Isle of Man
Gambling Supervision Commission

Online Gambling
Guidance Notes for the Prevention of Money Laundering and Countering of Terrorist Financing

Whilst this publication has been prepared by the Isle of Man Gambling Supervision Commission for general guidance, it is not a legal document and should not be relied upon in respect of points of law. Reference for that purpose should be made to the appropriate statutory provisions.

To be used as guidance notes for the following legislation:

(a) Online Gambling Regulation Act 2001

(b) Proceeds of Crime Act 2008

(c) Proceeds of Crime (Money Laundering - Online Gambling) Code 2010

(d) Terrorism (Finance) Act 2009

(e) Prevention of Terrorism Financing (Online Gambling) Code 2011

Contact:

Isle of Man Gambling Supervision Commission
Ground Floor St. Georges Court
Douglas, Isle of Man
IM1 1ED
Tel: 01624 623355
Fax: 01624 621298
Website: www.gov.im/gambling
Email: gaming@gov.im

CONTENTS

SUMMARY

The Isle of Man is a well regulated and progressive jurisdiction, as confirmed by various IMF reports, the latest being the report of September 2009[1]. These guidance notes have been produced by the Gambling Supervision Commission (GSC) to assist licence holders with their duties and obligations under the Online Gambling Regulation Act 2001 (OGRA), Proceeds of Crime Act 2008 (POCA) and Proceeds of Crime (Money Laundering - Online Gambling) Code 2010 (the AML Code), Terrorism (Finance) Act 2009 (TFA) and the Prevention of Terrorist Financing (Online Gambling Code 2011 (CFT Code) (together referred to as "the codes") in relation to the detection and prevention of money laundering and terrorist financing.

All licence holders must have appropriate systems and processes in place to detect and prevent money laundering and the financing of terrorism. To achieve this they should:

- Adopt a risk-based approach which is flexible and proportionate;
- Ensure total commitment from senior management;
- Develop and implement systems which are appropriate for the business;
- Maintain appropriate records of participants/business participants and transactions that meet the needs of law enforcement investigations tackling money laundering and the financing of terrorism;
- Provide appropriate initial and ongoing training to all staff;
- Ensure nominated officers have adequate support/resources and authority;
- Regularly assess the adequacy of their systems and controls;
- Ensure business engages in an appropriate manner with the GSC and relevant law enforcement bodies; and
- Apply industry best practice across the business.

In developing and implementing their systems and processes, licence holders should have consideration of these guidance notes. However, these guidance notes do provide for licence holders to implement other systems and processes which may achieve the same goal.

[1] http://www.imf.org/external/pubs/cat/longres.cfm?sk=23269.0

SECTION 1 - INTRODUCTION

1.1 Purpose

The purpose of these guidance notes is to:

- Outline the legal and regulatory framework for anti money laundering and countering of terrorist financing in relation to online gaming;
- Outline best industry practice;
- Outline proportionate risk based procedures and approaches;
- Set out the procedures to be followed by licence holders where there is suspicion, knowledge or reasonable grounds to suspect money laundering or terrorist financing;
- Outline the particular money laundering and terrorist financing risks that apply to some of the services and products offered by licence holders;
- Assist operators to design and implement policies and procedures to mitigate the risks of being used in connection with money laundering and the financing of terrorism;
- Ensure adherence to international standards; and
- Outline the role of the GSC.

These guidance notes provide guidance to those who have responsibility for setting the operator's risk management policies and procedures in relation to money laundering and the financing of terrorism. They are not intended to provide an exhaustive list of recommended anti-money laundering/combating the financing of terrorism (AML/CFT) controls. It is intended that operators have the flexibility to develop systems and controls which are based on the risk profile of their business.

Throughout these guidance notes we have used the term "must" where the requirements are statutory or are regulatory requirements placed on licence holders and "should" where the guidance is advisory and the licence holder has discretion.

Also, where reference is made to participant, this will mean participant and business participant.

1.2 Offences

To ensure that a licence holder complies with their legal and regulatory obligations in relation to money laundering and/or the financing of terrorism (ML/FT) it is important that it understands what the terms mean and what offences a licence holder and the staff of a licence holder could commit.

1.2.1 Money Laundering

Money Laundering is defined in the AML Code as "an act which falls within section 158(11) of the Proceeds of Crime Act 2008".

Section 158(11) of POCA states that:

"Money Laundering is an act which:-

(a) constitutes an offence under section 139, 140 or 141;

(b) constitutes an attempt, conspiracy or incitement to commit an offence specified in paragraph;

(c) constitutes aiding, abetting, counselling or procuring the commission of an offence specified in paragraph; or

(d) would constitute an offence specified in paragraph (a), (b) or (c) if done in the Island."

1.2.2 Terrorist Financing

Terrorist Financing is defined in section 3 of the Terrorism (Finance) Act 2009 as meaning-

(a) the use of funds, or making available of funds, for the purposes of terrorism; or

(b) the acquisition, possession, concealment, conversion or transfer of funds that are (directly or indirectly) to be used or made available for those purposes.

The Terrorism (Finance) Act 2009 contains various offences. In particular, section 13 of the Terrorism (Finance) Act 2009 provides that a person who fails to comply with a requirement of a direction imposed by the Treasury under Part 2 of the Schedule to the Terrorism (Finance) Act 2009 commits an offence.

Terrorism is defined in section 1 of the Anti-Terrorism and Crime Act 2003, which provides that:

"(1) 'terrorism' means the use or threat of action where-

(a) the action falls within subsection (2),

(b) the use or threat is designed to influence the government or to intimidate the public or a section of the public, and

(c) the use or threat is made for the purpose of advancing a political, religious, racial or ideological cause.

(2) Action falls within this subsection if it-

(a) involves serious violence against a person;

(b) involves serious damage to property;

(c) endangers a person's life, other than that of the person committing the action;

(d) creates a serious risk to the health or safety of the public or a section of the public; or

(e) is designed seriously to interfere with or seriously to disrupt an electronic system.

(3) The use or threat of action falling within subsection (2) which involves the use of firearms or explosives is terrorism whether or not subsection (1)(b) is satisfied.

(4) In this section-

(a) 'action' includes action outside the Island;

(b) a reference to any person or to property is a reference to any person, or to property, wherever situated;

(c) a reference to the public includes a reference to the public of a country or territory other than the Island; and

(d) 'the government' means the government of the Island, of the United Kingdom, of a part of the United Kingdom or of any other country or territory.

(5) In this Act a reference to action taken for the purposes of terrorism includes a reference to action taken for the benefit of a proscribed organisation."

1.2.3 Contravention of the Codes

Paragraph 21 of the AML Code (a copy of which is attached as appendix A to these guidance notes) and paragraph 21 of the CFT Code (a copy of which is attached as appendix B) both state that a person who contravenes the Code shall be guilty of an offence. Both Codes clarify the extent to which individuals will be held responsible for an offence committed by a body corporate.

1.3 Role of the GSC and Status of Guidance Notes

Pursuant to section 11 of OGRA, the GSC must, subject to the provisions of OGRA and of regulations:

"(a) supervise the operation of any online gambling conducted in the Island;

(b) investigate the character and financial status of any person applying for or holding any licence or otherwise concerned with the operation of any online gambling conducted in the Island; and

(c) ensure that all fees payable to the Treasury by a person conducting online gambling in the Island are duly paid and accounted for;"

with a view to securing that online gambling is fairly and properly conducted, and that the provisions of OGRA and regulations, and the conditions of any licences, are complied with. The GSC is therefore entrusted with a supervisory function in regard to the operation of any online gambling conducted in the Island, and this includes the prevention of ML/FT.

Specifically, in relation to the prevention of ML/FT, the Codes refer to situations where guidance issued by the GSC is relevant:

(a) under paragraph 5(2)(e) of the Codes, "the risk assessment must estimate the risk of money laundering and terrorist financing on the part of the participant or business participant, having regard to - [amongst others] *any relevant supervisory or regulatory guidance given*" by the GSC (emphasis added); and

(b) under paragraph 21(2)(a) of the Codes, in determining compliance with the Codes, "a court may take account of *any relevant supervisory or regulatory guidance given"* by the GSC (emphasis added).

It is therefore critical for all licence holders to incorporate these guidance notes when developing and implementing systems, controls and procedures. The GSC recognises that licence holders may have systems and procedures in place which, whilst not identical to those outlined in these guidance notes, nevertheless impose controls and procedures which are at least equal to if not higher than those contained in these guidance notes. This will be taken into account by the GSC when assessing the adequacy of a licence holder's systems and controls.

The GSC will regularly review the guidance provided and, where appropriate, will amend these guidance notes in light of changing practices, legislative changes and the development of international standards.

SECTION 2 – CORPORATE GOVERNANCE AND RISK BASED APPROACH

2.1 Statutory Responsibility

Paragraph 3 of the Codes sets out the responsibilities all licence holders have in relation to detecting and preventing ML/FT. It is the responsibility of the officers of the licence holder to ensure the business establishes, maintains and operates appropriate policies and procedures.

Where an offence is committed with the consent or connivance of, or is attributable to neglect on the part of an officer of the business, he too shall be deemed to have committed a criminal offence. An officer includes a director, manager or secretary or a person purporting to act as such; if the affairs of the business are managed by its members, a member; in relation to a limited liability company constituted under the Limited Liability Companies Act 1996, a member, the company's manager, or registered agent; and an operations manager as set out in section 10A of OGRA.

2.2 The Appointment of a Money Laundering Reporting Officer (MLRO)

Paragraph 20 of the AML Code requires licence holders to appoint an MLRO. Paragraph 20 of the CFT Code requires licence holders to appoint an Officer. The CFT Code allows for the person to be appointed under the CFT Code to be the same as the person appointed under the AML Code.

In order to avoid any unnecessary division of responsibility and the increased risk of confusion about reporting lines for suspicions of money laundering or terrorist financing within licence holders, the Commission expects licence holders to appoint the same individual as the Officer under the CFT Code as the person who is appointed as the MLRO under the AML Code. In essence the role of the MLRO and the Officer under the CFT Code is the same. Therefore, where the term MLRO is used throughout this guidance, it also includes the Officer appointed under paragraph 20 of the CFT Code.

The MLRO is the person who is nominated to ultimately receive internal reports and who considers any report in the light of all other relevant information for the purpose of determining whether or not it gives rise to a knowledge or suspicion of money laundering and/or terrorist financing.

Licence holders may also appoint a Deputy MLRO to cover for any absence of the MLRO. The Deputy MLRO should be of similar status and experience to the MLRO.

For the avoidance of doubt, the Deputy MLRO should cover all of the MLRO's responsibilities in their absence, including those under the CFT Code. MLROs and Deputy MLROs should not be placed in any situation of conflict of interest.

In order that they can carry out their responsibilities effectively the MLRO and Deputy MLRO should:

(a) normally be resident in the Isle of Man;

(b) have a sufficient level of seniority, independence and authority within the business;

(c) be carrying out a compliance, audit or legal role;

(d) have sufficient resources, including sufficient time and support staff;

(e) have regular contact with, and ready access to, the Board and other members of senior management to ensure that executive management is able to satisfy itself that the statutory obligations are being met and that the business is taking sufficiently robust measures to protect itself against the risk of money laundering and terrorist financing;

(f) be fully aware of both their own and their organisation's AML/CFT obligations; and

(g) have access to all relevant information, which may be of assistance in evaluating STRs.

2.2.1 Role and Responsibilities of the MLRO

The principal objective of the MLRO is to act as the focal point within a licence holder for the oversight of all activity relating to the prevention and detection of money laundering and terrorist financing.

The responsibilities of the MLRO will normally include:

(a) undertaking the internal review of all suspicions in the light of all available relevant information and determining whether or not such suspicions have substance and require disclosure to the FCU;

(b) maintaining all related records;

(c) giving guidance on how to avoid tipping off the customer if any disclosure is made and managing any resulting constructive trust scenarios;

(d) providing support and guidance to the Board and senior management to ensure that money laundering and terrorist financing risks are adequately managed;

(e) liaising with the FCU and if required the Commission and participating in any other third party enquiries in relation to money laundering or terrorist financing prevention and detection, investigation or compliance; and

(f) providing reports and other information to senior management.

Additional guidance on the role of the MLRO is contained in Section 6.

2.3 A Risk Based Approach

To accompany the legal regime that underpins the detection and prevention of ML/FT, a risk based approach is necessary to ensure that individual licence holders respond to current and future risks that could leave their businesses vulnerable to ML/FT.

A risk based approach aims to direct resources where they are perceived to be most needed. As such, licence holders and employees of those licence holders must use their acumen, skills and experience to make useful and sound decisions in implementing a risk based approach.

A risk based approach essentially involves recognising key areas of risk and adopting procedures and policies to mitigate against that risk. It does not involve a rigid, formulaic approach but instead involves constant analysis and revision. Key issues and guidance will be highlighted in this section as to how to comply with the requirements of the Codes regarding risk assessment. It is for each licence holder, however, to conduct risk analysis and implement its own policies and procedures in relation to the specific risks that it may face.

2.3 What is Risk?

Risk can be categorised in a number of ways. One such way is to categorise risk as risk to the organisation or business, risk posed by the type, nature and number of participants and risk posed by the type, nature and number of products. This categorisation is not definitive.

2.3.1 Organisational/Business Risk and Outsourcing

Organisational risk may include external factors that impact on the business of a licence holder such as geographic location of participants, monetary policies, fluidity of business and outsourcing.

The geographic location of a participant may present a higher risk if the participant is located in a country or territory:

(a) which is classified by the Financial Action Task Force (FATF) as non-cooperative;

(b) where important public officials are listed on recognised sanctions lists;

(c) with insufficient AML/CFT controls;

(d) with a large amount of white collar crime or which is known for being susceptible to corruption; or

(e) which is perceived to be strongly associated with terrorism.

To assist in the risk assessment for geographic location, the licence holder should consult data from the IMF, FATF, US Department of State (International Narcotics Control Strategy Report), US Treasury Office of Foreign Assets Control and other relevant organisations.

In relation to outsourcing, delegating licence holders remain responsible for their statutory and regulatory requirements to prevent and detect ML/FT. The delegating licence holder must ensure that the provider it delegates to has sufficient policies and procedures to prevent and detect ML/FT.

2.3.2 Participant risk

Participant risk depends on the level of risk each participant poses to the licence holder. A list of the type of participants that could pose a risk of ML/FT should be compiled and maintained. Participants who have a steady source of income from a traceable source, which they use to participate in online gambling, are likely to present a lower risk. Licence holders should also be aware that seemingly innocent participants may be used by known criminals to place bets on their behalf and so policies and procedures should be implemented as far as possible to guard against the risk of ML/FT occurring.

Key risk factors include:

(a) Type of participant - a politically exposed person (PEP), high net worth individual, or a non-quoted company will potentially present a higher risk;

(b) Complexity of the relationship, including unexplained use of corporate structures and express trusts and the use of nominees;

(c) Delegation of authority (e.g. power of attorney, mixed boards and representative offices);

(d) Request to use numbered accounts;

(e) The public profile of the participant or involvement with, or connection to, PEPs;

(f) Any linked accounts or business partners;

(g) Whether participants are high spenders or business participants who have large amounts of money;

(h) Reputation of the business participant- for example, a well-known, reputable company, with easily available independent information about it and its beneficial owners and controllers is likely to present a lower risk;

(i) Behaviour of the participant. -for example, where there is no commercial rationale for a business participant using the products/services that he seeks, where there are requests for undue levels of secrecy, or where it appears that a relationship or transaction is being made unnecessarily complex; and

(j) Whether there is a large volume of transactions composed of a lot of low value amounts or a low volume of transactions composed of a lot of high value amounts.

2.3.3 Product Risk

Licence holders should be aware that the nature of their products may leave them more vulnerable to money laundering and the financing of terrorism due to the paucity of face to face business. As part of the risk assessment, the types of products that the licence holder offers to participants should be evaluated in line with participant risk to see the type of participant who is using that product.

2.4 Risk Assessment Under the Codes

Paragraph 5(1) of the Codes provides that "a licence holder must carry out a risk assessment as soon as reasonably practicable".

Paragraph 5(2) of the Codes provides that "the risk assessment must estimate the risk of money laundering and terrorist financing on the part of the participant or business participant, having regard to:

(a) value of funds deposited with the licence holder;

(b) jurisdiction of participant;

(c) source of funds deposited;

(d) any other relevant matter brought to the attention of the licence holder during the account opening process for the participant;

(e) any relevant supervisory or regulatory guidance given by the Isle of Man Gambling Supervision Commission;

(f) the legal nature of the business participant."

Each licence holder should therefore carefully record and monitor its risk assessment, having particular regard to the matters listed in paragraph 5(2) of the Codes. The requirement to undertake a risk assessment is not static and as such, should be a continual process that is repeated as and when necessary. How often risk assessment is required may well depend on the nature and size of the licence holder, as an expanding business is likely to require more frequent risk assessment than an established business with no new products or participants.

2.5 Monitoring

2.5.1 Monitoring of Transactions

As part of the risk assessment process, transactions should be monitored so that licence holders may detect suspicious activity at an early stage. In particular, higher risk participants should be monitored more thoroughly and frequently than lower risk ones.

2.5.2 Compliance Monitoring

Paragraph 20 of the Codes provides that "a licence holder must maintain adequate procedures for monitoring and testing compliance" with statutory requirements. Regard must be had to:

(a) the risk of ML/FT; and

(b) the nature and size of the organisation of the licence holder.

As part of the risk assessment, licence holders should therefore regularly monitor transactions and must ensure that they have procedures in place for monitoring and testing their policies and procedures for preventing ML/FT.

If determined fit, having regard to the risk of money laundering and/or terrorist financing and the nature and size of the organisation of the licence holder, the senior management should ensure that a regular (annually, as a minimum) report from the Compliance Officer or MLRO is made. Such a report will assist the licence holder to evaluate whether it is compliant with ML/FT requirements and should include what level of compliance has been achieved.

2.6 Guidance for Risk Assessment

The key steps in a risk assessment should include:

1. Identifying and categorising the relevant ML/FT risks to a licence holder;

2. Producing policies and procedures that would reduce the risks to the licence holder of ML/FT occurring (as identified in the first step);

3. Implementing these policies and procedures and ensuring that employees receive sufficient training, where necessary;

4. Documenting the identification, policy planning and implementation and the reasons behind why particular choices have been made; and

5. Determining a timescale for when the risk assessment should be re-visited and ensuring that this is appropriately diarised and followed up.

Please note that the above is not definitive and licence holders should tailor their risk assessment in accordance with the individual nature and size of their business.

2.7 Higher Risk

Paragraph 5(3) of the Codes provides that where in accordance with the risk assessment, a licence holder determines that a participant poses a higher risk, the licence holder must carry out enhanced participant due diligence in accordance with paragraph 9 of the Codes.

Pursuant to paragraph 9(2) of the Codes, "matters which pose a higher risk include but are not restricted to a participant or business participant who is or has a substantial connection with —

(a) a PEP; or

(b) a person, legal person or legal arrangement resident or located in a country which the licence holder has reason to believe does not apply, or insufficiently applies, the FATF Recommendations.

(c) a person, legal person or legal arrangement that is the subject of any notices or warnings issued from time to time by the Isle of Man Gambling Supervision Commission."

Paragraphs 9(2) do not contain an exhaustive list, and so the individual licence holder should always be aware of other matters that may pose a higher risk, as determined by its risk assessment. Similarly, even if a participant is categorised as a higher risk, this alone does not mean that the participant is a money launderer or financer of terrorism. The same principle applies if a participant is categorised as a lower risk, as although the risk of ML/FT occurring may be low, there is still a risk and the licence holder's employees should remain cautious and alert.

Where a participant is categorised as a higher risk, it is necessary to take additional steps under paragraph 9(3) of the Codes, namely —

"(a) considering whether additional identification data needs to be obtained;

(b) considering whether additional aspects of the participant's identity or the identity of the business participant need to be verified;

(c) taking reasonable measures to establish the source of any funds and of the wealth of the participant and any beneficial owner and underlying principal; and

(d) considering what ongoing monitoring should be carried on in accordance with paragraph 10."

SECTION 3 – KNOW YOUR PARTICIPANT

3.1 Introduction

It is important for licence holders to design and implement procedures and policies to identify and verify participants using appropriate measures. The overall process of knowing who you are dealing with is commonly referred to as customer or client due diligence (CDD), and appropriate measures involve:

(a) Identifying a participant and verifying their identity using reliable, independent source documents, data or information;

(b) Identifying the beneficial ownership and control of a business participant and taking reasonable measures to verify the identity of the beneficial owners and controllers such that a business is satisfied that it knows who the beneficial owners and controllers are;

(c) Obtaining information on the nature of the participant's economic circumstances;

(d) Obtaining information on the purpose and intended nature of the relationship;

(e) Obtaining information on the type, volume and value of the activity that can be expected within the relationship;

(f) Obtaining information on the source of funds and, subject to the risk assessment, obtaining information on the source of wealth;

(g) Monitoring activity and transactions undertaken within the relationship to ensure that the activity or transaction being conducted is consistent with the licence holder's knowledge of the participant; and

(h) Keeping the information relevant and up to date.

Inadequate or absent satisfactory CDD standards and controls can subject a licence holder to serious participant and counterparty risks, especially reputational, operational, legal and concentration risks, which can result in significant financial cost to a licence holder's business.

CDD information is also a vital tool for employees in recognising whether there are grounds for knowledge or suspicion of money laundering or where there are reasonable grounds to suspect terrorist financing. The information is also essential for the MLRO in assessing whether an internal report has foundation. It is only through knowledge of what constitutes normal activity for a participant that unusual activity can be recognised and, from the unusual that suspicious transactions or activity can be determined.

In relation to CDD, the GSC believes that it is prudent practice for licence holders to be clear about the risk that individual participants or categories of participants represent. The criteria used in assessing participant risk will vary from licence holder to licence holder, based on each institution's operations.

Licence holders therefore should have clear, documented participant acceptance policies and procedures which are based on their assessment of risk.

Licence holders should apply a graduated participant acceptance policy which requires more extensive CDD procedures to be undertaken on participants who represent a higher risk. However, even where a participant is considered to represent a lower risk of money laundering; a minimum standard of due diligence procedures must always be applied.

It is important to distinguish between the identification and verification of identity procedures on the one hand, and the wider CDD procedures which entail much more than the identification of a participant, whether a legal or natural person. The general CDD requirements and the nature of the information to be collected for each different participant type are covered in this Section of these guidance notes. The persons for whom information is to be obtained and the identification and verification of identity procedures which the GSC expects licence holders to apply are detailed in Section 4 of the Guidance. Exemptions and concessions from the identification requirements are also contained within Section 4.

CDD requirements apply at the outset of a participant relationship. They also apply, in relation to existing and continuing business relationships, when there is/are:

(a) A transaction that is suspected may be related to ML/FT.

(b) A pattern of behaviour that causes a licence holder to know or suspect that the behaviour is or may be related to ML/FT.

(c) Transactions or patterns of transactions that are complex or unusually large and which have no apparent economic or visible lawful purpose.

(d) Unusual patterns of transactions that have no apparent economic or visible lawful purpose.

(e) The licence holder becomes aware of anything which causes them to doubt the identity of the person who, in relation to the formation of the relationship, was the applicant for business.

(f) The licence holder becomes aware of anything which causes them to doubt the veracity or adequacy of CDD information and documentation already produced.

(g) A suspicion of ML/FT in respect of a person for whom identification evidence is not already held.

(h) A change in identification information of a participant.

(i) A change in underlying principals or third parties on whose behalf a business participant acts.

(j) A change in the beneficial ownership and control of a business participant.

(k) An absence of meaningful originator information on wire transfers.

3.2 A Risk-Based Approach to CDD

There are five stages within a risk-based approach to CDD requirements.

3.2.1 Stage 1- Collection of Relevant Information

CDD information comprises both identification and relationship information. To enable a participant profile to be prepared, licence holders must collect relevant CDD information on a risk sensitive basis to determine how and how far this should be done on the following:

(a) The participant;

(b) The beneficial ownership and control of the business participant;

(c) The nature of the participant's business and the participant's economic circumstances;

(d) The anticipated relationship with the licence holder; and

(e) The source of funds.

Whereas a participant will always be an individual natural person, a business participant will be one of the following:

(a) An individual natural person;

(b) The trustee of an express trust or other similar legal arrangements where they are acting on behalf of these entities; or

(c) A legal person – bodies corporate, foundations, anstalts, partnerships, associations, or any similar bodies that can establish a permanent business participant relationship with a licence holder.

Underlying principals of a business participant are the individuals who ultimately own or control a relationship, and/or the individuals on whose behalf the relationship is being conducted.

The Isle of Man Government considers it vitally important for the international standing and economic well-being of the Isle of Man that it conforms to established international standards for combating ML/FT. The FATF Recommendations and the Basel CDD principles both state the importance of

knowing the identity of the beneficial owner and/or underlying principals and of not operating anonymous accounts.

Licence holders must, in all cases, know the identity of underlying principals and/or beneficial owners at the outset of a business relationship. This is irrespective of the geographical origin of the client, or of the complexity of a legal structure.

As per paragraph 4 of the Codes, licence holders must not keep anonymous accounts or accounts in fictitious names.

Licence holders must properly identify and verify the identity of the participant in accordance with the Codes and the guidance notes.

In all cases the participant identification and verification records should be available to the Compliance Officer, MLRO, other appropriate staff and competent authorities.

Profiling participants

Certain types of product or service may provide an opportunity to build generic templates that predict expected patterns of activity. More complex products or services will require individual participant profiles.

It is important that participant profiles are kept up to date to reflect changing circumstances (see Section 5).

The participant profile must contain sufficient information on the rationale for the relationship and the nature of the activity that the participant expects to undertake in order for a licence holder to be able to:

(a) predict a pattern of expected activity within each participant relationship;

(b) Identify unusual complex or higher risk activity that may indicate ML/FT.

Identification information and the relationship information to be collected for each of the above participant types are described in the following Sections.

<u>The following situations 1 to 4 will apply to licence holders:</u>

Situation 1: Where the participant is a natural person

(a) Obtain identification information on the natural person.

Situation 2: Where the business participant is a legal person

(a) Obtain identification information on the legal person.

(b) Obtain identification information on the underlying principals i.e. persons exercising control over the management of the legal person, or any person(s) having power to direct the activities of the legal person. This will include directors or persons in equivalent roles, and account signatories.

(c) Obtain identification information on any person(s) purporting to act on behalf of the legal person or by whom binding obligations may be imposed on the legal person. This will include persons holding powers of attorney.

(d) Obtain identification information on the beneficial owners i.e. any individual who ultimately owns or controls a business participant.

Situation 3: Where the business participant is a trustee of an express trust

(a) Obtain identification information on the business participant i.e. the trustee(s) or other persons controlling the applicant.

(b) Obtain identification information on the trust.

(c) Obtain identification information on the underlying principals i.e. the settlor(s) or other persons by whom the arrangement is made, protector(s), any other person having power to direct the activities of the applicant, any person(s) whose wishes the trustee may be expected to take into account, known beneficiaries and potential beneficiaries presenting a higher risk.

(d) Obtain identification information on any person(s) purporting to act on behalf of the trustee(s) or by whom binding obligations may be imposed on the trustee(s).

Situation 4: Where the business participant is acting other than as principal (except as trustee)

(a) Obtain identification information on the participant.

(b) Obtain identification information on the underlying principals (natural person, legal person or trustee of an express trust) on whose behalf the applicant is acting).

(c) Obtain information concerning the relationship between the business participant and the underlying principals.

In all of the above situations, relationship information must be obtained (for express trusts, the relationship information to be obtained is on the express trust). Relationship information to be collected is outlined at Section 3.3.

The identification information that must be collected in respect of each type of participant is contained in Section 4.

3.2.2 Stage 2 – Assess and Evaluate Relevant Information

On the basis of the information collected at Stage 1, or on the basis of the nature of the relationship, licence holders must evaluate the information against the risk areas identified by the risk assessment required by the Codes. Consideration must then be given to whether it is appropriate to collect further information on the applicant, on any underlying principals and on the relationship to be established.

In respect of any proposed relationship, licence holders must always ensure they understand:

(a) why an applicant for business has requested a particular product or service;

(b) details of any existing relationships with the licence holder;

(c) the nature and frequency of the participant's expected activity paying due regard to any linked accounts or other activity;

(d) the ownership and control structure of legal persons and arrangements.

For companies this would include identifying the underlying principals and beneficial owners as outlined above.

For trusts this would include identifying the Settlor or other person by whom the arrangement is made, the Trustee or other person(s) controlling the applicant, any other person whose wishes the trustee may be expected to take into account and the beneficiaries;

(a) the various relationships between signatories and underlying principals;

(b) the nature of a participant's business activities or occupation;

(c) the source of the funds for the product or transaction in question; and

(d) where relevant, the source of income or wealth of the participant (see Section 3.4).

For many simple relationships the reasons for a relationship may be self-evident. However, for more complex products/services they may not be. Not all participants, products or services carry the same ML/FT risk and a risk-based

and proportionate approach should be adopted in determining the amount of CDD information required in each case.

3.2.3 Stage 3 – Determine Initial Risk Profile

On the basis of Stages 1 and 2, licence holders must determine and record a risk profile for the relationship. This should show whether the participant is to be treated as standard risk or where additional CDD is required. It will determine which underlying principal's identity needs to be verified, how identity is to be verified and the ongoing CDD to be conducted throughout the course of the relationship. For higher risk relationships, enhanced CDD must be performed.

Licence holders should consider whether inconsistencies between the CDD information obtained, specific information concerning source of funds or source of wealth, and the nature of transactions increases the participant's risk classification.

The risk profile should be reviewed and updated throughout the relationship.

3.2.4 Stage 4 – Verify the Identity of the Participant and any Underlying Principals

Licence holders must satisfactorily verify the identity of the participant where appropriate as required by the Codes or where the risk profile indicates that verification should be carried out, but must always verify identity in all relationships with a business participant (including the identity of any underlying principals).

Identity should normally be verified before or during the course of establishing a relationship. Sometimes, in the normal course of business and where there is little risk of ML/FT occurring, it is necessary to start a relationship before the verification of identity procedure can be completed. In such cases, verification procedures must be completed as soon as reasonably practicable. Licence holders must ensure that the money laundering and/or terrorism financing risks are effectively managed. Controls must be placed on the nature of the activity that can be undertaken before the verification of identity procedures have been completed. Requirements for verifying identity are set out in Section 4.

3.2.5 Stage 5 – Conduct Ongoing Due Diligence

Licence holders should review the CDD information held in relation to all participants on a periodic basis, and for higher risk ones, at least annually. The opening of a new account or a meeting with the participant may provide an

opportunity to confirm or update the information held in respect of that participant. Further detailed guidance is contained in Section 5.

Procedures should ensure that up-to-date CDD information is readily accessible to the MLRO (and any designated person), and to the GSC and the Financial Crime Unit (FCU) on request.

3.3 Collecting Relationship Information

Unless it is obvious from the product being provided, the following must be established:

In all Situations

(a) Purpose and intended nature of relationship
(b) Expected type, volume and value of activity
(c) Expected geographical sphere of the activity
(d) Activity providing the source of funds for the relationship and geographical sphere of the activity
(e) Details of any existing relationships with the licence holder

Express Trusts – Additional information (business participants)

(a) Type of trust (e.g. fixed interest, discretionary, testamentary)
(b) Structure of any underlying companies (if applicable) and nature of activities undertaken by the trust and any underlying companies (having regard for sensitive activities and trading activities)
(c) Classes of beneficiaries, including charitable causes named in the trust deed.
(d) Name of trustee's regulator, if applicable

Legal Persons – Additional information (business participants)

(a) Company and, if applicable, group ownership and structure enough to understand the ownership and control structure
(b) Nature of activities undertaken (having regard for sensitive activities and trading activities)
(c) Geographical sphere of the legal person's activities and assets
(d) Name of regulator, if applicable

3.4 Source of Funds, Income and Wealth – Taking a Risk Based Approach

A licence holder is expected to understand the source of funds for all applicants.

When entering a new relationship licence holders must understand the source of income or wealth for higher risk applicants.

Source of funds includes the immediate source of funds from which property has derived i.e. a bank account. Knowing who provided the funds and the account is necessary in every case. Licence holders are reminded that no third party funding is permitted.

Source of wealth is distinct from source of funds and describes the origins of a participant's financial standing or total net worth i.e. those activities which have generated a participant's funds and property. Information regarding source of income or wealth should be obtained for all higher risk relationships.

3.5 PEPs

Much international attention has been paid in recent years to PEP risk, the term given to the risk associated with providing financial and business services to those with a high political profile or who hold public office. PEP status itself does not automatically mean that the individual is corrupt nor that they have been incriminated in any corruption. However, their office and position can leave them vulnerable to corruption. The risks increase when the person concerned is from a country with widely-known problems of bribery, corruption and financial irregularity within their governments and society. This risk is even more acute where such countries do not have adequate AML/CFT standards, or where these do not meet international financial transparency standards.

PEPs are defined in the Codes in paragraph 2 and include natural persons, resident outside the Isle of Man, entrusted with prominent public functions and their immediate family members, and close associates. This definition would include royal families as well as persons entrusted with prominent public functions.

Prominent public functions include:

(i) a head of state, head of government, minister or deputy or assistant minister;
(ii) a senior government official;
(iii) a member of parliament;
(iv) a senior politician;
(v) an important political party official;
(vi) a senior judicial official;
(vii) a member of a court of auditors or the board of a central bank;
(viii) an ambassador, chargé d'affaires or other high-ranking officer in a diplomatic service;
(ix) a high-ranking officer in an armed force; and
(x) a senior member of an administrative, management or supervisory body of a state-owned enterprise;
(xi) a senior official of an international entity or organisation; and

(xii) an honorary consul.

Immediate family members include:

(i) a spouse;
(ii) a partner considered by national law as equivalent to a spouse;
(iii) a child or the spouse or partner of a child;
(iv) a brother or sister (including a half-brother or half-sister);
(v) a parent;
(vi) a parent-in-law;
(vi) a grandparent; and
(vii) a grandchild.

Close associate includes any natural person:

(i) who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with such a person;
(ii) who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of such a person; and
(iii) who is in a position to conduct substantial financial transactions on behalf of such a person.

Licence holders that handle the proceeds of corruption, or handle illegally diverted government, supranational or aid funds, face the risk of severe reputational damage and the possibility of criminal charges for having assisted in laundering the proceeds of crime. Licence holders also face the risk of constructive trust suits in such situations.

The Isle of Man as a jurisdiction faces considerable reputational damage should any of its licence holders have a relationship of this nature involving the proceeds of foreign corruption.

Licence holders can reduce risk by conducting detailed CDD at the outset of the relationship and on an ongoing basis where they know or suspect that the business relationship is with a PEP.

All licence holders must assess which countries with which they have financial relationships are most vulnerable to corruption. Licence holders that are part of an international group might also use the group network as another source of information.

Where licence holders do have business in countries vulnerable to corruption, they must establish who are the senior political figures in that country and, must seek to determine whether or not their participant has any connections with such individuals (e.g. they are immediate family or close associates). Licence holders should note the risk that individuals may acquire such connections after the business relationship has been established.

The Codes requires licence holders to have in place enhanced CDD measures to address PEP risk.

In particular, detailed CDD must include:

(a) Appropriate procedures to determine, as far as reasonably practicable, whether a participant, any natural person having power to direct the activities of a business participant, a beneficial owner or a known beneficiary of a legal arrangement is a PEP.

(b) Close scrutiny of any complex structures (e.g. involving companies, trusts and multiple jurisdictions) so as to establish that there is a clear and legitimate reason for using such structures. It should be borne in mind that most legitimate political figures would expect their personal affairs to be undertaken in a more than usually open manner, rather than the reverse.

(c) Every effort to establish the source of income/wealth (including the economic activity that created the wealth) as well as the source of funds involved in the relationship, establishing that these are legitimate, both at the outset of the relationship and on an ongoing basis.

(d) Approval of senior management before commencing the business relationship and regular review, on at least an annual basis, of the development of the relationship.

(e) Close scrutiny of any unusual features, such as very large transactions, the use of government or central bank accounts, particular demands for secrecy, the use of cash or bearer bonds or other instruments which break an audit trail, the use of small and unknown financial institutions in secrecy jurisdictions and regular transactions involving sums just below a typical reporting amount.

There should be full documentation of the information collected in line with the above. Given the above safeguards, the GSC would not necessarily expect licence holders to avoid or close relationships with PEPs. If the risks are understood and properly addressed, then the acceptance of such persons becomes a commercial decision as with all other types of participant.

New and existing participants may not initially meet the definition of a PEP. Licence holders should, as far as practicable, be alert to public information relating to possible changes in the status of its participants with regard to political exposure. Where an existing participant is subsequently found to be a PEP, senior management approval to continue the relationship must be sought.

Licence holders may wish to make use of independent electronic data sources which can be of particular value in the context of business relationships with PEPs.

Licence holders should not enter into or continue a business relationship where they know or have reasonable grounds to suspect that the funds derive from

bribery, corruption or the misuse of national or supranational assets, without prejudice to any other obligation they may have under criminal law or other applicable laws. However, closing out any such relationship must be subject to preliminary discussion with the FCU.

SECTION 4 - IDENTIFICATION AND VERIFICATION

The Codes require licence holders to establish, maintain and operate procedures which require participants to provide satisfactory information as to their identity. The GSC has set out below guidance on how licence holders should identify and verify participants' identity.

Licence holders must use their risk assessment to determine the measures to be taken when carrying out due diligence as required by paragraph 6, 7, 8 and 9 of the Codes. Licence holders must determine the extent of participants' due diligence measures over and above the minimum requirements to be undertaken, on a risk sensitive basis and depending on the risk posed by the participants and their level of gambling.

A licence holder should be alert to any relevant matter that may arise during the account opening process for the player and also ensure that their policies and procedures for managing ML/FT risks are kept under regular review.

4.1 Identification of Individual Participants

In accordance with Paragraph 6 of the Codes, the GSC expects licence holders to identify all players before they open an account or accept any money from them, and before any online gambling takes place. In order to do this, licence holders must obtain the following information concerning all players:

(i) full name;
(ii) residential address including postcode (or equivalent);
(iii) date of birth;
(iv) place of birth; and
(v) nationality

It is necessary to establish the participant's nationality in order to establish whether the player is a citizen of a nation which is subject to the sanctions by the United Nations or any other official body or government which would prohibit them partaking.

The participant should be required by the terms and conditions of business between the licence holder and the participant, to advise the licence holder immediately or as soon as practical thereafter, of any changes in the above information to that provided on registration.

4.2 Evidence of Identity

For those players whose withdrawals from their account exceed €3,000, in any 30 day rolling period (defined in Paragraph 7(3) of the Codes as a "qualifying

payment"), licence holders must establish, maintain and operate procedures to obtain satisfactory documentary evidence of the player's identity and their address.

The GSC considers that the following evidence should be obtained:

Documentation for evidence of identity

Before making a qualifying payment, documentation should be obtained and retained to support, or give evidence to support, the identity of the player.

Identification documents, either originals, photocopies, faxed or computer scanned copies should be clear and legible, bear a signature of the player, be within the expiry period, and show valid and clear document numbering (e.g. Passport Numbers). Where reliance is being placed on faxed or computer scanned copies, licence holders need to be vigilant, as such copies can be altered or modified. Examples of acceptable identification documents are as follows:-

(i) current valid "full" passport; or
(ii) Armed Forces ID card; or
(iii) known employer ID card; or
(iv) provisional or full driving licence; or
(v) government issued national identity card

All documents should be plainly legible. Where players put forward documents with which a licence holder is unfamiliar, either because of origin, format or language, the licence holder must take reasonable steps to verify that the document is indeed genuine, which may include contacting the relevant authorities.

Documentation for evidence of address

Licence holders should take appropriate steps to evidence the residential address of each player. The GSC has set out below some examples of acceptable methods to evidence the player's residential address:

(i) requesting either an original, photocopy, faxed or computer scanned copy of a recent rates, council tax or utility bill. Care must be taken that the document is not more than 3 months old. Mobile telephone bills are not acceptable as evidence of address;

(ii) an account statement from a recognised bank or recognised bank credit card. The statement should be the most recent available. Statements featuring a "care of" or accommodation address are not acceptable. Non-bank cards, such as store cards are not acceptable;

(iii) checking a register of electors;

(iv) making a credit bureau check which should validate various address and identity details;

(v) using an address validation/verification service, whether stored electronically or by other means;

(vi) a recent mortgage statement from a recognised lender.

Whichever method or combination of methods are followed, a copy of any relevant document or documents should be retained, either physically or electronically, to evidence that this has been undertaken (see Section 7 of these guidance notes).

Where a player's address is temporary accommodation, (for example an expatriate on a short term contract in the Middle East) or is a Post Office (PO) Box number, licence holders should adopt flexible procedures to obtain evidence.

Irrespective of the method used, the GSC expects licence holders to be able to produce evidence of the procedures followed, and that these procedures are adequate, together with any documentary or electronic evidence arising from such procedures.

Additional player information required for qualifying payments

Prior to making a qualifying payment to a player, the licence holder should also obtain the following further information:

(i) any former names, any aliases used and reason for any aliases;
(ii) place of birth; and
(iii) nationality.

It should be noted that this additional information need not be specifically evidenced by the licence holder. However, depending on the jurisdiction of the player, part of this information is likely to be contained in the evidence obtained from the player under section 4.2 of these guidance notes.

The GSC recognises that licence holders may have alternative systems to evidence a player's identity and address, which provide the same degree of comfort and assurance as the procedures set out above. If a licence holder wishes to use such alternative systems, the GSC has no objection, provided that they all fully comply with the Codes.

The participant should be required by the terms and conditions of business between the licence holder and the participant, to advise the licence holder immediately, or as soon as practical thereafter, of any changes in the above information to that provided on registration.

4.3 Evidence of Identity for Business Participants

In accordance with paragraph 8 of the Codes, licence holders must require a business participant to produce satisfactory evidence of its identity before they open an account or accept any money from it. A business participant means any player that is participating in online gambling in the course of business. This will include (but is not limited to) any corporate body, trust or other entity or organisation set up on behalf of a beneficial owner.

An individual participant not acting in the course of business need only provide satisfactory evidence of their identity if they make a qualifying payment. This differs from business participants as business participants must provide satisfactory evidence of their identity as soon as reasonably practicable after first contact is made.

Paragraph 8(2) of the Codes provides that a licence holder must, in the case of all business participants:

- understand the ownership and control structure of the business participant;
- determine the legal status of the business participant and who is the ultimate beneficial owner;
- verify that any person purporting to act on behalf of the business participant is authorised to do so;
- obtain satisfactory evidence to identity and take reasonable steps to verify the identity of those persons or any natural persons having power to direct the business participant's activities, using relevant information or data obtained from a reliable source; and
- obtain satisfactory evidence to identify and take reasonable steps to verify the identity of the beneficial owner, using relevant information or data obtained from a reliable source.

Documentation for evidence of identity

Before entering into a business relationship with any business participant, documentation should be obtained and retained to support the identity of the business participant. Identification documents should be originals, photocopies, faxed or computer scanned copies and must be clear and legible. Where reliance is being placed on faxed or computer scanned copies licence holders need to be vigilant as such copies can be altered or modified. Examples of acceptable identification documents are as follows:

- Certificates of incorporation in respect of a company;
- Constitutional documents e.g. Memorandum and Articles of Association, trust deeds;
- Details and nature of the business participant's business;
- An indication as to the activity to be expected i.e. details of volume and value of transactions anticipated;

- Satisfactory evidence of each of the beneficial owners and any persons on whose instructions the signatories may act;
- Satisfactory evidence of the directors or trustees;
- Satisfactory evidence of the identity of account signatories;
- A copy of a board resolution authorising the opening of the account in respect of a company;
- Copies of powers of attorney or any other authority affecting the operation of the account.

A risk based approach must be applied in respect of satisfactory evidence. Satisfactory evidence is as per 3.3 of these guidance notes and should be obtained in respect of beneficial owners, signatories and directors and/or trustees. In the case of numerous beneficial owners, directors and/or trustees a common sense approach should be applied.

The business participant should be required, by the terms and conditions of business between the licence holder and the business participant, to advise the licence holder immediately, or as soon as practical thereafter, of any changes in the above information to that provided on registration. In addition the licence holder should conduct periodic checks to ensure the information they hold is correct and up to date such as by conducting company searches.

4.4 Enhanced Participant Due Diligence

Paragraph 9 of the Codes require that where a licence holder has assessed a participant as posing a higher risk of ML/FT the licence holder must conduct enhanced due diligence in respect of that participant.

4.4.1 PEPs

A participant will be assessed as posing a higher risk if he is or has a substantial connection with a PEP. A person will be deemed to be a PEP if he falls within the definition as set out in paragraph 2 of the Codes and includes any person outside the Isle of Man who is or has been entrusted with prominent public functions and specific members of their family.

Establishing whether individuals are PEPs is not always straightforward and can present difficulties. Resources such as Transparency International's Corruption Perceptions Index which ranks approximately 180 countries and territories according to their perceived level of corruption, may be helpful in terms of assessing the risk or subscription to a specialist PEP database.

It is important to monitor the status of a participant as although a party may not be a PEP at the time of registration he may later become a PEP and vice versa. If a PEP ceases to be so, this does not automatically indicate that enhanced due diligence is no longer required. A risk based approach should be applied.

All licence holders should assess who are the senior political figures within the countries in which they do business and seek to determine whether or not any participant has any connections with such individuals. Licence holders should note the risk that parties may acquire such connections after the business relationship has been established.

The participant should be required by the terms and conditions of business between the licence holder and the participant, to advise the licence holder immediately, or as soon as practical thereafter, of any changes in the above information to that provided on registration.

4.4.2 Countries Non-Compliant with FATF Recommendations

FATF has issued recommendations with a view to combating ML/FT within jurisdictions. The IMF determines whether a particular jurisdiction is compliant with these recommendations.

A list of countries which are currently compliant with the FATF Recommendations can be found at Schedule 1 to the Codes, which are in Appendix A and B to these guidance notes. Any participant which is resident or conducting business in a country other than those listed in Schedule 1 to the Codes (i.e. countries non-compliant with the FATF Recommendations) should be assessed as posing a higher risk of money laundering and or terrorist financing. As such enhanced player due diligence may need to be carried out in respect of that relationship.

A risk based approach should be adopted: the higher the risk perceived by the licence holder to be posed by a particular country, greater levels of due diligence should be carried out.

4.4.3 Notices Issued by Isle of Man Government and/or the GSC

From time to time the Isle of Man Government and the GSC may issue notices or warnings in respect of certain persons, legal persons or legal arrangements.

The licence holder must take all steps reasonable to ascertain whether any such person, legal person or legal arrangement has any connection and/or business relationship with the licence holder. This should include making appropriate staff aware of the fact that such a notice or warning has been given.

Where a notice or warning has been given in respect of a participant, the licence holder should carry out enhanced due diligence.

4.4.4 Paragraph 9(3) of the Codes

Under Paragraph 9(3) of the Codes, enhanced participant due diligence means (in addition to the checks contained in Paragraphs 6, 7, and 8 of the Codes):

(a) considering whether additional identification data needs to be obtained;

(b) considering whether additional aspects of the participant's identity or the identity of the business participant need to be verified;

(c) taking reasonable measures to establish the source of any funds and of the wealth of the participant and any beneficial owner and underlying principal; and

(d) considering what ongoing monitoring should be carried on in accordance with paragraph 10 of the Codes.

4.5 Additional Checks

The GSC considers that in addition to the information provided by the player in Sections 3.1, 3.2 and 3.3 of these guidance notes, and as a form of additional verification of players, licence holders should ensure that, as part of their online registration process, the following types of controls should be in place to know their player:

(i) An Internet Protocol (IP) address check of the registrant login. This will assist in denying a participant from taking part in online gambling from sanctioned countries or "unknown" addresses, based on this IP address. This control should also check for consistency against the country/region of registration details supplied by a player;
(ii) A participant database check, which should test for duplicate registration details of a player or previous accounts held;
(iii) A validation of the participant registration data against the licence holder's blacklisted persons;
(iv) A validation of registration data against recent/previous attempts.

The licence holder must maintain a record of when any automated check is overridden. A complete explanation of the reason for overriding the check must form part of the record, and must be signed by the person authorising the system override, or if electronic means are used, then the identity of the person authorising the override must be shown, e.g. by means of a password, or electronic signature.

4.6 Other Matters

(a) Persons without standard identification documentation

Due to the worldwide nature of licence holders' businesses, the GSC is aware that some players may not be able to produce the usual types of evidence of identity, such as a driving licence or passport. In these circumstances, the GSC recommends that licence holders adopt a common sense approach and some flexibility. Such participants are generally able to provide an original, photocopy, faxed or computer scanned copy of other documents, which cumulatively give licence holders comfort regarding the identity and address of the player.

Licence holders may apply some flexibility in evidencing a participant's identity and residential address, but it must always be remembered that the rigorous anti-money laundering and/or terriorism financing procedures must not be compromised. It is expected that such procedures should only be used sparingly, and only in the limited circumstances described above. In each case there should be a review and sign off procedure undertaken by either the MLRO or a person of an appropriate level of authority.

(b) Translation of documents in a foreign language

Licence holders should ensure that, where appropriate, any documents in a foreign language can be adequately translated into a language that is understood by the licence holder's MLRO or their staff, so that the true significance of the document may be appreciated. Licence holders who employ staff fluent in more than one language may hold such documentation in a non-translated form only if it has been signed off by a person of adequate authority, and if a translation into a language understood by the MLRO (and also understandable to the authorised officers of the GSC) can be obtained at any time. All staff members translating the documents must be fluent in both the language it is to be translated into, as well as in the language of the document received.

(c) Existing Accounts

Licence holders must obtain full identity details of all of their players, and evidence of identity, where applicable, to comply with the Codes. All accounts established prior to the implementation of the Codes, which are still in use, must comply fully with the Codes.

(d) Face-to-face

Where there is any direct face-to-face contact between a participant and a member of the licence holder's staff, or its group's staff, the participant can show such staff original documents, and copies can be taken immediately and retained.

4.7 Introduced Business

When considering an introduced application for business, licence holders should note that an introducer procedure does not represent an exemption from a licence holder's obligations under the legislation. All information and documentation must still be received and maintained by the licence holder.

SECTION 5 - ONGOING MONITORING OF PARTICIPANTS ACCOUNTS

5.1 Introduction

Once the identification and verification procedures have been completed and the relationship is established, licence holders must monitor the conduct and activities of the participant to ensure that they are consistent with the risk profile, source of funding and estimated turnover that was determined when the relationship was established.

Effective ongoing monitoring is vital to maintain a proper understanding of a participant's activities, and is an integral part of any effective AML/CFT programme. It is key to allowing a licence holder to detect unusual or suspicious activity. An unusual transaction may be in the form of activity that is inconsistent with the expected pattern for that relationship, or with the normal activities for the type of product or service that is being delivered. Complex, large and unusual transactions or patterns of transactions that have no apparent visible or economic purpose may indicate ML/FT.

Failure to adequately monitor participants' activities could expose a licence holder to potential abuse by criminals, and may call into question the adequacy of the systems and controls, as well as the prudence, the integrity, the competence or the character and status of the management of licence holders.

Licence holders must give special attention to relationships and transactions with countries that do not sufficiently apply the FATF Recommendations. Particular attention must be paid to transactions and business connected with countries and territories assessed as higher risk or which have been classified by the FATF as non-cooperative in the fight against money laundering and terrorist financing.

In determining which jurisdictions do not, or insufficiently apply the FATF Recommendations, a licence holder may consider:

(a) Findings of reports conducted by the FATF, FATF-style regional bodies, the Offshore Group of Banking Supervisors, the IMF, and the World Bank.

(b) Its own experience or the experience of other group entities (where part of a multi-national group) which may have indicated weaknesses in other jurisdictions.

Where the basis of the relationship changes significantly, licence holders must carry out further CDD procedures to ensure that the revised risk and basis of the relationship is fully understood. Ongoing monitoring procedures must take account of these changes.

Licence holders must ensure that any updated CDD information obtained through meetings, discussions, or other methods of communication with the participants is recorded and retained with the participants' records. That information must be available to the MLRO.

Ongoing monitoring of a participant's activities will allow licence holders to continue to build a profile of the participants, and will entail the ongoing collection of CDD information.

The GSC is aware that some or all duties of participants' support staff may be sub-contracted by licence holders. In these instances, the GSC expects the licence holders to ensure that their sub-contractor's staff are aware of their responsibilities concerning the monitoring of participants' accounts. This function may be carried out either by the licence holder or by the sub-contractor, but the responsibility to ensure that it has been carried out rests with the licence holder.

5.2 Monitoring – Taking a Risk-Based Approach

The extent of monitoring will be linked to the risk profile of the participants which has been determined through the risk assessment required by paragraph 5 of the Codes. To be most effective, resources should be targeted towards relationships presenting a higher risk of ML/FT.

Licence holders should have particular regard to whether a relationship poses a higher risk. High risk relationships, for example (but not limited to) those involving PEPs, will generally require more frequent intensive monitoring. In order to monitor high risk situations, a licence holder must consider:

(a) whether it has adequate procedures or management information systems in place to provide relationship managers and reporting officers with timely information, including information on any connected accounts or relationships;

(b) how it will monitor the sources of funds, wealth and income for higher risk participants and how any changes in circumstances will be recorded;

(c) conducting regular independent review of CDD information, activity and transactions.

5.3 Monitoring – Methods and Procedures

Under paragraph 10 of the Codes all licence holders must have systems and controls in place to monitor and record, on an ongoing basis, the activity on all participant accounts. The purpose of this monitoring is to enable licence holders to detect any transactions which are significantly different to the normal pattern of transactions or player behaviour or are suspicious, which may be indicative of money laundering and/or terrorist financing activities. Possible areas for consideration when monitoring may include: -

(a) transaction type

(b) frequency

(c) amount

(d) geographical origin/destination of funds

(e) attempted payment into accounts by/to third parties

(f) unusual gambling strategies

(g) different names on debit/credit cards used

(h) failed debit/credit card transactions

A copy of policies and procedures should be available to the GSC if requested, and the licence holder should be able to provide a demonstration of these procedures if requested.

The GSC believes that the most effective method for the monitoring of participant accounts is achieved through a combination of computerised and manual solutions. A corporate compliance culture, and properly trained, vigilant staff through their day-to-day dealing with participant accounts, should form an effective monitoring method. An additional computerised approach may be to include the setting of "floor levels" for monitoring the accounts by amount.

Whilst some licence holders may wish to invest in expert computer systems specifically designed to assist in the detection of fraud, money laundering and terrorist financing, the GSC recognises that this may not be a practical option for many licence holders for the reasons of cost, the nature of their business, or difficulties of systems integration.

It is not just new business relationships which may be used to launder money or finance terrorism. Relationships with existing and long-standing players should also be monitored closely for money laundering and terrorist financing.

5.4 Electronic Payment and Message Systems

In order to comply with the requirements of the FATF and EU Regulations which have been adopted by the Isle of Man, licence holders must ensure that details of senders and beneficiaries are incorporated in all payment messages sent via electronic payment and message systems.

The GSC expects that the following information should be included as a minimum:

(a) Bank account number

(b) Name of account

(c) Name of bank

(d) Address of branch

(e) Branch sort code

Where the required information is not present, or the information is not precise (e.g. the remitter of the funds is not shown as the "player", due to the funds having been first passed through an intermediary's suspense account), licence holders should reject the transfer of funds. Licence holders may, however, hold the received funds on a (non-interest paying) suspense account for a period of no more than seven bank working days, while ascertaining the source of the funds. If the origin and source of the funds have not been ascertained at the end of that time, the funds should be rejected.

Licence holders should be vigilant of attempts to obscure the ownership or origin of funds, and in particular should be cautious where the payment originates in any jurisdiction known to apply secrecy provisions to its banking and financial operations and their dealings with account holders, which could include countries that are FATF members.

Records of all electronic payments and messages must be retained in accordance with Paragraphs 13 and 14 of the Codes. (See Section 7 of these guidance notes).

5.5 Recognising and Evaluating Suspicious Transactions and Activity and Suspicious Attempted Transactions

5.5.1 The importance of CDD Information to the Recognition and Evaluation of Suspicious Activity and Suspicious Attempted Activity

Satisfactory CDD procedures provide the basis for recognising unusual and suspicious transactions and events. An effective way of recognising suspicions is knowing enough about participants, their particular circumstances and their normal expected activities to recognise when a transaction or instruction, or a series of transactions or instructions, is abnormal.

Sufficient guidance must be given to staff to enable them to form a suspicion or to recognise when ML/FT is taking place. This should involve training that will enable appropriate staff, adequately and responsibly, to seek and assess the information that is required for them to judge whether a transaction or instruction is suspicious in the circumstances. Guidance and training will need to take account of the nature of the transactions and instructions that staff are likely to encounter, the type of product or service.

Further guidance on staff training is provided at Section 8.

5.5.2 What Constitutes Knowledge and Suspicion of Money Laundering or Terrorist Financing?

Licence holders have an obligation to report where there is knowledge or suspicion of money laundering or terrorist financing (see Section 6 below).

Generally speaking, knowledge under POCA means actual knowledge, which came to that person in the course of a business in the regulated sector or (for the nominated officer) in consequence of a disclosure made by another employee. Knowledge may be imputed however, such as if there has been a failure to ask obvious questions.

Suspicion is more subjective. Suspicion is personal and falls short of proof based on firm evidence. Suspicion has been defined by the courts as being beyond mere speculation and based on some foundation. For example, it has been held that:

> *"the essential element in the word "suspect" and its affiliates… is that the Defendant must think that there is a possibility,*

which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice."[2]

As the types of transactions which may be used by money launderers and financiers of terrorism are almost unlimited, it is difficult to determine what will constitute a suspicious transaction. However, it is important to properly differentiate between the terms "unusual" and "suspicious".

The key is knowing enough about the participant to recognise that a transaction, or a series of transactions, is unusual and from an examination of the unusual, whether there is a suspicion of ML/FT.

Where a transaction is inconsistent in amount, origin, destination, or type with a participant's known activities, the transaction must be considered *unusual*, and the licence holder put "on enquiry".

Where the licence holder conducts enquiries and obtains what he considers to be a satisfactory explanation of the activity or transaction, he may conclude that there are no grounds for suspicion, and therefore take no further action as he is satisfied with matters. However, where the licence holder's enquiries do not provide a satisfactory explanation of the activity or transaction, he may conclude that there are grounds for *suspicion*, and must make a disclosure.

One issue that should arouse the licence holder's attention is if the transaction or series of transactions has no commercial reason, or does not constitute the most logical, convenient or secure way to do business.

For a person to have knowledge or be suspicious, he does not need to know the exact nature of the criminal activity underlying the money laundering, or that the funds themselves were definitely those arising from the criminal offence.

5.5.3 What Constitutes Reasonable Grounds for Knowledge or Suspicion?

In addition to establishing a criminal offence when suspicion or actual knowledge of money laundering or terrorist financing is proved, Section 14 of the Anti-Terrorism and Crime Act 2003 provides for an offence to be committed where there are reasonable grounds to know or suspect that property relates to the funding of terrorism. This introduces an objective test of suspicion. The test would be likely to be met when there are facts or circumstances, known to an employee of a licence holder, from which another person in similar

[2] Per Longmore, LJ., R v Da Silva [2006] EWCA Crim 1654

circumstances would have inferred knowledge or formed the suspicion that terrorist financing was involved.

To defend themselves against a charge of failing to meet the objective test of suspicion licence holders and their employees would need to be able to demonstrate that they took reasonable steps in the particular circumstances to know the participants and the rationale for the transaction or instruction.

5.5.4 The Type of Situations Giving Rise to Suspicion

An illustration of the type of situations that might give rise to suspicion in certain circumstances are:

(a) unusual patterns of gambling; and

(b) gambling involving significantly large amounts of money.

This is not, however, an exhaustive list. The MLRO or relevant senior management should consider all the circumstances and be prepared to ask further questions, if necessary.

5.5.5 Questions to Ask When Assessing Suspicious Activity

The following factors should be borne in mind when seeking to identify a suspicious transaction:

(a) is the transaction in keeping with the participant's normal activity known to the licence holder?

(b) does the IP address check indicate that the country/region in which the participant is located has changed?

(c) is the transaction coming from, or going to, an unusual financial institution?

(d) is it a significant transaction (relative to a relationship)?

(e) has there been a material change in the operation of the account?

(f) is the operation of the account operated in a normal fashion?

(g) has there been a change in the existing participant's details which increases a risk profile?

(h) is the participant known personally?

(i) is the transaction or pattern of transactions unusually complex?

(j) does the transaction or pattern of transactions have an apparent economic or visible lawful purpose?

(k) are there a number of transactions taking place at a value just below that of a Qualifying Transaction under paragraph 7(3) of the Codes?

This list is not intended to be exhaustive and is only to provide examples.

SECTION 6 - REPORTING SUSPICIONS AND CONTINUED SUSPICIONS

6.1 Reporting Suspicions and Continued Suspicions

POCA makes it an offence to fail to disclose knowledge or suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering. Likewise the Anti-Terrorism and Crime Act 2003 makes it an offence to fail to disclose where a person knows or suspects or has reasonable grounds for knowing or suspecting that a terrorist financing offence has been committed.

Once knowledge or suspicion (or in the case of terrorist financing, reasonable grounds for knowledge or suspicion) has been formed the following general principles must be applied:

(a) In the event of suspicion of money laundering, a disclosure must be made even where there has been no transaction by or through the licence holder.

(b) Disclosures must be made as soon as is practicable after the suspicion was first identified (See Section 6.2 below).

(c) Licence holders must ensure that they do not commit the offence of tipping off the participant or any other person who is the subject of the disclosure. Licence holders should also take care that their line of enquiry with participants is such that tipping off cannot be construed to have taken place. (Further guidance concerning tipping off is available under Section 6.8 below).

(d) Licence holders must ensure that any disclosure is made in good faith, as an absence of good faith may leave the licence holder open to legal action from the participant who may sue for breach of confidentiality or duty of care.

Paragraph 16(3)(c) of the Codes provides that licence holders must "establish, maintain and operate written internal procedures" which will require staff to make reports to the MLRO with any information or other matter which comes to their attention and in their opinion gives rise to a suspicion or knowledge that a participant is engaged in ML/FT or an attempt of ML/FT. The MLRO is required by paragraph 16(3)(d) of the Codes to "*consider any report in the light of all other relevant information available to him for the purpose of determining whether or not it gives rise to a knowledge or suspicion of money laundering or terrorist financing or attempted money laundering or attempted terrorist financing*". This

must also include staff of any sub-contractors, who may be providing support services to the licence holders.

6.2 The Timing of Disclosures

When a licence holder has suspicion or knowledge that money laundering is taking place, a disclosure must be made to the FCU as soon as is practicable. Disclosures can be made either before a suspicious transaction or activity occurs in circumstances where an intended transaction appears suspicious, or after a transaction or activity has been completed if the transaction appears suspicious only with the benefit of hindsight. Disclosures that are made after the activity or transaction has taken place are not intended as alternatives to reports that should have been made prior to the transaction or activity being processed or completed.

Licence holders must make the submission of a disclosure a priority, whilst at the same time ensuring that the disclosure itself is comprehensive and meaningful.

When a licence holder has suspicion or knowledge that ML/FT is taking place, the need for prompt disclosures is especially important where a participant has instructed the licence holder to move funds, close the account, or carry out significant changes to the business relationship. In the case of significant movement of funds licence holders must contact the FCU urgently, before funds are moved. This may be vital to avoid a constructive trust claim where it is suspected that the funds in question have been fraudulently obtained (see Section 6.8.2 below).

6.3 Internal Reporting Procedures

It is the responsibility of the MLRO (or if appropriate the deputy MLRO) to consider all internal disclosures he/she receives in the light of full access to all relevant documentation and other parties. All licence holders must ensure that the MLRO receives full co-operation from all staff and full access to all relevant documentation so that he/she is in a position to decide whether money laundering or terrorist financing is suspected or known.

Failure by the MLRO to diligently consider all relevant material may lead to vital information being overlooked and the suspicious transaction or activity not being disclosed to the FCU in accordance with the requirements of the legislation. Alternatively, it may also lead to vital information being overlooked which may have made it clear that a disclosure would have been unnecessary. As a result, the MLRO must document internal disclosures made by employees to record the results of the assessment of each disclosure and pursuant to paragraph 15(1)(b) of the Codes, establish and maintain in the Isle of Man, a register of all money laundering and financing of terrorism reports made to the MLRO or deputy MLRO.

The register established and made pursuant to paragraph 15(1)(b) of the Codes must be kept separate from other records and must contain details of:

(a) the date on which the report is made;

(b) the person who makes the report;

(c) whether it is made to the MLRO or deputy MLRO; and

(d) information sufficient to identify the relevant papers.

6.3.1 Setting Internal Reporting Procedures

Licence holders must ensure that:

(a) All employees are made aware of the identity of the MLRO and his/her deputy, and of the procedure to follow when making an internal disclosure report to the MLRO.

(b) All disclosure reports must reach the MLRO without any undue delay. Under no circumstances should reports be filtered out by supervisors or managers such that they do not reach the MLRO.

Reporting lines should be as short as possible with the minimum number of people between the employee with the suspicion and the MLRO. This ensures speed, confidentiality and accessibility to the MLRO.

Larger groups may choose to appoint an assistant MLRO within divisions or subsidiaries to enable the validity of disclosure reports to be examined before being passed to a central MLRO. In such cases, the role of the assistant MLRO must be clearly specified and documented. All procedures and responsibilities must be documented in appropriate manuals and job descriptions.

All suspicions reported to the MLRO must be documented (in urgent cases this may follow an initial discussion by telephone). The report should include the full details of the participants and as full a statement as possible of the information giving rise to the suspicion.

The MLRO must acknowledge receipt of the report and at the same time provide a reminder of the obligation to do nothing that might prejudice enquiries i.e. tipping off the participant or any other third party.

The reporting of a suspicion in respect of a participant, does not remove the need to report further suspicions that arise subsequently in respect of that participant. If other suspicious transactions or events occur, whether of the same nature or different to the previous suspicion, these new suspicions must continue to be reported to the MLRO as they arise. The MLRO must make repeated disclosures to the FCU when suspicious activity continues or re-occurs.

The requirement to report also covers situations where the business or transaction has not proceeded and as a result there is a suspicion of money laundering or terrorist financing (see Section 6.4).

6.3.2 Evaluating Internal Disclosures

When evaluating an internal disclosure, the MLRO must take reasonable steps to consider all relevant CDD information available within the licence holder concerning the participants, to whom the report relates. This may include making a review of other transaction patterns and volumes through connected accounts, any previous patterns of instructions, the length of the business relationship and reference to CDD information and documentation.

As part of the review, other connected accounts or relationships may need to be examined. Connectivity can arise through commercial connections e.g. linked accounts, introducers etc, or through connected individuals. The need to search for information concerning connected accounts or relationships should not delay making a report to the FCU.

The MLRO should document the evaluation process that they follow in each case and their reasons for their conclusions.

If after completing the evaluation, the MLRO decides that there are grounds for knowledge, suspicion or reasonable grounds to suspect ML/FT, he must disclose the information to the FCU as soon as practicable after his evaluation is complete. Nevertheless, care should be taken to guard against a report being submitted as a matter of routine to the FCU without undertaking reasonable internal enquiries to determine that all available information has been taken into account.

The MLRO will be expected to act honestly and reasonably and to make their determinations in good faith. Providing they do act in good faith in deciding not to pass on any suspicious transaction report, it is unlikely that there will be any criminal liability for failing to report.

6.4 Reporting Declined Business

The GSC understands that it is normal practice for licence holders to turn away business that they know is, or suspect might be, criminal in intent or origin. In such a circumstance licence holders must also make a disclosure to the FCU, albeit that no transaction or activity has taken place.

Reporting of such events will allow the FCU to build a clearer picture of the money laundering and terrorist financing threat to the Isle of Man, and to use such intelligence on a proactive basis. A further benefit of reporting such declined business is that money launderers and terrorist financiers will perhaps be discouraged from trying to place criminal business on the Isle of Man in future. This approach is consistent with developing international best practice.

6.5 Reporting Suspicions – Liaising with Law Enforcement

Knowledge or suspicion of money laundering or terrorist financing or attempted money laundering or terrorist financing in the Isle of Man or elsewhere must be disclosed to "a constable" serving with the FCU.

Any disclosure that is Customs & Excise related must be made to the FCU as per paragraph 20(2)(f) of the codes.

Disclosures or STRs should be sent directly to the following address and not to any other regulating authority:-

The Officer in Charge
The Isle of Man Constabulary
Financial Crime Unit
PO Box 51
Douglas
Isle of Man IM99 2TD

Tel: (01624) 686000 (Office hours)
Fax: (01624) 686039
Email: fcu@gov.im

The disclosure of suspicious transactions should only be made on the FCU's prescribed disclosure form. This form should then be forwarded directly to the FCU, at the address mentioned above.

Licence holders are encouraged to provide as much detail as possible and may wish to send supporting documentation with the prescribed disclosure form. In cases where licence holders inform the GSC of matters surrounding an imminent

disclosure, it is not sufficient to merely state on the disclosure to the FCU that the GSC has been informed, and nothing more. Licence holders may state that they have informed the GSC, but they must also provide full details of their knowledge or suspicion to the FCU on the disclosure form.

Failure to provide sufficient information at the outset may hinder the commencement or progress of an investigation by the authorities, and may result in a "consent letter" being initially withheld.

6.6 Recording Disclosures to the FCU

Under paragraph 15(1)(c) of the Codes licence holders must establish and maintain a register of all disclosures made to the FCU. It is not necessary to establish separate registers under the AML code and the CFT code. A single register covering both requirements of paragraph 20(5) of both Codes is sufficient provided it is clear that it does so.

The register must include details of the date of the disclosure, the person making the disclosure, the constable to whom the disclosure is being made (by reference to the disclosure acknowledgement from the FCU), and information to allow the papers relevant to the disclosure to be located.

6.7 Actions After Reporting

6.7.1 Acknowledgment of a Disclosure

Disclosing institutions will receive an acknowledgement in every case and appropriate advice and feedback wherever possible.

6.7.2 Investigation and the use of Court Orders

Following the receipt of a disclosure and initial enquiries by the FCU, reports are allocated to trained financial investigation officers for further investigation. Intelligence from reports submitted to the FCU may be disseminated by the FCU to other law enforcement or government agencies.

Where additional information is required from a reporting institution following a suspicious transaction report, it will generally be obtained pursuant to a production order issued by the court under POCA or an account monitoring order under the anti-terrorism legislation. Licence holders must ensure that they respond to all court orders within the required time limit and provide all of the information or material that falls within the scope of such orders. Licence holders are advised to check that the information supplied in compliance with an order is restricted to the information that is covered by the order. It cannot be

assumed that non-disclosable or privileged material, e.g. copies of legal advice, will be filtered by the authorities before the information leaves the Isle of Man.

During the course of an investigation, a licence holder may be served with a restraint order, designed to freeze particular funds or property pending the outcome of an investigation. A licence holder must ensure that it is able to freeze the relevant property that is the subject of the order. It should be noted that the restraint order may not apply to all funds or assets involved within a particular business relationship and licence holders should consider what if any property may be utilised subject to having obtained the appropriate consent from the FCU.

Upon the conviction of a defendant, a court may order the confiscation of his criminal proceeds and a licence holder may be served with a confiscation order in the event that it holds funds or other property belonging to that defendant that are deemed by the courts to represent his benefit from criminal conduct.

Property may also be forfeited in the Isle of Man utilising civil proceedings under anti-terrorism legislation.

6.7.3 Feedback From the FCU

Because a significant proportion of disclosures/STRs received by the FCU relate to the accounts or transactions of non-Isle of Man residents, it is not always possible for the FCU to provide detailed feedback on individual disclosures. However, on a regular basis, the FCU will provide statistics and give information on identified trends, as well as giving advice on common mistakes or other misunderstandings which will serve to enhance the quality of disclosures.

6.8 Avoiding Committing a Tipping Off Offence

6.8.1 Communicating with Suspected Participants and Their Advisers

The refusal to act upon a participant's request for a transaction to take place may lead to civil proceedings being instituted by the participant/business participant. In such cases a licence holder must notify the FCU. Licence holders should also seek legal advice on the information that they should disclose without 'tipping off' a suspected participant and/or his advisers. It may be necessary in such circumstances for the licence holder to seek the directions of the court.

Licence holders can reduce the potential threat of civil proceedings being instigated by suspected participants for breach of contract by ensuring that the

terms of business governing their participant relationships specifically exclude breaches in circumstances where following a participant instruction may lead to the commission of an offence.

6.8.2 Managing a Constructive Trust Scenario

A licence holder holding property that it knows, or suspects, or has reasonable grounds to suspect does not belong to its participant may be regarded in law as a constructive trustee. In such a situation the licence holder is deemed to hold the property on a constructive trust for the benefit of the actual owner of the property (referred to as the constructive beneficiary).

In such circumstances, a transfer of the property by a licence holder may constitute a breach of trust, even where the transfer is made with the "consent" of the FCU.

Although each case should be considered on its facts, effective use of CDD information including verification of source of funds and source of wealth where necessary can help licence holders to guard against potential constructive trust liability arising out of fraudulent misuse or misappropriation of funds as well as against money laundering and terrorist financing.

6.8.3 Terminating a Relationship

The consent letter issued by the FCU following a disclosure is provided to a licence holder as a defence against a charge of assisting to launder criminal funds or to assist in terrorist financing. It is not intended to override normal commercial judgement, and licence holders are not obliged to continue relationships with participants if such action would place them at commercial risk. However, it is recommended that, before terminating a relationship that has been the subject of a report, licence holders may wish to consider liaising with the FCU to enquire whether termination will place it in danger of tipping off the participant or prejudicing the investigation in any other way.

6.8.4 Tipping Off

The offence of tipping off is set out in section 145 of POCA, which provides that:

"145 Tipping off: regulated sector

(1) A person commits an offence if-

(a) the person discloses any matter within subsection (2);

(b) the disclosure is likely to prejudice any investigation that might be conducted following the disclosure referred to in that subsection; and

(c) the information on which the disclosure is based came to the person in the course of a business in the regulated sector.

(2) The matters are that the person or another person has made a disclosure under this Part [of the Codes]-

(a) to a constable or customs officer serving (in either case) with the Financial Crime Unit of the Isle of Man Constabulary; or

(b) to a nominated officer,

of information that came to that person in the course of a business in the regulated sector.

(3) A person commits an offence if-

(a) the person discloses that an investigation into allegations that an offence under this Part [of the Codes] has been committed, is being contemplated or is being carried out;

(b) the disclosure is likely to prejudice that investigation; and

(c) the information on which the disclosure is based came to the person in the course of a business in the regulated sector.

(4) A person guilty of an offence under this section is liable-

(a) on summary conviction, to custody for a term not exceeding 3 months, or to a fine not exceeding £5,000, or to both;

(b) on conviction on information, to custody for a term not exceeding 2 years, or to a fine, or to both.

(5) This section is subject to-

(a) section 146 (disclosures within an undertaking or group);

(b) section 147 (other permitted disclosures between institutions); and

(c) section 148 (other permitted disclosures etc).”

SECTION 7 - RECORD KEEPING

7.1 Introduction

Paragraphs 11 to 15 of the Codes provide obligations for a licence holder regarding record keeping.

Where a disclosure is made to a constable, records should be kept in accordance with Paragraph 13(3) of the Codes. (i.e. retained for "*as long as required by the constable.*")

Paragraph 14 of the Codes provides that a licence holder must ensure that any records that are required to be established and maintained under the Codes are:

(a) if the records are in the form of hard copies kept on the Isle of Man, capable of retrieval without undue delay;

(b) if the records are in the form of hard copies kept outside the Isle of Man, capable of being sent to the Isle of Man and made available within 7 days; and

(c) in the case of other records (e.g. copies kept on a computer system), readily accessible in or from the Isle of Man and that they are capable of retrieval without undue delay.

A licence holder may rely on the records of a third party in respect of the details of transactions, provided that the licence holder is satisfied that the third party is willing and able to retain (in accordance with paragraph 13 of the Codes) and, if asked, to produce copies of the records required.

7.2 Records

(a) Identification information and evidence records

Paragraph 11 of the Codes requires the licence holder to establish and maintain a record in the Isle of Man containing identification information and evidence of participants. The record must indicate the nature of the information held and comprise either a copy of the information or, where this is not reasonably practicable, contain such information as would allow a copy of such evidence to be obtained. [Such records must be retained for the period of the business relationship with the participant or business participant plus at least 6 years from the date that the relationship is formally ended or where the relationship has not been formally ended, the date of the last transaction.]

(b) Transaction records

Licence holders are required by the Codes to maintain a record of all transactions undertaken. These records may be in the form of electronic transaction reports, original documents or copy form. (It is recommended that such copies should be of a form admissible in Court proceedings.) These will be records in support of entries in the accounts of whatever nature is appropriate to the business of the licence holder, and must be retained for a period of at least 6 years from the date of the transaction.

Paragraph 12 of the Codes provides that Transaction Records must be sufficient *"to identify the source and recipient of payments from which investigating authorities will be able to compile an audit trail for suspected money laundering or terrorist financing".*

(c) Training records

So that licence holders can demonstrate that they have complied with the provisions of Paragraphs 17 and 18 of the Codes concerning staff screening and training, they should maintain records which include:

(i) details of the content of the training programmes provided;

(ii) the names of staff who have received the training;

(iii) the date on which the training was delivered.

Although the Codes does not state over what period training records must be retained, the GSC considers that licence holders should retain such records for a minimum of 6 years from the date the training took place.

7.3 Contents of Transaction Records

Licence holders are required by regulations made under OGRA, to maintain certain records relating to participant or business participants and their transactions. It is necessary to ensure that a satisfactory audit trail can be established for anti-money laundering purposes and that a financial profile of any suspected account can be established. To satisfy this requirement, the following additional information may be sought as appropriate, and transaction records retained of:

(a) the volume of funds flowing through the account/turnover of the participant or business participant;

(b) the origin of the funds where known;

(c) the form in which the funds were deposited or withdrawn, i.e. credit card, cheque, etc. to/by the participant or business participant;

(d) the identity of the person undertaking the transaction;

(e) the form of instruction and authority;

(f) the external financial account details from which the funds were paid (including, bank name, sort code, account number and name of account holder);

(g) the form and destination of payments made by the licence holder to the participant;

(h) a record of all deposits, both successful and unsuccessful, made to the participant's account.

7.4 Establishment of Registers

The Codes requires licence holders to establish and maintain registers as follows:

(a) money laundering and terrorist financing enquiries from the authorities;

(b) ML/FT reports made to the MLRO and deputy MLRO; and

(c) ML/FT reports and/or STRs made to the authorities.

Licence holders must keep, in the Isle of Man, registers in accordance with the requirements of Paragraph 15 of the Codes. The Codes requires that such registers must be kept separate from other records. The register must contain the following information as a minimum:

(a) in respect of enquiries made from the authorities:
    (i) the date of the enquiry;
    (ii) the nature of the enquiry;
    (iii) the name of the agency;
    (iv) the name of the inquiring officer;
    (v) the powers being exercised by that officer;
    (vi) details of the participants and/or business participants involved; and
    (vii) details of the transactions involved;

(b) in respect of enquiries made to the MLRO or deputy MLRO:
    (i) the date of the report;
    (ii) the person making the report;
    (iii) whether it is made to the MLRO or deputy MLRO; and

(iv) information sufficient to identify the relevant papers;

and

(C) in respect of reports made to the authorities:

(i) date of the report;

(ii) the person making the report;

(iii) the Constable to whom the report was made;

(iv) information sufficient to identify the relevant papers; and

(v) acknowledgment of receipt of report from the FCU (once received).

The GSC requires that registers should be readily accessible to authorised officers of the GSC.

7.5 Responding to Production Orders

The GSC expects all licence holders to be in a position to retrieve relevant information without undue delay in response to any request, production order, warrant etc.

Much international damage may be done to the Isle of Man's reputation if requests for international assistance, duly authorised by the Isle of Man Attorney General's Chambers, are not serviced within the time period specified in the notice.

Due to the importance the Isle of Man Government places on its mechanisms for international cooperation, in circumstances of repeated failure by a licence holder to comply with such requests or notices, the GSC will consider that the licence holder is not complying with Paragraph 14 of the Codes (i.e. records to be retrievable without undue delay), which can only impact upon the view held by the GSC of the licence holder's prudence, integrity, competence or the character and status of the management of the licence holder.

SECTION 8 - STAFF SCREENING, TRAINING AND AWARENESS

8.1 The Need for Vigilance

Successful AML/CFT strategies rely on effective communication of a licence holder's policies and procedures to prevent and detect money laundering and terrorist financing. Communication of policies and procedures, and training in how to apply those procedures, provides the basis from which licence holders ensure compliance with AML/CFT legislation and guidance.

In particular, participant facing employees and those who handle or are managerially responsible for the handling of participant transactions or business relationships will provide the business with its strongest defence or its weakest link.

Licence holders must ensure that all directors, and all appropriate employees receive induction training and on-going training on money laundering and terrorist financing prevention on a regular basis. Licence holders must also ensure all staff fully understand the policies and procedures of the licence holder and their importance, and that they will be committing criminal offences if they contravene the provisions of the legislation.

Licence holders must have a clear and well articulated policy for ensuring that their appropriate employees are:

(a) competent and have integrity;

(b) aware of their personal obligations and liabilities under POCA, the Terrorism (Finance) Act 2009, section 9 of the Prevention of Terrorism Act 1990, the Anti-Terrorism and Crime Act 2003, the AML Code, the CFT Code and this guidance;

(c) aware of any new developments including current techniques, methods and trends in money laundering and terrorist financing; and

(d) trained in the identification and reporting of anything that gives grounds for knowledge or suspicion or reasonable grounds to know or suspect that money laundering or terrorist financing is taking place.

The term employee should not be read as to be limited to individuals working under a contract of employment, but should also include temporary and contract staff and the staff of any third parties under an outsourcing agreement.

8.2 New Employees – Vetting

Paragraph 17 of the Codes requires that licence holders maintain and operate appropriate procedures in order to satisfy themselves of the integrity of all new directors and new appropriate employees. The extent of procedures undertaken must take into account the role of the employee and should be appropriate to the risk of ML/FT, the size and complexity of the business.

The term 'appropriate employees' is not unique to high level staff such as the MLRO, deputy MLRO and compliance officers, it may also include other members of staff (e.g. frontline staff) where there are money laundering or terrorist financing risks.

In order to meet these requirements, licence holders must where possible:

(a) obtain and confirm references;

(b) confirm employment history and the qualifications advised;

(c) request details of any regulatory action taken against the individual (or the absence of such action);

(d) request details of any criminal convictions (or the absence of such convictions) and verify where possible.

Licence holders must document the steps taken to satisfy these requirements including the information and confirmations obtained. Licence holders must also document where it has not been possible to obtain such information including the reasons why this is the case.

8.3 Employee Awareness and Training

Under paragraph 18 of the Codes employee awareness raising and training must cover:

(a) the provisions of AML/CFT legislation;

(b) employees' personal obligations under AML/CFT legislation;

(c) the licence holder's internal reporting procedures;

(d) the licence holder's policies and procedures to prevent money laundering and terrorist financing including:

CDD requirements and the need to know the participant's true identity and enough about the type of business activity expected in relation to the participant at the outset (and on an ongoing basis) so that unusual and suspicious activity can be identified in the future and record keeping and other procedures for AML/CFT;

(f) the recognition and handling of suspicious transactions; and

(g) employees' personal liability for failure to report information or suspicions in accordance with the statutory requirements and the internal procedures of the licence holder relating thereto.

8.4 Awareness of Legislation and Procedures

Employee awareness can be achieved and demonstrated in a number of ways and licence holders should consider the following means of demonstrating and monitoring awareness:

(a) Providing employees with a document consolidating information outlining the licence holder's and their own obligations and potential criminal liability under AML/CFT legislation;

(b) Requiring employees to acknowledge that they have received and understood the information contained in the above document; and

(c) Providing relevant employees with a copy of the licence holder's procedures manual for AML/CFT.

It is not sufficient solely to provide employees with a copy of these guidance notes; one of the purposes of these guidance notes is to enable licence holders to design policies and procedures that are appropriate to their business.

8.5 Ongoing Awareness Raising Techniques

Consideration must be given to maintaining employee vigilance between training initiatives. This may be achieved in a variety of ways including:

(a) Keeping employees aware of AML/CFT developments (such as updates issued by the GSC or developments in international standards) as they occur;

(b) Ongoing employee training to keep employees informed of new developments, including information on current ML/FT techniques, methods and trends (including sources of information such as the FATF's Typologies);

(c) Advising employees of sanitised case studies that illustrate how suspicions may have been formulated in certain relationships;

(d) Advising employees of current news stories involving money laundering and terrorist financing activity; and

(e) Emailing reminders of the need to remain vigilant at all times.

With the passage of time between training initiatives the level of employee awareness of the risk of money laundering and terrorist financing will decrease. Using techniques to maintain a high level of awareness can greatly enhance the effectiveness of a licence holder's defences against ML/FT.

8.6 Timing and Content of Training Programmes

Training should be structured to ensure compliance with all of the requirements of the applicable legislation including the requirement under paragraph 18 of the Codes that it be undertaken at least annually. Each licence holder can tailor its training programmes to suit its own needs and those of their employees to whom it is delivered, depending on size, resources and the type of business they undertake. Smaller organisations with no in-house training function may wish to approach competent third parties e.g. specialist training agencies.

If an employee's role within a business changes and, as a result, they become exposed to new products and services with money laundering vulnerabilities with which they are not familiar, or high-risk participant relationships, additional relevant training should be provided.

Training will need to take account of the nature of the transactions and instructions that employees are likely to encounter, the type of product or service and the means of delivery of that product or service, i.e. whether face-to-face or remote. Relevant employees should be able to distinguish between activity that is consistent with relationships that exist for legitimate purposes and activity that is not. They must also be able to understand the legitimate commercial rationale for the existence of the types of relationship to which they are exposed. Relevant employees should be trained to "think risk" in their day-to-day activities and to understand the basis of their employer's risk-based strategy.

Training should highlight to employees the importance of the contribution that they can individually make to the prevention and detection of money laundering and terrorist financing. There is a tendency, in particular on the part of more junior employees to mistakenly believe that the role that they play is less pivotal than that of more senior colleagues. Such an attitude can lead to failures to report important information because of mistaken assumptions that the information will have already been identified and dealt with by more senior colleagues.

The guiding principle of all AML/CFT training should be to encourage employees, irrespective of their level of seniority, to understand and accept their responsibility to contribute to the protection of the business against the threat of money laundering and terrorist financing.

8.7 New Employees

Irrespective of seniority, training for all new employees who will be dealing with participants or their transactions must cover:

(a) a general introduction to the background to money laundering and terrorist financing;

(b) a clear indication of the importance placed on AML/CFT issues by the organisation;

(c) the legal requirement to make disclosures and their personal legal obligations in this regard; and

(d) the procedures for reporting suspicious transactions to the MLRO.

This training must be provided prior to them becoming actively involved in day-to-day operations.

8.8 Front Line Employees

Employees who deal directly with participants are the first point of contact with potential money launderers. Their efforts are vital to an organisation's effectiveness in combating money laundering at the new business stage, and as the business relationship progresses.

Employees who are responsible for dealing with new participants must receive relevant training in:

(a) the need to obtain satisfactory information and verification for all areas of CDD including documentary evidence of the participant's identity;

(b) their obligation to make disclosures even if the transaction or business relationship does not proceed, in respect of both new and existing business relationships.

(c) factors that may give rise to suspicions about a participant; and

(d) the procedures to follow when a transaction is considered to be suspicious.

Employees should also be vigilant when dealing with occasional participants.

Employees involved in processing deals or transactions must receive relevant training in:

(a) processing and verification procedures;

(b) recognising abnormal activity, abnormal settlement, payment instructions, or any change in the normal pattern of business;

(c) the type of suspicious transactions that may need reporting to the relevant authorities regardless of whether the transaction was completed; and

(d) the procedures to follow when a transaction is considered to be suspicious.

All employees should be vigilant in circumstances where a known, existing participant changes the existing known profile. Whilst the licence holder may have previously obtained satisfactory evidence of the participant's identity, the licence holder should not presume that he "knows" the participant, as his knowledge is limited to the participant's previous and different circumstances.

Therefore, in terms of CDD requirements, the licence holder must treat the participant as if the applicant for business were unknown to him, and should take steps to learn as much as possible about the participant's new activities.

8.9 Training for Managerial Employees

Employees who are managerially responsible for handling participant transactions or business relationships must receive a higher level of training covering all aspects of AML/CFT procedures including:

(a) offences and penalties arising from relevant legislation for non-reporting or for assisting money launderers;

(b) procedures for dealing with production and restraint orders;

(c) requirements for verification of identity and retention of records; and

(d) in particular, the application of the licence holder's risk-based strategy and procedures.

8.10 Training for the Money Laundering Reporting Officer

The MLRO and any deputies must receive in depth training on all aspects of money laundering and terrorist financing prevention and detection including:

(a) AML/CFT legislative and regulatory requirements;

(b) the international standards and requirements on which the Isle of Man strategy is based;

(c) the identification and management of ML/FT risk;

(d) the design and implementation of internal systems of AML/CFT control;

(e) the design and implementation of AML/CFT compliance testing and monitoring programs;

(f) the identification and handling of suspicious activity and arrangements;

(g) the money laundering and terrorist financing vulnerabilities of relevant services and products;

(h) the handling and validation of internal disclosures;

(i) liaising with law enforcement;

(j) ML/FT trends and typologies;

(k) the risk of constructive trusteeship;

(l) managing the risk of tipping off;

(m) the handling of monitoring, production and restraint orders.

The role of the MLRO is critical. The MLRO acts as the final arbiter on whether internal disclosures have substance and thus whether they should form the basis of reports to the FCU. MLRO training must reflect the seriousness of the role.

8.11 Monitoring the Effectiveness of Training

Licence holders must monitor the effectiveness of training provided. This may be achieved by:

(a) Testing employees' understanding of the licence holder's policies and procedures to combat ML/FT, the understanding of their statutory and regulatory obligations, and also their ability to recognise money laundering and terrorist financing activity.

(b) Monitoring the compliance of employees with the licence holder's AML/CFT systems, controls, policies and procedures and taking any remedial action that may be necessary.

(c) Monitoring internal reporting patterns and taking any remedial action that may be necessary.

(d) Assessing any court orders to determine whether relevant suspicions were recognised and disclosed.

APPENDICES

Appendix A – Proceeds of Crime (Money Laundering – Online Gambling) Code 2010

Statutory Document No. 509/10

PROCEEDS OF CRIME ACT 2008

PROCEEDS OF CRIME (MONEY LAUNDERING — ONLINE GAMBLING) CODE 2010

INDEX

INTERNAL PROCEDURES

STAFF, EDUCATION, TRAINING AND DEVELOPMENTS

PROCEEDINGS

Statutory Document No. 509/10

PROCEEDS OF CRIME ACT 2008

PROCEEDS OF CRIME (MONEY LAUNDERING — ONLINE GAMBLING) (CODE 2010

Approved by Tynwald: 14th July 2010

Coming into operation: 1st September 2010

The Department of Home Affairs makes this Code under section 157(1) of the Proceeds of Crime Act 2008[3] and after consulting such persons and bodies that appeared to it to be appropriate.

1. Title and commencement

The title of this Code is the Proceeds of Crime (Money Laundering — Online Gambling) Code 2010 and, subject to Tynwald approval[4], it shall come into operation on the 1 September 2010

2. Interpretation

In this Code —

"authorised person" means any person which carries on deposit taking under the provisions of the Financial Services Act 2008[5]; or, is on the register maintained by the Isle of Man Treasury as a money service operator, holds an e-money licence from the Isle of Man Financial Supervision Commission; or, is a regulated party carrying on deposit taking in any of the jurisdictions detailed in Schedule 1 of this Code; or, is on the list of persons detailed in Schedule 2 of this Code deemed to be authorised persons for the purposes of this Code;

[3] 2008 c.13

[4] As required by section 223(3) of the Proceeds of Crime Act 2008.

[5] 2008 c.8

Price Band B £2.00

"beneficial owner" means the natural person who ultimately owns or controls a business participant;

"business participant" means a party participating, in the course of business, in online gambling other than as a licence holder;

"competent authority" means all Isle of Man administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including; the Financial Supervision Commission, the Insurance and Pensions Authority, the Isle of Man Gambling Supervision Commission, the Department of Home Affairs, the Financial Crime Unit of the Isle of Man Constabulary, the Office of Fair Trading, Customs and Excise;

"constable" includes an officer under the Customs and Excise Management Act 1986[6];

"FATF Recommendations" means the 40 Recommendations of the Financial Action Task Force on Money Laundering and the Task Force's 9 Special Recommendations on Terrorist Financing;

"licence holder" means a person conducting online gambling in accordance with a licence granted under the Online Gambling Regulation Act 2001[7];

"money laundering means an act which falls within section 158(11) of the Proceeds of Crime Act 2008;

"the Money Laundering and Terrorist Financing Requirements" means —

(a) part 3 of the Proceeds of Crime Act 2008;

(b) part 2 of the Terrorism (Finance) Act 2009[8];

(c) section 9 of the Prevention of Terrorism Act 1990[9];

(d) sections 7 to 11 and section 14 of the Anti-Terrorism and Crime Act 2003[10]; and

(e) this Code,

and includes, in the case of anything done otherwise than in the Island, anything which would constitute an offence under the provisions specified in paragraphs (a) to (e) if done in the Island;

[6] 1986 c.34

[7] 2001 c.10

[8] 2009 c.8

[9] 1990 c.19 (Although the Act is repealed, it is possible for proceedings to be taken in respect of acts undertaken when it was in force)

[10] 2003 c.6

"online gambling" means online gambling within the meaning given in section 1(1) of the Online Gambling Regulation Act 2001;

"participant" means any person (other than a business participant) participating as a player in online gambling other than as a licence holder;

"payment" means a payment in money or money's worth, but does not include the credit of winnings to an account operated by the licence holder for the benefit of the participant or business participant to whom the winnings are payable;

"peer to peer gambling" means online gambling between two or more participants or online gambling where participants are not hazarding payments against the bank which is facilitated (in both cases) by a licence holder;

"politically exposed person" means any of the following resident in a country outside the Isle of Man —

(a) a natural person who is or has been entrusted with prominent public functions, including —

(i) a head of state, head of government, minister or deputy or assistant minister;

(ii) a senior government official;

(iii) a member of parliament;

(iv) a senior politician;

(v) an important political party official;

(vi) a senior judicial official;

(vii) a member of a court of auditors or the board of a central bank;

(viii) an ambassador, chargé d'affaires or other high-ranking officer in a diplomatic service;

(ix) a high-ranking officer in an armed force; and

(x) a senior member of an administrative, management or supervisory body of a state-owned enterprise;

(xi) a senior official of an international entity or organisation;

(xii) an honorary consul.

(b) any of the following family members of a person mentioned in sub-paragraph (a) —

(i) a spouse;

(ii) a partner considered by national law as equivalent to a spouse;

(iii) a child;

(iv) the spouse or partner of a child;

(v) a sibling;

(vi) a parent;

(vii) a parent in law;

(viii) a grandparent;

(ix) a grandchild;

(c) any close associate of a person mentioned in sub-paragraph (a) or sub-paragraph (b), including —

(i) any natural person who is known to be a joint beneficial owner of a legal entity or legal arrangement, or any other close business relations, with such a person;

(ii) any natural person who is the sole beneficial owner of a legal entity or legal arrangement which is known to have been set up for the benefit of such a person;

(iii) any natural person who is in a position to conduct substantial financial transactions on behalf of such a person;

"terrorism" has the same meaning as in section 1 of the Anti-Terrorism and Crime Act 2003

"transaction" includes —

(a) payments made by a participant or business participant to a licence holder;

(b) payments made by a licence holder to a participant or business participant;

(c) participation in online gambling.

3. General requirements

(1) In conducting online gambling a licence holder shall —

(a) establish, maintain and operate —

(i) identification procedures in accordance with paragraphs 4 to 10;

(ii) record keeping procedures in accordance with paragraphs 11 to 15;

(iii) internal reporting procedures in accordance with paragraph 16;

(iv) staff screening and training procedures in accordance with paragraph 17 to 18;

(v) internal controls and communication procedures which are appropriate for the purposes of forestalling and preventing money laundering and terrorist financing; and,

(vi) procedures and controls in accordance with paragraphs 19 and 20.

(b) take appropriate measures from time to time for the purpose of making employees aware of —

(i) the procedures established, maintained and operated under sub-paragraph 1(a); and,

(ii) the provisions of the Money Laundering and Terrorist Financing Requirements.

(2) A licence holder shall not accept, and shall not permit any third party to accept on its behalf, cash from, or on behalf of a participant or business participant in relation to online gambling.

(3) Any winnings from online gambling due to a participant or business participant from a licence holder shall only be paid to the account held with the licence holder in the name of the relevant participant or business participant as required by the Online Gambling (Registration and Accounts) Regulations 2008[11].

IDENTIFICATION PROCEDURES

4. Anonymous accounts

(1) A licence holder must not in relation to online gambling maintain —

[11] SD 283/08

(a) an anonymous account; or,

(b) an account in a fictitious name.

5. Risk assessment

(1) For the purpose of determining the measures to be taken when carrying out participant or business participant due diligence, under the terms of paragraphs 6, 7 and/or 8 and enhanced participant and business participant due diligence (as such is defined in paragraph 9) under paragraph 9, a licence holder shall carry out a risk assessment in accordance with this paragraph as soon as reasonably practicable.

(2) The risk assessment must estimate the risk of money laundering and terrorist financing on the part of the participant or business participant, having regard to—

(a) value of funds deposited with the licence holder;

(b) jurisdiction of participant or business participant;

(c) source of funds deposited;

(d) any other relevant matter brought to the attention of the licence holder during the account opening process for the participant or the business participant;

(e) any relevant supervisory or regulatory guidance given by the Isle of Man Gambling Supervision Commission;

(f) the legal nature of the business participant.

(3) Where in accordance with the risk assessment, a licence holder determines that a participant or business participant poses a higher risk, the licence holder must carry out enhanced participant and business participant due diligence in accordance with paragraph 9.

6. Identity of prospective participants

(1) A licence holder shall establish, maintain and operate procedures which require the prospective participant to provide satisfactory information as to his identity (either online or in writing) as soon as reasonably practicable after contact is first made between them.

(2) Procedures comply with this paragraph and paragraph 5 if they require that unless satisfactory information as to the prospective participant's identity is provided —

(a) no account will be opened for him,

(b) no money will be accepted from or on behalf of him, and

(c) no participation in online gambling by him will be permitted.

7. Evidence of identity for participants

(1) Subject to the terms of sub-paragraph 5, this paragraph applies in respect of the first occasion on which a qualifying payment is to be made to a participant in relation to online gambling.

(2) A licence holder shall establish, maintain and operate procedures which require the participant to produce satisfactory evidence of his identity before making the qualifying payment.

(3) In relation to online gambling, a payment is a qualifying payment if —

(a) the payment exceeds Euro 3,000; or

(b) when taken with all other payments made to the participant within the 30 days immediately preceding the date on which the payment is to be made, the aggregate amount exceeds Euro 3,000.

(4) Procedures comply with this paragraph if they require that if satisfactory evidence is not produced —

(a) the qualifying payment will not be made unless that evidence is produced;

(b) no further participation in online gambling by the participant will be permitted; and

(c) a licence holder considers whether a suspicious transaction report should be made

(5) In relation to peer to peer gambling, provided that the licence holder complies with paragraph 3(2), and accepts only payments from an authorised person and makes payments to an authorised person on behalf of a participant , a licence holder shall not be required to comply with paragraphs 7 (1) to (4).

8. Evidence of identity for business participants

(1) A licence holder shall establish, maintain and operate procedures which require the business participant to produce satisfactory evidence of its identity before a business relationship is entered into.

(2) A licence holder must, in the case of all business participants —

(i) understand the ownership and control structure of the business participant;

(ii) determine the legal status of the business participant and who is the beneficial owner;

(iii) verify that any person purporting to act on behalf of the business participant is authorised to do so;

(iv) obtain satisfactory evidence to identify and take reasonable steps to verify the identity of those persons or any natural persons having power to direct the business participant's activities, using relevant information or data obtained from a reliable source; and

(v) obtain satisfactory evidence to identify and take reasonable steps to verify the identity of the beneficial owner, using relevant information or data obtained from a reliable source.

9. Enhanced participant and business participant due diligence

(1) Where in accordance with the risk assessment in paragraph 5, a licence holder determines that a participant or business participant poses a higher risk, the licence holder must carry out enhanced participant and business participant due diligence.

(2) Matters which pose a higher risk include but are not restricted to a participant or business participant who is or has a substantial connection with —

(a) a politically exposed person; or

(b) a person, legal person or legal arrangement resident or located in a country which the licence holder has reason to believe does not apply, or insufficiently applies, the FATF Recommendations.

(c) a person, legal person or legal arrangement that is the subject of any notices or warnings issued from time to time by the Isle of Man Gambling Supervision Commission.

(3) In this Code "enhanced participant and business participant due diligence" means steps, additional to the measures specified in paragraphs 6, 7 and 8 of this Code, namely —

(a) considering whether additional identification data needs to be obtained;

(b) considering whether additional aspects of the participant's identity or the identity of the business participant need to be verified;

(c) taking reasonable measures to establish the source of any funds and of the wealth of the participant and any beneficial owner and underlying principal; and

(d) considering what ongoing monitoring should be carried on in accordance with paragraph 10.

10. Ongoing monitoring

(1) A licence holder shall establish, maintain and operate procedures which require the ongoing and effective monitoring of any transactions undertaken by a participant or business participant, including —

(a) review of information provided as to the participant's identity which has been provided under paragraph 6 (1) of this Code;

(b) review of evidence of identity which has been provided under paragraphs 7, 8 and/or 9 of this Code.

(2) This paragraph applies where transactions are undertaken by a participant or business participant which are significantly different (in number or value) to the normal pattern of previous transactions undertaken, or appear complex, or have no apparent economic or lawful purpose.

(3) A licence holder shall establish and maintain procedures which, as soon as reasonably practicable after the variation in the pattern of transactions —

(a) require satisfactory confirmation of the information as to identity provided under paragraph 6; and

(b) in cases in which evidence of identity has been produced under paragraphs 7, 8 and 9, require satisfactory verification of the evidence of identity produced under those paragraphs.

(4) Procedures comply with this paragraph if they require that —

(a) when satisfactory confirmation of the information as to the participant's identity is not provided; or

(b) when satisfactory verification of the evidence of the participant's or business participant's identity is not provided,

no further participation in online gambling by such will be permitted; and

(c) the licence holder considers whether a suspicious transaction report should be made.

RECORD KEEPING

11. Identity Records

(1) Where a licence holder is required under this Code to obtain information as to the identity of a person or confirm such information, the licence holder shall establish and maintain a record in the Island which —

(a) indicates the nature of the information obtained; and

(b) comprises either a copy of the information or, where this is not reasonably practicable, contains such information as would enable a copy of the information to be obtained in accordance with paragraph 14.

(2) Where a licence holder is required under this Code to verify the identity of a person, the licence holder shall establish and maintain a record in the Island which —

(a) indicates the nature of the evidence obtained; and

(b) comprises either a copy of the evidence or, where this is not reasonably practicable contains such information as would enable a copy of the evidence to be obtained in accordance with paragraph 14.

12. Records of transactions

The licence holder shall establish and maintain a record of all transactions carried out by or on behalf of participants or business participants (for example, records sufficient to identify the source and recipient of payments from which investigating authorities will be able to compile an audit trail for suspected money laundering or terrorist financing) and such other records as are sufficient to demonstrate that the Money Laundering and Terrorist Financing Requirements have been complied with.

13. Retention of records

(1) A licence holder shall keep the records required by paragraph 12 for at least 6 years from the date when —

(a) the person concerned formally ceases to be participant or business participant; or

(b) if sub-paragraph (1) (a) does not apply, when the last transaction was carried out by the former participant or business participant.

(2) A licence holder shall maintain the records required by paragraph 12 for at least 6 years from the date of the transaction.

(3) Where a report has been made to a constable under paragraph 16 (3)(f), or the person knows or believes that a matter is under investigation, that person shall, without prejudice to sub-paragraph (1), retain all relevant records for as long as required by the constable.

14. Format and retrieval of records

(1) A licence holder shall ensure that any records that are required to be established and maintained under this Code are —

(a) where the records are in the form of hard copies kept on the Island, then ensure that they are capable of retrieval without undue delay.

(b) where the records are in the form of hard copies kept outside the Island, then ensure that the copies can be sent to the Island and made available within 7 days; and

(c) in the case of other records (e.g. copies kept on a computer system), then ensure that they are readily accessible in or from the Island and that they are capable of retrieval without undue delay.

(2) A licence holder may rely on the records of a third party in respect of the details of transactions, provided that the licence holder is satisfied that the third party is willing and able to retain (in accordance with paragraph 13) and, if asked, to produce copies of the records required.

15. Register of money laundering enquiries and reports

(1) A licence holder shall establish and maintain, in the Island —

(a) a register of all money laundering and financing of terrorism enquiries made of it by law enforcement or other competent authorities;

(b) A register of all money laundering and financing of terrorism reports made to the MLRO or deputy MLRO in accordance with paragraph 16(3)(c);

(c) a register of all money laundering and financing of terrorism reports made to a constable in pursuance of paragraph 16(3)(f).

(2) The registers maintained under sub-paragraph (1) shall be kept separate from other records and —

(a) the register maintained under sub-paragraph (1)(a) shall contain as a minimum the date and nature of the enquiry, the name and agency of the inquiring officer, the powers being exercised, and details of the participants, business participants and transactions involved;

(b) the register maintained under sub-paragraph (1)(b) shall contain details of the date on which the report is made, the person who makes the report, whether it is made to the MLRO or deputy MLRO and information sufficient to indentify the relevant papers; and

(c) the register maintained under sub-paragraph (1)(c) shall contain details of the date on which the report is made, the person who makes the report, the constable to whom it is made and information sufficient to identify the relevant papers. The register shall also contain details of acknowledgement of receipt of report from the Financial Crime Unit.

INTERNAL PROCEDURES

16. Recognition and reporting of suspicious transactions and suspicious attempted transactions

(1) A licence holder shall appoint a Money Laundering Reporting Officer ("MLRO") to exercise the functions conferred on him by this paragraph.

(2) The MLRO must be —

(a) sufficiently senior in the organisation of the licence holder; or

(b) if not within that organisation, have sufficient experience and authority; and

(c) must have a right of direct access to the directors or the managing board (as the case may be) of the licence holder.

(3) A licence holder shall establish, maintain and operate written internal reporting procedures which, in relation to his online gambling business, will —

(a) enable all its directors or, all other persons involved in its management, and all appropriate employees to know to whom they should report any knowledge or suspicions of money laundering or terrorist financing or attempted money laundering or attempted terrorist financing;

(b) ensure that there is a clear reporting chain under which those suspicions will be passed to the MLRO;

(c) require reports to be made to the MLRO of any information or other matter which comes to the attention of the person handling that business and which in that person's opinion gives rise to a suspicion or knowledge that another person is engaged in money laundering or terrorist financing or attempted money laundering or attempted terrorist financing;

(d) require the MLRO to consider any report in the light of all other relevant information available to him for the purpose of determining whether or not it gives rise to a knowledge or suspicion of money laundering or terrorist financing or attempted money laundering or attempted terrorist financing;

(e) ensure that the MLRO has reasonable access to any other information which may be of assistance to him and which is available to the licence holder; and

(f) require that the information or other matter contained in a report is disclosed as soon as is practicable to a constable who is for the time being serving with the Financial Crime Unit on the Island where the MLRO knows or suspects that another is engaged in money laundering or terrorist financing or attempted money laundering or attempted terrorist financing.

STAFF, EDUCATION AND TRAINING

17. Staff screening

A licence holder shall establish, maintain and operate appropriate procedures to enable the licence holder to satisfy itself of the integrity of new directors and new appropriate employees of the licence holder.

18. Staff training

A licence holder shall provide or cause to be provided, education and training including refresher training (not less than annually) for all directors or all other persons involved in its management, all key staff and all appropriate employees to ensure that they are aware of —

(a) the provisions of the Money Laundering and Terrorist Financing Requirements;

(b) their personal obligations under the Money Laundering and Terrorist Financing Requirements;

(c) the internal reporting procedures established under paragraph 16;

(d) the licence holder's policies and procedures to prevent money laundering and terrorist financing;

(e) the licence holder's participant and business participant identification, verification, record-keeping and other procedures to prevent money laundering and terrorist financing;

(f) the recognition and handling of suspicious transactions;

(g) their personal liability for failure to report information or suspicions in accordance with the Money Laundering and Terrorist Financing Requirements and the internal procedures of the licence holder relating thereto.

19. Technological developments

A licence holder must maintain appropriate procedures and controls for the purpose of preventing the misuse of technological developments for the purpose of money laundering or the financing of terrorism.

20. Monitoring and testing compliance

A licence holder must maintain adequate procedures for monitoring and testing compliance with the Money Laundering and Terrorist Financing Requirements, having regard to –

(a) the risk of money laundering and terrorist financing; and

(b) the nature and size of the organisation of the licence holder.

PROCEEDINGS

21. Offences

(1) Any person who contravenes this Code shall be guilty of an offence and liable —

(a) on summary conviction to a fine not exceeding £5,000 or to custody not exceeding 6 months, or to both;

(b) on conviction on information to custody not exceeding 2 years or to a fine, or to both.

(2) In determining whether a person has complied with any of the requirements of any part of this Code a court may take account of —

(a) any relevant supervisory or regulatory guidance which applies to that person and which is given by the Isle of Man Gambling Supervision Commission; or

(b) in a case where no guidance falling within sub-paragraph (a) applies, any other relevant guidance issued by a body that regulates, or is representative of, any trade, business, profession or employment carried on by that person.

(3) In proceedings against a person for an offence under this Code, it shall be a defence for that person to show that he took all reasonable steps and exercised all due diligence to avoid committing the offence.

(4) Where an offence under this Code is committed by a body corporate and it is proved that the offence—

(a) was committed with the consent or connivance of an officer of the body, or

(b) was attributable to neglect on the part of an officer of the body;

the officer, as well as the body, shall be guilty of the offence.

(5) Where a person is convicted of an offence under sub-paragraph (4) he shall be liable —

(a) on summary conviction to a fine not exceeding £5,000 or to custody not exceeding 6 months, or to both;

(b) on conviction on information to custody not exceeding 2 years or to

a fine, or to both.

(6) In this paragraph, "officer" includes —

(a) a director, manager or secretary

(b) a person purporting to act as a director, manager or secretary

(c) if the affairs of the body are managed by its members, a member, and

(d) in relation to a limited liability company constituted under the Limited Liability Companies Act 1996[12], a member, the company's manager, or registered agent;

(e) an operations manager as such is set out in section 10A of the Online Gambling Regulation Act 2001[13].

22. Revocation

The Criminal Justice (Money Laundering - Online Gambling) (No. 2) Code 2008[14] is revoked.

Made June 2010

Minister for Home Affairs

[12] 1996 c.19
[13] 2001 c.10
[14] SD 945/08

Paragraph 2

SCHEDULE 1

Argentina	Italy
Australia	Japan
Austria	Jersey
Belgium	Luxembourg
Bermuda	Malta
British Virgin Islands	Mauritius
Brazil	Monaco
Canada	Netherlands
Cayman Islands	New Zealand
Cyprus	Norway
Denmark	Portugal
Finland	Singapore
France	South Africa
Germany	Spain
Gibraltar	Sweden
Guernsey	Switzerland
Hong Kong	Taiwan
Iceland	United Kingdom
Ireland	United States of America

Aruba and the Netherlands Antilles should not be treated as part of the Kingdom of the Netherlands

Paragraph 2

SCHEDULE 2

[Intentionally left blank]

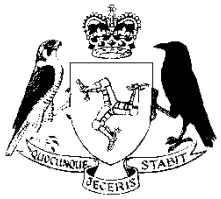
Explanatory Note

(This note is not part of the Code)

The Proceeds of Crime (Money Laundering — Online Gambling) Code 2010 is made under section 157(1) of the Proceeds of Crime Act 2008 and revokes and replaces the Criminal Justice (Money Laundering –Online Gambling) (No. 2) Code 2008 (SD 945/08). The provisions of the Code impose requirements on the online gambling businesses to establish anti-money laundering procedures, training and record keeping. Failure to comply is a criminal offence.

Appendix B – Prevention of Terrorist Financing (Online Gambling) Code 2011

Statutory Document No. 492/11



TERRORISM (FINANCE) ACT 2009

PREVENTION OF TERRORIST FINANCING (ONLINE GAMBLING) CODE 2011

INDEX

STAFF, EDUCATION, TRAINING AND DEVELOPMENTS

PROCEEDINGS

Statutory Document No. 492/11

TERRORISM (FINANCE) ACT 2009

PREVENTION OF TERRORIST FINANCING (ONLINE GAMBLING) CODE 2011

Approved by Tynwald: *14 July 2011*

Coming into operation: *1 September 2011*

The Department of Home Affairs makes this Code under section 27A of the Terrorism (Finance) Act 2009[15] after consulting such persons and bodies that appeared to it to be appropriate.

1. Title, commencement and revocation

This Code is the Prevention of Terrorist Financing (Online Gambling) Code 2011 and, if approved by Tynwald[16], it comes into operation on 1 September 2011.

2. Interpretation

In this Code —

"authorised person" means any person holding a licence to carry on deposit taking, issuing e-money or money transmission services issued under section 7 of the Financial Services Act 2008; or, is a regulated party carrying on deposit taking in any of the jurisdictions detailed in Schedule 1 of this Code; or, is on the list of persons detailed in Schedule 2 of this Code deemed to be authorised persons for the purposes of this Code;

"beneficial owner" means the natural person who ultimately owns or controls a business participant;

[15] 2009 c.8

[16] As required by section 27A(5) of the Terrorism (Finance) Act 2009.

"business participant" means a party participating, in the course of business, in online gambling other than as a licence holder;

"competent authority" means all Isle of Man administrative and law enforcement authorities concerned with combating terrorist financing, including; the Financial Supervision Commission, the Insurance and Pensions Authority, the Isle of Man Gambling Supervision Commission, the Department of Home Affairs, the Financial Crime Unit of the Isle of Man Constabulary, the Office of Fair Trading, Customs and Excise;

"constable" includes an officer under the Customs and Excise Management Act 1986[17];

"FATF Recommendations" means the 40 Recommendations of the Financial Action Task Force on Money Laundering and the Task Force's 9 Special Recommendations on Terrorist Financing;

"licence holder" means a person conducting online gambling in accordance with a licence granted under the Online Gambling Regulation Act 2001[18];

"online gambling" means online gambling within the meaning given in section 1(1) of the Online Gambling Regulation Act 2001;

"participant" means any person (other than a business participant) participating as a player in online gambling other than as a licence holder;

"payment" means a payment in money or money's worth, but does not include the credit of winnings to an account operated by the licence holder for the benefit of the participant or business participant to whom the winnings are payable;

"peer to peer gambling" means online gambling between two or more participants or online gambling where participants are not hazarding payments against the bank which is facilitated (in both cases) by a licence holder;

"politically exposed person" means any of the following resident in a country outside the Isle of Man —

(a) a natural person who is or has been entrusted with prominent public functions, including —

(xiii) a head of state, head of government, minister or deputy or assistant minister;

(xiv) a senior government official;

(xv) a member of parliament;

[17] 1986 c.34

[18] 2001 c.10

(xvi) a senior politician;

(xvii) an important political party official;

(xviii) a senior judicial official;

(xix) a member of a court of auditors or the board of a central bank;

(xx) an ambassador, chargé d'affaires or other high-ranking officer in a diplomatic service;

(xxi) a high-ranking officer in an armed force; and

(xxii) a senior member of an administrative, management or supervisory body of a state-owned enterprise;

(xxiii) a senior official of an international entity or organisation;

(xxiv) an honorary consul.

(b) any of the following family members of a person mentioned in sub-paragraph (a) —

(x) a spouse;

(xi) a partner considered by national law as equivalent to a spouse;

(xii) a child;

(xiii) the spouse or partner of a child;

(xiv) a sibling;

(xv) a parent;

(xvi) a parent in law;

(xvii) a grandparent;

(xviii) a grandchild;

(c) any close associate of a person mentioned in sub-paragraph (a) or sub-paragraph (b), including —

(i) any natural person who is known to be a joint beneficial owner of a legal entity or legal arrangement, or any other close business relations, with such a person;

(ii) any natural person who is the sole beneficial owner of a legal entity or legal arrangement which is known to have been set up for the benefit of such a person;

(iii) any natural person who is in a position to conduct substantial financial transactions on behalf of such a person;

"the prevention of terrorist financing requirements" means the requirements of the following enactments —

(a) section 9 of the Prevention of Terrorism Act 1990[19];

(b) sections 7 to 11 and section 14 of the Anti-Terrorism and Crime Act 2003[20];

(c) Part 2 of the Terrorism (Finance) Act 2009; and

(d) this Code,

and includes, in the case of anything done otherwise than in the Island, anything which would constitute an offence under the provisions specified in paragraphs (a) to (c) if done in the Island;

"terrorism" has the same meaning as in section 1 of the Anti-Terrorism and Crime Act 2003;

"terrorist financing" has the same meaning as in section 3 of the Terrorism (Finance) Act 2009 (and "financing of terrorism" is to be construed accordingly);

"transaction" includes —

(d) payments made by a participant or business participant to a licence holder;

(e) payments made by a licence holder to a participant or business participant;

(f) participation in online gambling.

3. General requirements

(1) In conducting online gambling a licence holder must —

(c) establish, maintain and operate —

(vii) identification procedures in accordance with paragraphs 4 to 10;

[19] 1990 c.19 (Although the Act is repealed, it is possible for proceedings to be taken in respect of acts undertaken when it was in force)

[20] 2003 c.6

(viii) record keeping procedures in accordance with paragraphs 11 to 15;

(ix) internal reporting procedures in accordance with paragraph 16;

(x) staff screening and training procedures in accordance with paragraph 17 to 18;

(xi) internal controls and communication procedures which are appropriate for the purposes of forestalling and preventing terrorist financing; and,

(xii) procedures and controls in accordance with paragraphs 19 and 20.

(d) take appropriate measures from time to time for the purpose of making employees aware of —

(iii) the procedures established, maintained and operated under sub-paragraph 1(a); and,

(iv) the provisions of the prevention of terrorist financing requirements.

(2) A licence holder must not accept, and must not permit any third party to accept on its behalf, cash from, or on behalf of a participant or business participant in relation to online gambling.

(3) Any winnings from online gambling due to a participant or business participant from a licence holder must only be paid to the account held with the licence holder in the name of the relevant participant or business participant as required by the Online Gambling (Registration and Accounts) Regulations 2008[21].

IDENTIFICATION PROCEDURES

4. Anonymous accounts

(1) A licence holder must not in relation to online gambling maintain —

(a) an anonymous account; or,

(b) an account in a fictitious name.

[21] SD 283/08

5. Risk assessment

(1) For the purpose of determining the measures to be taken when carrying out participant or business participant due diligence, under the terms of paragraphs 6, 7 and/or 8 and enhanced participant and business participant due diligence (as such is defined in paragraph 9) under paragraph 9, a licence holder must carry out a risk assessment in accordance with this paragraph as soon as reasonably practicable.

(2) The risk assessment must estimate the risk of terrorist financing on the part of the participant or business participant, having regard to—

(a) value of funds deposited with the licence holder;

(b) jurisdiction of participant or business participant;

(c) source of funds deposited;

(d) any other relevant matter brought to the attention of the licence holder during the account opening process for the participant or the business participant;

(e) any relevant supervisory or regulatory guidance given by the Isle of Man Gambling Supervision Commission;

(f) the legal nature of the business participant.

(3) Where in accordance with the risk assessment, a licence holder determines that a participant or business participant poses a higher risk, the licence holder must carry out enhanced participant and business participant due diligence in accordance with paragraph 9, or conduct an adequate investigation.

6. Identity of prospective participants

(1) A licence holder must establish, maintain and operate procedures which require the prospective participant to provide satisfactory information as to his identity (either online or in writing) as soon as reasonably practicable after contact is first made between them.

(2) Procedures comply with this paragraph and paragraph 5 if they require that unless satisfactory information as to the prospective participant's identity is provided —

(a) no account will be opened for him,

(b) no money will be accepted from or on behalf of him, and

(c) no participation in online gambling by him will be permitted.

7. Evidence of identity for participants

(1) Subject to the terms of sub-paragraph 5, this paragraph applies in respect of the first occasion on which a qualifying payment is to be made to a participant in relation to online gambling.

(2) A licence holder must establish, maintain and operate procedures which require the participant to produce satisfactory evidence of his identity before making the qualifying payment.

(3) In relation to online gambling, a payment is a qualifying payment if —

(a) the payment exceeds Euro 3,000; or

(b) when taken with all other payments made to the participant within the 30 days immediately preceding the date on which the payment is to be made, the aggregate amount exceeds Euro 3,000.

(4) Procedures comply with this paragraph if they require that if satisfactory evidence is not produced —

(a) the qualifying payment will not be made unless that evidence is produced;

(b) no further participation in online gambling by the participant will be permitted; and

(c) a licence holder considers whether a suspicious transaction report should be made

(5) In relation to peer to peer gambling, provided that the licence holder complies with paragraph 3(2), and accepts only payments from an authorised person and makes payments to an authorised person on behalf of a participant , a licence holder is not required to comply with paragraphs 7 (1) to (4).

8. Evidence of identity for business participants

(1) A licence holder must establish, maintain and operate procedures which require the business participant to produce satisfactory evidence of its identity before a business relationship is entered into.

(2) A licence holder must, in the case of all business participants —

(vi) understand the ownership and control structure of the business participant;

(vii) determine the legal status of the business participant and who is the beneficial owner;

(viii) verify that any person purporting to act on behalf of the business participant is authorised to do so;

(ix) obtain satisfactory evidence to identify and take reasonable steps to verify the identity of those persons or any natural persons having power to direct the business participant's activities, using relevant information or data obtained from a reliable source; and

(x) obtain satisfactory evidence to identify and take reasonable steps to verify the identity of the beneficial owner, using relevant information or data obtained from a reliable source.

9. Enhanced participant and business participant due diligence

(1) Where in accordance with the risk assessment in paragraph 5, a licence holder determines that a participant or business participant poses a higher risk, the licence holder must carry out enhanced participant and business participant due diligence.

(2) Matters which pose a higher risk include but are not restricted to a participant or business participant who is or has a substantial connection with —

(a) a politically exposed person; or

(b) a person, legal person or legal arrangement resident or located in a country which the licence holder has reason to believe does not apply, or insufficiently applies, the FATF Recommendations.

(c) a person, legal person or legal arrangement that is the subject of any notices or warnings issued from time to time by the Isle of Man Gambling Supervision Commission.

(3) In this Code "enhanced participant and business participant due diligence" means steps, additional to the measures specified in paragraphs 6, 7 and 8 of this Code, namely —

(a) considering whether additional identification data needs to be obtained;

(b) considering whether additional aspects of the participant's identity or the identity of the business participant need to be verified;

(c) to establish the source of any funds and of the wealth of the participant and any beneficial owner and underlying principal; and

(d) considering what ongoing monitoring should be carried on in accordance with paragraph 10.

10. Ongoing monitoring

(1) A licence holder must establish, maintain and operate procedures which require the ongoing and effective monitoring of any transactions undertaken by a participant or business participant, including —

(a) review of information provided as to the participant's identity which has been provided under paragraph 6 (1) of this Code;

(b) review of evidence of identity which has been provided under paragraphs 7, 8 and/or 9 of this Code.

(2) This paragraph applies where transactions are undertaken by a participant or business participant which are significantly different (in number or value) to the normal pattern of previous transactions undertaken, or appear complex, or have no apparent economic or lawful purpose.

(3) A licence holder must establish and maintain procedures which, as soon as reasonably practicable after the variation in the pattern of transactions —

(a) require satisfactory confirmation of the information as to identity provided under paragraph 6; and

(b) in cases in which evidence of identity has been produced under paragraphs 7, 8 and 9, require satisfactory verification of the evidence of identity produced under those paragraphs.

(4) Procedures comply with this paragraph if they require that —

(a) when satisfactory confirmation of the information as to the participant's identity is not provided; or

(b) when satisfactory verification of the evidence of the participant's or business participant's identity is not provided, no further participation in online gambling by such will be permitted; and

(c) the licence holder considers whether a suspicious transaction report should be made.

RECORD KEEPING

11. Identity Records

(1) Where a licence holder is required under this Code to obtain information as to the identity of a person or confirm such information, the licence holder must establish and maintain a record in the Island which —

(a) indicates the nature of the information obtained; and

(b) comprises either a copy of the information or, where this is not reasonably practicable, contains such information as would enable a copy of the information to be obtained in accordance with paragraph 14.

(2) Where a licence holder is required under this Code to verify the identity of a person, the licence holder must establish and maintain a record in the Island which —

(a) indicates the nature of the evidence obtained; and

(b) comprises either a copy of the evidence or, where this is not reasonably practicable contains such information as would enable a copy of the evidence to be obtained in accordance with paragraph 14.

12. Records of transactions

The licence holder must establish and maintain a record of all transactions carried out by or on behalf of participants or business participants (for example, records sufficient to identify the source and recipient of payments from which investigating authorities will be able to compile an audit trail for suspected terrorist financing) and such other records as are sufficient to demonstrate that the prevention of terrorist financing requirements have been complied with.

13. Retention of records

(1) A licence holder must keep the records required by paragraph 12 for at least 6 years from the date when —

(a) the person concerned formally ceases to be participant or business participant; or

(b) if sub-paragraph (1) (a) does not apply, when the last transaction was carried out by the former participant or business participant.

(2) A licence holder must maintain the records required by paragraph 12 for at least 6 years from the date of the transaction.

(3) Where a report has been made to a constable under paragraph 16 (3)(f), or the person knows or believes that a matter is under investigation, that person must, without prejudice to sub-paragraph (1), retain all relevant records for as long as required by the constable.

14. Format and retrieval of records

(1) A licence holder must ensure that any records that are required to be established and maintained under this Code are —

(a) where the records are in the form of hard copies kept on the Island, then ensure that they are capable of retrieval without undue delay.

(b) where the records are in the form of hard copies kept outside the Island, then ensure that the copies can be sent to the Island and made available within 7 days; and

(c) in the case of other records (e.g. copies kept on a computer system), then ensure that they are readily accessible in or from the Island and that they are capable of retrieval without undue delay.

(2) A licence holder may rely on the records of a third party in respect of the details of transactions, provided that the licence holder is satisfied that the third party is willing and able to retain (in accordance with paragraph 13) and, if asked, to produce copies of the records required.

15. Register of terrorist financing enquiries and reports

(1) A licence holder must establish and maintain, in the Island —

(a) a register of all financing of terrorism enquiries made of it by law enforcement or other competent authorities;

(b) A register of all financing of terrorism reports made to the officer[22] or the officer's deputy referred to in paragraph 16(1) in accordance with paragraph 16(3)(c);

(c) a register of all financing of terrorism reports made to a constable in pursuance of paragraph 16(3)(f).

(2) The registers maintained under sub-paragraph (1) must be kept separate from other records and —

(a) the register maintained under sub-paragraph (1)(a) must contain as a minimum the date and nature of the enquiry, the name and agency of the inquiring officer, the powers being exercised, and details of the participants, business participants and transactions involved;

(b) the register maintained under sub-paragraph (1)(b) must contain details of the date on which the report is made, the person who makes the report, whether it is made to the officer or the officer's deputy and information sufficient to indentify the relevant papers; and

[22] Such a person may be the same as is required under a Code made under section 157 of the Proceeds of Crime Act 2008.

(c) the register maintained under sub-paragraph (1)(c) must contain details of the date on which the report is made, the person who makes the report, the constable to whom it is made and information sufficient to identify the relevant papers. The register must also contain details of acknowledgement of receipt of report from the Financial Crime Unit.

INTERNAL PROCEDURES

16. Recognition and reporting of suspicious transactions and suspicious attempted transactions

(1) A licence holder must appoint an officer[23] to exercise the functions conferred on him by this paragraph.

(2) The officer must be —

(a) sufficiently senior in the organisation of the licence holder; or

(b) if not within that organisation, have sufficient experience and authority; and

(c) must have a right of direct access to the directors or the managing board (as the case may be) of the licence holder.

(3) A licence holder must establish, maintain and operate written internal reporting procedures which, in relation to his online gambling business, will —

(a) enable all its directors or, all other persons involved in its management, and all appropriate employees to know to whom they should report any knowledge or suspicions of terrorist financing or attempted terrorist financing;

(b) ensure that there is a clear reporting chain under which those suspicions will be passed to the officer;

(c) require reports to be made to the officer of any information or other matter which comes to the attention of the person handling that business and which in that person's opinion gives rise to a suspicion or knowledge that another person is engaged in terrorist financing or attempted terrorist financing;

[23] Such a person may be the same as is required under a Code made under section 157 of the Proceeds of Crime Act 2008

(d) require the officer to consider any report in the light of all other relevant information available to him for the purpose of determining whether or not it gives rise to a knowledge or suspicion of terrorist financing or attempted terrorist financing;

(e) ensure that the officer has reasonable access to any other information which may be of assistance to him and which is available to the licence holder; and

(f) require that the information or other matter contained in a report is disclosed as soon as is practicable to a constable who is for the time being serving with the Financial Crime Unit on the Island where the officer knows or suspects that another is engaged in terrorist financing or attempted terrorist financing.

STAFF, EDUCATION, TRAINING AND DEVELOPMENT

17. Staff screening

A licence holder must establish, maintain and operate appropriate procedures to enable the licence holder to satisfy itself of the integrity of new directors and new appropriate employees of the licence holder.

18. Staff training

A licence holder must provide or cause to be provided, education and training including refresher training (not less than annually) for all directors or all other persons involved in its management, all key staff and all appropriate employees to ensure that they are aware of —

(a) the provisions of the prevention of terrorist financing requirements;

(b) their personal obligations under the prevention of terrorist financing requirements;

(c) the internal reporting procedures established under paragraph 16;

(d) the licence holder's policies and procedures to prevent terrorist financing;

(e) the licence holder's participant and business participant identification, verification, record-keeping and other procedures to prevent financing;

(f) the recognition and handling of suspicious transactions;

(g) their personal liability for failure to report information or suspicions in accordance with the prevention of terrorist financing requirements and the internal procedures of the licence holder relating thereto.

19. Technological developments

A licence holder must maintain appropriate procedures and controls for the purpose of preventing the misuse of technological developments for the purpose of the financing of terrorism.

20. Monitoring and testing compliance

A licence holder must maintain adequate procedures for monitoring and testing compliance with the prevention of terrorist financing requirements, having regard to –

(a) the risk of terrorist financing; and

(b) the nature and size of the organisation of the licence holder.

PROCEEDINGS

21. Offences

(1) Any person who contravenes this Code is guilty of an offence and liable —

(c) on summary conviction to a fine not exceeding £5,000 or to custody not exceeding 12 months, or to both;

(d) on conviction on information to custody not exceeding 2 years or to a fine, or to both.

(2) In determining whether a person has complied with any of the requirements of any part of this Code a court may take account of —

(c) any relevant supervisory or regulatory guidance which applies to that person and which is given by the Isle of Man Gambling Supervision Commission; or

(d) in a case where no guidance falling within sub-paragraph (a) applies, any other relevant guidance issued by a body that regulates, or is representative of, any trade, business, profession or employment carried on by that person.

(3) In proceedings against a person for an offence under this Code, it is a defence for that person to show that he took all reasonable steps including either exercising all due diligence or conducting an adequate investigation, to avoid committing the offence.

(4) Where an offence under this Code is committed by a body corporate and it is proved that the offence—

(a) was committed with the consent or connivance of an officer of the body, or

(b) was attributable to neglect on the part of an officer of the body;

the officer, as well as the body, is guilty of the offence.

(5) Where a person is convicted of an offence under sub-paragraph (4) he is liable —

(a) on summary conviction to a fine not exceeding £5,000 or to custody not exceeding 12 months, or to both;

(b) on conviction on information to custody not exceeding 2 years or to

a fine, or to both.

(6) In this paragraph, "officer" includes —

(a) a director, manager or secretary

(b) a person purporting to act as a director, manager or secretary

(c) if the affairs of the body are managed by its members, a member, and

(d) in relation to a limited liability company constituted under the Limited Liability Companies Act 1996[24], a member, the company's manager, or registered agent;

(e) an operations manager as such is set out in section 10A of the Online Gambling Regulation Act 2001[25].

[24] 1996 c.19

[25] 2001 c.10

Made 13 July 2011

[Adrian Earnshaw, MHK]

Minister for Home Affairs

Paragraph 2

SCHEDULE 1

Australia
Austria
Belgium
Bermuda
British Virgin Islands
Brazil
Canada
Cayman Islands
Cyprus
Denmark
Finland
France
Germany
Gibraltar
Guernsey
Hong Kong
Iceland
Ireland
Italy
Japan
Jersey
Luxembourg
Malta
Mauritius
Monaco
Netherlands
New Zealand
Norway
Portugal
Singapore
South Africa
Spain
Sweden
Switzerland
Taiwan
United Kingdom
United States of America

Aruba and the Netherlands Antilles should not be treated as part of the Kingdom of the Netherlands

Paragraph 2

SCHEDULE 2

[Intentionally left blank]

Explanatory Note

(This note is not part of the Code)

The Prevention of Terrorist Financing (Online Gambling) Code 2011 is made under section 27A of the Terrorism (Finance) Act 2009. The Code contains provisions in line with the Financial Action Task Force's Recommendations on preventing terrorist financing and accompanying methodology.

Appendix C – Suspicious Transactions

The below list of examples that might constitute suspicious circumstances is not intended to be exhaustive and only provides examples of the most basic ways by which money may be laundered. However, identification of any of the types of transactions listed below may prompt an internal report to the MLRO for further enquiry.

Nominal play levels:

1. Significant deposits, with minimal play (or no play) followed by withdrawal.
2. Multiple deposits (adding up to a significant amount) with minimal play (or no play) followed by withdrawal.
3. Large deposits with no play record after significant time period.
4. Suspicious ID Details:
   (a) The provision of identification details a licence holder believes to be false or altered.
   (b) A change of ID details or repeated significantly incorrect verification of ID details.
   (c) Attempts to bribe, corrupt or unduly influence licence holder's staff to change transaction data, sensitive ID data etc.
5. Significant re-routing of funds:
   (a) Attempts to transfer to third parties.
   (b) Attempts to transfer to jurisdictions of concern.
6. Attempts to create a false handle with a significant deposit. The issue of significant deposit is important as it will sort out the real suspicious activity from the common bonus hunting activity where first time depositors try to convert welcome bonus money into real money balances via the same method.
7. Even money betting strategies as applied typically to Roulette, Baccarat and Craps, as follows:

   (a) **Roulette**

   Placing equal bets on Black and Red, Red and Black, Odd and Even, High and Low and suffering the loss of half the stakes each time zero appears.

   Placing the same bet on every number (0-36) and suffering the loss of 2.7% of the total stake each spin.

Variations of these bets to achieve the same reduction of risk. For example, on roulette backing the first dozen for 2 units, the six line 13/18 for one unit and High for 3 units. There are other variations that achieve a similar outcome and these will be apparent to an experienced casino supervisor.

(b) **Baccarat**

Playing both participant and banker.

(c) **Craps**

Playing both Pass and Don't Pass lines or Come and Don't Come lines.

1. Collusive attempts by two or more participant or business participants, in multi-participant or business participant mode of the casino, to affect even-money betting strategies (e.g. one bets odd and the other even and at the end of the day the kitty is intact).
2. Any deposits by participant or business participants that a licence holder has good reason to suspect of being involved in illicit business.

Appendix D - Useful Contact References

The GSC encourages use of the Internet as an information resource for anti-money laundering, and encourages licence holders and other interested parties to periodically access the GSC website at www.gov.im for information relating to money laundering and due diligence issues.

Licence holders may also find the following sites useful for due diligence or general information purposes. The list is not exhaustive, and licence holders are encouraged to use other Internet resources:

- www.gov.im/treasury/customs for information on sanctions.
- customs@gov.im to email IOM Customs & Excise.
- www.fsc.gov.im/aml for information on anti-money laundering and false identity documents.
- www.dti.gov.uk for information on embargoes.
- http://dailynews.yahoo.com/fc/business/money_laundering for money laundering news stories and related web sites.
- www.oecd.org/fatf for anti-money laundering information and updates from FATF.
- www.occ.treas.gov/ for helpful information about money laundering prevention and detection from the Office of the Comptroller of the Currency in the USA; and
- www.treas.gov/ for information about the activities of the Financial Crimes Enforcement Network of the US Department of the Treasury.
- Access to some sites requires Adobe Acrobat Reader software, which can be obtained at www.adobe.com.