner is of the view that S.17 POCA and the Directive require all remote gambling customers to be subject to an EDD process if they make a deposit. S.18 of POCA and the Directive indicate that EDD is Basic Due Diligence, plus an additional third stage, that includes:

undertaking additional identification checks, or
supplementary measures to verify or certify documents, or
ensuring that payments from or to the customer are from/to a bank account in his name.

3.7 Whilst these provisions are not elaborated on, the first and third are self evident, and the Commissioner interprets the second to include the technical measures operators take, often without the customer being aware, to establish and record the electronic footprint and audit trail of the customer; any data held by other parties to the transactions such as payment processors, or any historic data held by the operator or other sources. To qualify as sufficient to conclude EDD, these measures should be in addition to any other arrangement to establish identity or age and should be recorded.

3.8 The Commissioner expects that remote licence holders will develop a range of methodologies for establishing and confirming the identification (and age) of customers to satisfy their AML obligations. These are likely to be determined by the information available in a customer’s country of residence or origin or other demographic detail as well as technical and other developments. The measures applied and proposed by licence holders will be considered by the Commissioner in terms of their sufficiency and effectiveness in the formal engagement processes between operators and the Commissioner’s staff.

3.9 The Commissioner is of the view that BDD and EDD processes are the respective baselines for customer due diligence for the non remote and remote industries, to be applied on a risk sensitive basis, but which may need to be escalated if the apparent risk escalates. The risk based approach does not allow licence holders to avoid BDD/EDD processes outside any exceptions created by statute or regulation.

3.10 Any additional measures are expected to proportionately reflect the value and speed of deposits, the nature of the gambling and the apparent antecedents or developing knowledge of the customer. These are equivalent to responsible gambling, security or customer service triggers in respect of high value and VIP

customer interventions and may include bespoke public source or more discrete or directed enquiries into the background of a customer.

3.11 Retrospective examination of customers. The Commissioner does not expect all existing customer accounts to be reviewed and subject to BDD/EDD, but that active accounts should be subject to a risk based review process over a planned timeframe, consistent with the requirements of SS. 11, 12 and 17 POCA and Articles 8 and 13 of the Directive in respect of the ‘Ongoing Monitoring’ of ‘Business Relationships’ (see below).

3.12 Reviews of such accounts should take into consideration the known reputation and standing of an existing customer when assessing their AML risk and any further measures to be applied. This means that whilst identified customers with consistent and established accounts are not exempt from due diligence procedures, resources should be focussed on those who are less well established, or those whose pattern of gambling or spending profile is outside the expected parameters.

3.13 The Commissioner is of the view that basic customer due diligence (Stages 1 and 2) may include an identified manager, on a risk sensitive basis, appropriately designating a well known customer’s account as properly identified, consistent and established. This is likely to occur where the customer account has been active, transparent and non problematic for an extended period.

3.14 Ongoing due diligence (Ongoing Monitoring). Licence holders should be alert to significant changes, differences or methodologies in the status or practices around all customers, games, states or transaction methods. Typically, these alerts are consistent with security, responsible gambling and marketing alerts, but should also be viewed from an AML perspective. Consequently, due diligence should be recognised by licence holders as a dynamic process, meaning any customer may be subject to periodic but proportionate and documented reviews (including negative checks) based on the conventional, expected or developing gambling profile of customers, especially where that profile changes substantially or appears unconventional. All information arising from this process should be recorded and retained as set out below.

3.15 Analysing games and players. The known history of games, states or transaction methods should also be taken into account when applying due diligence. For example, the Commissioner recognises that the majority of games, bets and spending profiles are largely unproblematic, whereas certain games and markets have proven to be more problematic. This is invariably reflected in general security arrangements. The Commissioner supports licence holders developing criteria, matrices or programs to evaluate which groups of their existing customers and areas of activity should be reviewed and to what degree.

3.16 Training of staff. As a consequence of these responsibilities, licence holders are expected to take steps to develop adequate and proportionate automated or manual systems of risk assessing customers and applying due diligence techniques. Operators should also train all relevant staff to monitor reports regarding customer registration, deposit patterns, gambling activities and personal information for indications of money laundering, and how to respond to alerts or when they suspect or believe that money laundering activities may be taking place.

3.17 Record keeping. Consistent with data protection legislation and AML requirements, licence holders are required to keep records of the measures they have applied to establish the identity of customers, and records of the value of their transactions, for at least 5 years after the relationship ends. The detail and retention of such records should be commensurate with the nature of the apparent risk and sufficient to support any subsequent investigation or court proceedings; i.e. high spending customers with no history with the licence holder or whose source of funds is uncertain should be subject to more substantive enquiries and record keeping than those who were occasional but sufficient gamblers to trigger examination. The Commissioner supports systems that 'step down' the amount of data retained after say, 1, 3 and 5 years.

3.18 Third Party due diligence. Whilst licence holders may use third parties to provide the information that they use for due diligence purposes, i.e. they may use third party databases or information services, or make reasonable inferences regarding the identity of a customer from their particular deposit method etc, they cannot 'rely' on third parties to have concluded basic or enhanced customer due diligence on their behalf and for the purposes of gambling activities unless they satisfy the following condition: Under S.25(6) POCA and Articles 14 and 15 of the Directive, the third party provider must undertake to make available immediately to the licence holder copies of the relevant information it holds and has used to establish CDD. The Commissioner is of the view that the restrictions around this provision make third party reliance viable only if the third party is contracted to obtain and provide such information to the licence holder immediately on request, and/or is part of the same corporate group. For remote licence holders any such information held/provided will have to pass the 'three stage' process (see s.4 of this Code) and should be considered on a risk sensitive basis – i.e. does it remain adequate.

3.19 By contrast, a customer using a payment method that is known to incorporate recognised due diligence arrangements around identity or age verification (ideally 3MLD or FATF consistent) can be inferred to have been subject to and have satisfied these criteria within the context of that entity's business activities and knowledge of the customer's transactions. This inference can be taken into account by the licence holder together with any other information the licence holder has obtained. The Commissioner believes that this allows licence holders to take into account as an element of their own EDD process the method of deposit used by a customer. Conversely, licence holders should take into account the means of deposit as not supporting identity verification where that means is known to involve no due diligence procedures.

3.20 Where third parties undertake due diligence activities on behalf of a licence holder, or where licence holders use third party information and processes, overall responsibility for effective due diligence still resides with the licence holder and not with the third party.

3.21 Anonymous Accounts. Licence holders are not permitted to host anonymous or 'nominal' account records. Any existing anonymous accounts or accounts believed to be 'nom de plume' or that have inconsistent identification should be subject to appropriate due diligence to establish the identity and bona fides of the account holder at an early opportunity.

3.22 Duplicate/Multiple Accounts. Many customers wish to operate parallel accounts in order to segregate their gambling spend. Others choose to open a series of accounts for various reasons, including forgetfulness or a desire for a

change in luck. The Commissioner recognises that there are innocent and legitimate reasons for customers to open more than one account with a licence holder. Notwithstanding this activity, licence holders must be able to identify and associate 'linked' accounts that may belong or be under the control of the same person. The concept of KYC is compromised by a customer who is able to open a second or further account without the licence holder being able to detect this.

3.23 Submission of SARs. Whether or not due diligence has been satisfactorily completed, where the conduct or activities of a customer gives rise to the knowledge or suspicion that the customer is or is attempting money laundering, an internal suspicious activity report should be made by the relevant staff member to a nominated manager or the nominated officer at the earliest opportunity. This will usually be after the event and in the format to be concluded in the consultation process (Annex A). SARs should be provided directly to the GFIU electronically via email and copied in parallel to the Commissioner, who may liaise with the GFIU on any technical aspects of the SAR.

3.24 Urgent Cases. There may, however, be cases of significant events occurring or internal reports being made orally or technically whilst gambling is taking place or bets are pending, and approval is being sought to continue the transactions. In these circumstances the nominated manager should consider whether to allow the gambling to continue or intervene pending any advice on the SAR, or in extremis, an oral report to GFIU/Gambling Division. Whilst different considerations will apply in respect of land based and remote facilities (where any winnings or losses are generally frozen for a predetermined period), unless highly unusual and excessive gambling is taking place it will not, normally, be necessary to suspend the gambling. It will, however, be for the nominated manager to apply experience and judgement in these circumstances with a view to protecting the licence holder by not allowing the situation to escalate and knowingly facilitate or permit money laundering either through the movements of illegitimate funds into the gambling process or the movement of potentially laundered funds out of the operator's control.

3.25 Tipping off. Where any report is made internally, or to the GFIU or the Commissioner, this should not be disclosed to any third party where disclosure might reveal that the report has been made and jeopardise any ensuing investigation. This does not prevent a licence holder from declining to allow any further gambling to take place in a way that does not obviously alert the individual to the initiation of the report, as opposed to general security measures having been initiated etc.

3.26 Politically Exposed Persons. Licence holders are required to make provision, on a risk sensitive basis, to respond to any attempt to gamble by any qualifying Politically Exposed Persons, i.e. any person holding significant public office (or who has held it at any time in the preceding year), having access to public funds or in a position of influence (see S. 20(2) and paragraph 3(1)(a) of Schedule 1 of POCA for full definition of PEP's). This is particularly relevant for persons associated with those states with a history of systemic corruption, but is not limited to those states. PEPs include the readily identifiable family and associates of such persons.

3.27 PEP Databases. A number of commercial databases and public search facilities are accessible to assist in establishing whether an individual may be a PEP. Where a person appears to be a PEP, on a risk sensitive basis, a senior manager (the nominated officer or a designated representative) must approve the deposit/gambling arrangements having taken adequate measures to establish the legitimacy of the source of funds used by the individual concerned, and such

measures must be maintained throughout the relationship. In exercising these responsibilities the Commissioner does not expect every customer to be 'PEP checked'. As elsewhere, a risk based approach should be applied based on the value and scale of gambling and the location of the customer.

3.28 Sanctions Lists. Gibraltar businesses are precluded from engaging in any form of business with persons who are included on relevant international 'sanctions lists'. The Government of Gibraltar publishes a sanctions list consistent with the EU Common Foreign and Security Policy at: http://eeas.europa.eu/cfsp/sanctions/consolidated/index_en.htm which is known as the Consolidated List of persons, groups and entities subject to EU financial sanctions. Licensees may also check the Office of Financial Sanctions consolidated list of targets at: <https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets>. The sanctions list does not provide for a monetary threshold or a 'risk based' approach.

3.29 The Commissioner requires licence holders to take steps to access this list, or an equivalent list provided by a commercial database, as part of their enhanced due diligence process. Where there is reason to believe a person appearing on a sanctions list is or has been engaged with a licence holder then the matter should be subject to immediate disclosure to the GFIU for advice. It may prove necessary to freeze, seize or surrender funds under the control of a person or institution on the sanctions list.

3.30 Repatriation of 'suspicious' funds. The law in respect of the possession, retention and recovery of criminal proceeds under the control of a gambling licence holder is complex and fluid, reliant on both the civil and criminal laws of Gibraltar and the civil and criminal laws of other states, and the location of a licence holder's assets and activities. S.3 POCA effectively states that it is an offence to possess stolen funds unless they have been obtained for 'adequate consideration' or subject to a disclosure in respect of the funds to GFIU as soon as reasonably practicable. 'Inadequate consideration' is defined as consideration that is significantly less than the value of the property. There is no provision for the valuation of 'services'.

3.31 S.35 POCA allows for a confiscation order to be made by the Gibraltar courts where a person has benefited from criminal conduct and appears before the court to be sentenced in respect of one or more indictable offences. The amount to be recovered under a confiscation order is determined as per S.38 POCA.

3.32 The European Freezing and Confiscation Orders Regulations 2014 allow for the mutual recognition of criminal freezing orders and confiscation orders and the Supreme Court must consider giving effect to an overseas confiscation order provided the order meets the relevant requirements. The reciprocal enforcement of confiscation orders may also be determined by the courts.

3.33 Part V of POCA details the regime for the civil recovery of the proceeds of unlawful conduct, thus allowing the seizure and confiscation of assets arising from unlawful conduct even in the event that no criminal proceedings have been brought against anyone based on the civil 'balance of probabilities' standard of proof. Additionally, operators with functions and assets in other states may be subject to local criminal or civil asset recovery arrangements.

3.34 The Gambling Commissioner is mindful of the reputational risk around money laundering and the gambling industry, and that the intention of POCA, the Directive and associated legislation in other States is to minimize the likelihood, benefits and impact of money laundering. Consequently it is the Commissioner's view that where the funds in question are substantial, can be demonstrated as criminally acquired by a reliable and recognised criminal conviction and sentence, that there is an identifiable and unambiguous loser of the funds, and the funds have been deposited/lost in a pattern that should have given, or did give rise to suspicion by the operator that the deposits/losses were suspicious, then their continued retention by the operator cannot be supported by the Gambling Commissioner.

4. Additional considerations for remote gambling licence holders –

4.1 POCA and the Directive require remote ('non face to face') operators to apply enhanced customer due diligence (EDD) procedures in respect of all depositing customers, irrespective of deposit level. EDD should be applied 'as soon as practicable' (S.13 POCA) and 'on a risk sensitive basis' (S.17 POCA) in accordance with the general principles of POCA and the Directive. These requirements are elaborated on below.

4.2 The Commissioner recognises that the timeframe for an EDD process should be risk based, reflect the facilities available to the licence holder in the customer's place of residence, the frequency of contact/transactions by the customer, and be consistent with the typical EDD processing time for that place. Typically, the Commissioner expects the EDD process to be initiated soon after the first deposit and be completed before any withdrawals are permitted, and generally within 28 days, assuming the customer continues to engage with the licence holder and co-operates with the EDD process.

4.3 For the purposes of this document the Commissioner interprets EDD as a three stage process arising from S. 10(a), S. 17 and S. 18 of POCA. Stage 1 is that of obtaining sufficient identification, Stage 2 is the verification of that identity against 'reliable and independent' means, and Stage 3 is further identity verification by way of additional database checks, 'supplementary measures', or a bank process in the name of the customer (as examples given in S.18). These stages are not prescribed as a separate or consecutive process, but this model is helpful in considering options to satisfy EDD.

4.4 The Commissioner recognises that registration details required under the Gambling Act of the name, residential address and date of birth of the customer, obtained through an effective registration scheme, will amount to Stage 1 of obtaining sufficient identification. Existing identity and age verification, security and certain payment processing procedures, other checks and electronic monitoring can satisfy the Stage 2 and Stage 3 requirements of EDD, where the results are provided and recorded in a coherent format:

For example:

4.5 Following or during an effective registration process, the licence holder uses an electronic database to verify the age and/or identity of customers. Such databases are usually composed of multiple data sources, e.g. credit checks, driving licence records, utility bill payees, voter list entries etc. Where a customer has more than one entry item ('hit') on such a database or databases (which may include two credit checks or two utility references), then this is likely to amount to more than one source of identity verification. A registered customer with more than one source of identity verification has completed all 3 stages of EDD.

4.6 In the case of database searches that do not verify (no hits) or fully verify (single hit) customer identity, then a combination of database, bank and credit card processes may also satisfy stages 2 and 3. i.e. bank identity verification may be 'reliable and independent' (stage 2) and S.18(c) POCA provides for a 'first payment' through a bank or credit card (i.e. an account in the name of the customer with a designated credit institution subject to AML requirements) to amount to 'further identity verification' (Stage 3). Such a deposit method, of even a nominal amount, in

conjunction with other bank security processes to establish identity, may conclude EDD.

4.7 Where a registered customer's identity cannot be verified (Stage 2) using database or bank/credit card processes then the licence holder is likely to resort to obtaining copies of or extracts from 'official' documents and/or other reliable and independent means of confirming identity, and using a combination of sources to complete Stage 2 and 3.

4.8 Whilst S.10 POCA requires Stage 2 to be undertaken using 'reliable and independent' source(s), S.18 (a) permits Stage 3 to be concluded by the use of 'additional documents, data or information' (See 3.6 above). On a risk sensitive basis, the Commissioner is prepared to accept that reliable, suitably structured and supported, 'Intelligent Registration Systems' that direct customers to accurately and consistently provide personal data, include automated or manual real time search facilities, deny obviously inaccurate data and use alert and follow up procedures where inaccurate or incomplete data is identified, may amount to 'additional data or information' that can meet the requirements of Stage 3 and possibly Stage 2.

4.9 The Commissioner interprets POCA and the Directive as meaning that whilst a database(s) with different sources of verification can be used for Stages 2 and 3, a single document cannot. Voice/video contact or e-mail contact can contribute to confirming identity (and age) when used in conjunction with other material (e.g. document checks, other personal information.) but are not sufficient for AML purposes.

4.10 It is not feasible for the Commissioner to detail the various permutations of identity verification a customer may provide or a licence holder may draw on, such matrices are for licence holders and their service providers to develop in accordance with the markets they operate in. The Commissioner recognises that licence holders will have to use different verification and further verification arrangements in respect of the residents of different states. The Commissioner expects licence holders to use the most reasonable and efficient methods available in each state, proportionate to the scale of the proposed gambling and consistent with the principles of the Directive and POCA.

4.11 The Commissioner is prepared to consider other proposals that may meet these principles as a means of accommodating the range of customers using remote gambling facilities, and consider these on a case by case basis and during formal engagements with licence holders.

4.12 Whilst EDD has to be initiated 'as soon as practicable', where a customer's deposits reach the equivalent of EUR 2000 or a customer seeks to withdraw funds then EDD must be initiated. If the EDD process is not concluded in a reasonable time frame the account should be subject to additional and proportionate supervision, consistent with the value and risk profile of the account and the deposits. An ongoing assessment should be made at an appropriate management level with a view to expediting the pending verification or other resolution using a risk based approach. Where the verification process fails then no further gambling transactions should take place, including transfers or cash out/withdrawals. In such circumstances, deposits should be retained until identification is resolved.

4.13 For the avoidance of doubt, the Commissioner recognises that EDD is often, but not always, a series of technical measures applied over a managed but varied

timescale, that may require the engagement of the customer, that may be delayed or protracted due to the use of postal services or technical issues, and is more likely to not be concluded due to innocent non co-operation or absence of data, rather than suspicious or criminal attempts to deceive. In parallel, where significant sums are involved, licence holders are in the practice of making direct contact with customers for marketing, responsible gambling or security purposes, and should be equally able to do so for AML purposes.

4.14 Where EDD procedures fail in suspicious circumstances, consideration should also be given to reporting these events to GFU and the Commissioner in the agreed format.

4.15 The Commissioner believes the arrangements set out above will permit remote licence holders to accept deposits and permit gambling subject to:

- 1) customers providing sufficient information at the point of registration in respect of their name, residential address and date of birth, and
- 2) licence holders verifying the customer's identity using a 'reliable and independent' source, and:
- 3) licence holders further verifying that identification from:
 - a. additional documents, data or information, or
 - b. from supplementary measures, or certified confirmation from a recognised credit or finance institution, of the documents/data supplied, or
 - c. by processing the customer's first payment (in or out or both) through a bank account in their gambling account name, and
- 4) the above processes being undertaken reasonably and expeditiously for all depositing customers, in all cases when the customer's deposits reach the equivalent of EUR 2000, and be completed before any withdrawals are permitted, and generally within 28 days.

4.16 The Commissioner recognises that some customers will clear EDD simply, quickly and by a significant margin, whereas others, for legitimate reasons, will not clear it as simply and therefore enter the system much closer to the operator's risk threshold. Licence holders should have arrangements in place to ensure that complementary measures are available for the accounts of slow and marginal clearances in order to ensure that EDD can be escalated on a risk sensitive basis should the scale of gambling increase to a level that is not commensurate with the risk profile of the customer.

4.17 Customers who engage in high deposit gambling should be known to licence holders' security and compliance staff in parallel to any arrangements for VIP management. In terms of what amounts to high deposit gambling, the Commissioner requires licence holders to take in to account the value and speed of deposits as well as the location and apparent identity of the customer. 'High deposit' gambling should trigger further due diligence considerations, such as a review of the outcome of the EDD process, with any additional measures applied on a risk sensitive basis. Such actions should be properly recorded.

5. Additional considerations for non-remote casino licence holders –

5.1 Land based casinos are increasingly designed and recognised as mainstream leisure venues providing a range of entertainment facilities, including various forms of gambling. Internationally the conventional entry controls have been adjusted to reflect the changing commercial offer and customer demand. The arrangements in Gibraltar are intended to reflect this developing position.

5.2 Casino licence holders will be required to exercise dedicated supervision at the entry points to all gambling facilities to ensure that no under age, vulnerable or otherwise excluded persons access the gambling facilities. This is likely to be a combination of personnel and electronic measures.

5.3 Unless the identity of all casino customers is established and verified on entry, casino licence holders must identify and verify the identity of any casino customer who,

- 1) in any period of 24 hours purchases or exchanges chips with a value in excess of the UK Sterling equivalent of EUR 2000; or,
- 2) irrespective of the amount gambled, frequents the licence holder's premises over such a period of time and/or frequency that they are recognised as established casino customers and have entered a business relationship with the casino, which the licence holder has reason to believe will have some duration.

5.4 In the above circumstances the Commissioner requires that licence holders undertake reasonable steps commensurate with the information available from the customer, the physical presence of the customer in the casino, the overt use of effective CCTV recording, and proportionate to scale of their evident casino gambling, to identify and verify the identity of the customer.

5.5 Identity is obtaining and recording the name, residential address and date of birth of the customer. Verification is the satisfactory checking of these details, in whole or in part, against an independent source. These two steps amount to the exercise of basic customer due diligence procedures.

5.6 Initial identification can be provided by the customer by any credible means, including a credible personal declaration. Verification of identity by way of a product from a credit institution (a mainstream bank) in the name of the customer, an electronic address or identity check, or a positive examination of statutory or other credible documents will be sufficient to verify identification and complete basic customer due diligence procedures.

5.7 Other means of verification, such as confirmation by a party known to the licence holder, the production of other credible documents or any other means may also be acceptable if appropriately assessed on a risk sensitive basis and subject to approval and recording by a nominated manager.

5.8 If the licence holder is unable to obtain satisfactorily identification and conclude verification of identity, on a risk sensitive basis, no further gambling transactions may take place, including cash out. In such circumstances,

consideration should also be given to reporting the events to GFIU or the Commissioner.

5.9 The Commissioner believes these arrangements will permit non-remote casino licence holders to allow customers direct access to casino facilities subject to:

- 1) Operators supervising entry to the premises in respect of age and vulnerable customers; and
- 2) Operators having floor systems in place to effectively monitor and respond to customer spend that may reach the threshold in a 24 hour period; and
- 3) Operators having entry and floor systems that can effectively identify and respond to customers who attend the premises to use the casino facilities on a regular basis over an extended period (i.e. 4 of 7 or 8 of 28 days)

5.10 Where a casino does not have these arrangements in place then it is required to revert to the provision of identifying and verifying the identity of all customers on or before entry, regardless of the value of gambling chips purchased through means set out above at 5.4 to 5.8.

5.11 The Commissioner does not regard traditional bingo games, or cash played into 'conventional slot machines', as the equivalent of purchasing or exchanging gambling chips, and at this stage does not intend to include either category of gambling in calculating the identification/verification threshold. High value (stake or prize) machines based on real or virtual casino games (roulette, poker, blackjack, etc.) such as Touch Bet Roulette or Virtual Event betting terminals (FOBT's) are not regarded as 'conventional slot machines'. This arrangement will be kept under review as 'slot machine' technology is developed.

5.12 Where a customer engages in high deposit casino gambling (see below), or establishes a long term, business relationship with the casino, the licence holder will be expected to undertake further due diligence to establish and record the bona fides of the customer, including taking further steps to develop knowledge of the antecedents of the customer and the source of the customer's funds.

5.13 In terms of what amounts to high deposit gambling, the Commissioner requires licence holders to take in to account the value and speed of deposits as well as the apparent antecedents and identity of the customer. 'High deposit' gambling should trigger further due diligence considerations consistent with additional security, VIP contact and facilities, or problem gambling monitoring, escalated proportionately to the value of deposits.

6. Contact

The various documents referred to in this text are available on the Gambling Division website.

<https://www.gibraltar.gov.gi/new/remote-gambling>

The Gambling Commissioner
Gambling Division
Suite 603
Europort
Gibraltar

T: 00350 20064145

F: 00350 20064150

E-mail:

gamblingcommissioner@gibraltar.gov.gi

Annex A

Overleaf is the preferred format for SAR's submitted by gambling licence holders. It is based on documents used by licence holders and is designed to address the problem of incomplete or over technical reports of events. It should be used for suspicious transactions valued at over EUR 2000 and PEPs or Sanctions List cases of any value.

To: Gibraltar Financial Intelligence Unit Suite 832, Europort, Gibraltar. Tel: 20070211/20070295 gfiu@gcid.gov.gi Copied to the Gambling Commissioner Suite 603, Europort, Gibraltar Tel 20064145 gcreports@gibraltar.gov.gi	From: (Operator) Date Submitted:
---	---

PRIVATE AND CONFIDENTIAL

GFIU Ref. DIS:GEN_____

Suspicious Activity Report: Disclosure under the Proceeds of Crime Act 2015.

1. Customer name, address, date of birth, email and telephone number(s).		Registration details.
2. Any other personal information provided or obtained.		Please state nature and source of any other personal information.
3. Account username/ number(s)		Include all account usernames/numbers registered by the customer
4. IP or other technical identification material.		IP and CIN as available.
5. Registration date		Date account registered
6. Products used		State nature of gambling facilities used (Poker, slots, roulette, sportsbook etc) and typical pattern of play/bets or unusual features.
7. Amount deposited - dates and method (card or account numbers).		Enter cumulative deposit values to-date and principal deposit methods.
8. Amount withdrawn – dates and method (card or account numbers).		Enter cumulative withdrawal values to-date
9. Current balance		Total current balance for all products.
10. Operator Profit/Loss to-date		Enter cumulative P/L to-date (customer profit as a minus)
11. Reasons for suspicion		Please detail in full the reasons you have for suspicion.

**Gibraltar Gambling Commissioner
Anti Money Laundering Code of Practice – July 2016**

12. ID and age verification -		What level of verification checks have been carried out? What documentation has the customer provided? Provide details/copies as appropriate.
13. Other checks (PEP, Sanctions, Guardian etc)		Results of any other database check or enquiry; if no check has been performed then carry one out and detail results here. Do not delay submission of the report.
14. Background checks		Detail any further background checks on the customer, What is their occupation? What is their home value? Directorships held, Detail any other useful information gained from wider searches.
15. Associated persons or accounts		Any other parties not already listed.
16. Action taken or other comments.		
17. Completed by:		Contact Person for any enquiries.
18. Date		
19. Supervisor (Nominated Officer/Manager for AML)		Sign off by N/O
20. Date		

This report will be evaluated by GFIU prior to a decision being made as to which agency it may be forwarded for intelligence purposes. Intelligence it is treated as confidential material.

Annex B: Consolidated Fraud Report

This is the preferred format for Fraud Reports to be submitted by gambling licence holders. It is based on a document piloted with one licence holder and is designed to address the problem of high volume, lower value incidents that may be replicated across operators or over time and otherwise escape being identified as repeat sources/beneficiaries of corrupted account details. The contents will be reviewed and searched by staff for any linkages.

.....2015. Operator Contact Person..... email.....

SENDER/SOURCE/COMPROMISEDACCOUNT						RECEIVER/BENEFICIARY OF FUNDS (If any)						
Ref No	Amount	Place	Card No	User name	User IP	Rec'rIP	Rec'r User name	Email prefix @	Current/main card or bank a/c number	Given place of abode	Known to us since	Comments on method or activities.
Sequential and date numbering of date of event(s)	Sum involved: rounded £	Eg: UK	Last 4(min) digits of deposit card or account.	User name	IP and Place	IP and Place	User name	Prefix only	Last 4(min) digits of receiving card or account	Eg: UK	Date this or any other account opened by the receiver	Fraud method (eg chip dumping) and any short observations.
Eg:												
1/12/09/09	125	SWE	2345 6789	flunkyd	81.52.612.1 (SWE)	81.52.211.0 (SWE)	mycash	Bloggs55	1234 5678	UK	10/09/09	Chipdumping, chargebacks to source
2/12/09/09	400	UK	Various	Redspin	192.46.22.1 (UK)	192.46.22.1 (UK)	Redspin	R_spinner	34567890	UK	6/05/08	20 £20 'anoncard' deposits, minimal play, then attempted cash-in.
3/6/10/09	850	FR	Vouchers	Francon	82.252.11.4 (NL)	56.213.42.12 (US)	Mondue	d.asser	01383678	FR	2/7/2007	Xcash vouchers obtained by fraud.

This format is relatively light touch in terms of its content. It provides for operators to meet their obligation to 'report all occurrences of money laundering' and suspected money laundering in appropriate cases. Events involving less than EUR 2000 should be reported on this form unless a SAR was submitted due to the circumstances.

We believe the above arrangements, supplied to the Gambling Commissioner, are comfortably within data protection rules in terms of what we are sent, keep and use the information for. We propose to undertake a regular scan of the information to identify any common senders or receivers where their activities are spread across operators, and where justified co-ordinate the release of that information to either relevant operators or authorities. The form and its utility will be kept under review.