ALDERNEY
GAMBLING CONTROL COMMISSION

THE PREVENTION OF MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM.

Guidance for the eGambling Industry based in Alderney.

The Alderney eGambling Ordinance, 2009 ("**Ordinance**") and the Alderney eGambling Regulations, 2009 ("**Regulations**") came into force on 1st January, 2010 and replaced the Alderney eGambling Ordinance, 2006 and the Alderney eGambling Regulations, 2006 (as amended). The Regulations further revised and updated the provisions already in existence for strengthening the regulatory requirements imposed on eGambling licensees and their associates to forestall, prevent and detect money laundering and terrorist financing using internationally agreed and adopted measures. These Regulations take their lead from the Financial Action Task Force (FATF) Forty Recommendations and nine special recommendations which set out global standards and identify those business areas where the risks of money laundering and terrorist financing would appear to be greatest.

How to use this Guidance.

This guidance has been written to assist those who are required to take part in the steps being taken by the Alderney Gambling Control Commission ("the Commission") in the fight against money laundering and the financing of terrorism. This guidance does not replace the provisions set out in the Ordinance or the Regulations and therefore this guidance should therefore be read in conjunction with the Ordinance and the Regulations. The Regulations

and the Ordinance set out the legal framework and requirements applicable to licensees and players.

In addition, licensees should refer to the published AGCC internal control system guidelines when preparing their Internal Control System, which has a section dedicated to AML/CFT. It should be noted that the ICS guidelines provide guidance to licensees regarding their entire operation and not just the risks of money laundering and terrorist financing. The current version of this document can be found in the library area of the Commission's website.

Licensees should note that all aspects of their operations relating to AML/CFT controls will be inspected in off-site supervisory activities as well during the course of every on-site inspection undertaken by the Commission.

For ease of reference, in the majority of cases, at the end of each Chapter there is an overview which summarises the key legislative provisions and the principle obligations and principals discussed in the Chapter. The key legislative provisions referred to in this Guidance can be found in Appendix 2 of this Guidance.

Unless specified, note that references in this Guidance to licensees means Category 1 eGambling licensees, Category 2 eGambling licensees, Category 2 Associate Certificate holders and Temporary eGambling licensees.

Originally published July 2010

Current version September 2014

Index

1. INTRODUCTION

The Alderney Gambling Control Commission was established to regulate online gambling (known as eGambling in Alderney) taking place on the island of Alderney. The key licensing objectives enshrined in the Ordinance are:-

- Protecting and enhancing the reputation of Alderney as a well regulated eGambling centre;
- Ensuring that eGambling is conducted honestly and fairly and in compliance with good governance;
- Preventing eGambling from being a source of crime, being associated with crime or being used to support crime, including preventing the funding, management and operation of eGambling from being under criminal influence; and
- Protecting the interests of young persons and other vulnerable persons from being harmed or exploited by eGambling.

The functions of the Commission in relation to eGambling include:-

- Taking such steps as the Commission considers necessary or expedient-
    - For the effective regulation, supervision, and control of eGambling in Alderney and pursuant to the Alderney eGambling (Operations in Guernsey) Ordinance, 2006 in Guernsey,
    - In order to pursue the licensing objectives,
    - For maintaining confidence in, and the safety, soundness and integrity of Alderney's eGambling sector.
- The countering of financial crime and the financing of terrorism in the eGambling sector, "financial crime" including offences involving
    - Fraud or dishonesty
    - Misconduct in, or misuse of information relating to, a financial market
    - Handling the proceeds of crime

  And "offence" includes acts or omissions that would be an offence if they had taken place in Alderney.

A robust AML/CFT regime will compliment a licensee's compliance with other regulatory objectives including excluding young persons and the vulnerable from eGambling and providing secure systems which offer player protection.

1.1 What is money laundering?

Money laundering is the term given to the process or processes by which criminals conceal or attempt to conceal the origin of the proceeds of their or others' criminal activities. After the money has been laundered it can then appear to be legitimate. Where criminal activity has generated a substantial profit, those involved will seek to find ways of disguising the origins of these profits, changing the form or nature of the funds as well as moving them around so as to legitimise the money and its source(s).

Money laundering is a term that is frequently misunderstood. In the Bailiwick of Guernsey it is a defined term; however, in simple terms it means trying to turn funds obtained from or through criminal activity into "clean" money. It also covers handling the benefits of crimes of acquisition such as theft, fraud and tax evasion. In addition it is an offence to be involved in the funding of terrorism or dealing with property that is being used or laundered for that purpose. Licensees are reminded that money laundering encompasses the application of funds from any form of criminal activity. The application of funds means spending or otherwise disposing of funds. There is no "*de minimis*" level.

1.2 What are the proceeds of crime?

At its most basic level money laundering is deception by attempting to make illegitimate funds appear to have been obtained through legal means – but what do we mean by illegitimate funds i.e. what offence has to be undertaken in order for the funds obtained by committing that offence to be considered as the proceeds of crime? Under section 1(1) of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 all offences that are indictable under the law of the Bailiwick are considered to be predicate offences and therefore funds obtained by committing a

predicate offence are considered to be the proceeds of crime. Under Bailiwick law all offences are indictable except for some minor public order and traffic offences.

Therefore, the range of predicate offences is extremely wide and includes the following:

- participation in an organised criminal group and racketeering;
- terrorism, including terrorist financing;
- trafficking in human beings and migrant smuggling;
- sexual exploitation, including sexual exploitation of children;
- illicit trafficking in narcotic drugs and psychotropic substances;
- illicit arms trafficking;
- illicit trafficking in stolen and other goods;
- corruption and bribery;
- fraud and tax evasion;
- counterfeiting and piracy of products;
- environmental crime;
- murder, grievous bodily injury;
- kidnapping, illegal restraint and hostage taking;
- robbery or theft;
- smuggling;
- extortion;
- forgery;
- piracy; and
- insider trading and market manipulation.

1.3 Why is this important?

Money laundering and terrorism financing are serious international issues and it is important that such criminal activities are identified and prevented by all available means. Unfortunately, it has been identified that the gaming industry – including online gaming – may be a vehicle for those who wish to commit crime, conceal the

profits of their crime or fund terrorist activity. The online gaming industry therefore has a duty to work to detect and prevent money laundering and the financing of terrorism wherever possible.

1.4 How does money laundering take place?

There are generally considered to be three stages to money laundering namely

- placement
- layering and
- integration.

These stages can also be termed, hiding, moving and investing or alternatively, conversion, concealment and acquisition.

1.4.1 Placement

The first stage, placement or hiding, is the stage at which the "dirty" money enters the financial system and this is where the greatest deal of vigilance is required. The onus in this respect will fall primarily on Category 1 eGambling licensees.

1.4.2 Layering

The second stage of moving or layering the money is when those who are engaged in money laundering endeavour to conceal the true origins of the money by the creation of complex sets of transactions, including those which may have little or no valid economic purpose. This is when attempts are made to make the money untraceable. This can include breaking down large sums of money, mingling funds from different sources and the transfer of money between numerous accounts held by numerous bodies, potentially in many jurisdictions. It should be noted that during the process of laundering the money, those involved are prepared to spend what might amount to significant sums of money in so doing. This could include the use of professional advisers to add a veneer of respectability to transactions, or the making of what might appear to be "bad" investments but which make it harder to trace any remaining funds. An example of this might be the purchase of luxury goods which are then subsequently resold, potentially at a lower value.

1.4.3 Integration

The final stage is when the funds are then extracted for legitimate use, such as the purchase of property or other assets which will not be tainted by the criminal funds.

1.5 What does this mean for licensees and the public?

The fight against money laundering and the financing of terrorism affects all involved in the eGambling industry. Licensees must comply with the various laws, ordinances and regulations that have been adopted in the fight against money laundering and the financing of terrorism. Customers will need to appreciate that it may mean a lengthier and potentially more detailed registration process before they can begin to use the services of the eGambling licensee, coupled with occasions when they may have to provide further information about themselves. Some aspects of this should already be familiar to customers from their experience of dealing with the wider banking and financial services sector.

The entire process requires that there be vigilance on the part of all concerned.

The nature of the eGambling sector is such that small weaknesses, if exploited, could pose great risks by virtue of the sums of money involved, the speed of transactions, and the levels of turnover, a vulnerability identified by the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (Moneyval). However one of the possible weaknesses of the sector, the fact that the transactions are not face to face also results in one of its strengths, namely the nature of the audit trail that is maintained of eGambling transactions.

1.6 What does a licensee need to do to comply with the legislation?

1.6.1 Risk assessments

Before they can commence operations, licensees must prepare an Internal Control System[1] ("ICS") and before this ICS is submitted for approval the licensee will have to have completed a Business Risk Assessment as defined in Regulation 265 of the Regulations. The Business Risk Assessment is an assessment of the licensee's exposure to money laundering and terrorist financing risks and vulnerabilities (see section 1.7), including those that may arise from new or developing technologies that might favour anonymity, taking into account its size, nature and complexity as well as its customers, products and services and the ways in which it provides those services.

Part of the ICS must address the procedures and processes a licensee[2] will adopt in relation to the area of anti-money laundering and countering the financing of terrorism.[3] The Commission maintains that the fight against money laundering and countering the financing of terrorism (collectively known for the purposes of this guidance as AML/CFT) are serious matters, and licensees are therefore required to have a complete understanding of the issues involved. The Commission requires that eGambling licensees demonstrate in their ICS that they have understood and implemented a comprehensive set of checks and controls to eliminate and deter money laundering, to continuously monitor customer activity, and to identify and report suspicious activity, should it take place appropriate to their category of licence or certificate.

A "tick box" approach is not feasible. eGambling licensees will need to apply a risk based approach when considering how they will meet their AML/CFT obligations. Automated systems can assist but cannot be relied upon as a licensee's sole solution in this area.

1.6.2 Levels of risk

[1] The Internal Control System is a complete description of the licensee's entire business and will cover all aspects of the operations, not simply those relating to AML.

[2] Unless specified, note that references to licensees means Category 1 eGambling licensees, Category 2 eGambling licensees, Temporary eGambling licensees and Category 2 Associate Certificate holders.

[3] When preparing the section of the ICS that relates to AML/CFT, a Licensee must conform to Regulations 175(3) and 233, and Schedule 16 of the Alderney eGambling Regulations, 2009 as amended.

In certain spheres of business activity, there are generally perceived to be three levels of risk, ranging from low/non-existent rising to standard risk and increasing further to higher risk. However, the nature of the online gaming world is such that the Commission has determined that all licensees are subject to the two higher levels of risk: standard risk and higher risk. As a result, under the Alderney eGambling regime the concepts of low risk and simplified customer due diligence do not exist. This is a reflection of the fact that eGambling transactions are not face-to-face, a considered vulnerability of eGambling.

For standard risk customer relationships customer due diligence measures are required and for higher risk customer relationships enhanced customer due diligence measures must be adopted. Once the licensee's gaming operations are active, there needs to be ongoing monitoring of these risks. Additionally there is an onus on the licensee to maintain their vigilance and ensure that they do not do business with persons who might be using criminal funds.

Under the Ordinance it is a criminal offence for a person to fail to comply with any regulations regarding anti money laundering and the Ordinance creates specific money laundering offences.

This guidance has therefore been written to assist those involved in ensuring compliance with the AML/CFT legislative framework applicable to licensees. In addition it is hoped that it will provide an explanation to those who transact with licensees about issues they might not have been fully aware of and which might impact upon their ability to do certain things.

1.7 Where do the vulnerabilities lie?

Within the eGambling sector a number of vulnerabilities have been identified. These include:-

- the cross border nature of online gambling
- the rapidity and cross border nature of transactions
- the non face to face nature of online gambling
- the low number of investigations and prosecutions of ML/TF cases

- crediting winnings to different accounts
- the use of multiple accounts
- the use of money service businesses
- the use of master accounts
- VIP accounts
- Mixed gambling chains
- The use of alternative methods of payment
- The deposit of funds through financial intermediaries
- The use of prepaid (stored value) cards.

The vulnerabilities listed above have been identified by the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism research report on the use of online gambling for money laundering and the financing of terrorism purposes published in April 2013. The Moneyval conclusions state that such vulnerabilities are significantly increased with "unregulated operators". Although, such vulnerabilities will be diminished due to the AGCC's robust regulatory and supervisory framework, the AGCC is of the opinion that is important that its licensed operators are aware of these vulnerabilities so that they can mitigate them effectively within their internal controls, policies and procedures. Each of these vulnerability/risk areas should be considered and tackled by each licensee when formulating and reviewing their internal controls, procedures and policies.

1.8 Who can help in AML and CFT?

Licensees must consider what staff they need to help them in the fight against money laundering and the financing of terrorism. Everyone working for the licensee in a customer facing role must be given training about the risks posed by money laundering and the financing of terrorism. In addition relevant employees[4] as defined under the Regulations will need to receive more detailed training in AML/CFT, the details of which are set out in section 11 of this Guidance (and paragraph 8 of Schedule 16 of the Regulations (see Appendix 2)) There will be few employees

[4] As defined in Regulation 265 of the Regulations and includes any member of the licensee's board of directors, or management team; and employees whose duties relate to eGambling whether or not they hold a key individual certificate or are directly employed by the licensee.

whose roles are not touched by this area. Those dealing with customer registration, customer funds and customer services will need to be made aware of the how important it is for them to be vigilant in this respect. Licensees should expand their general risk assessments from the position of "are we at risk of being defrauded by the customer?" which is a more traditional concern, to "is the customer acting in a way that cannot be explained"? The latter proposition covers instances where someone is trying to cheat the licensee, as well as those occasions where they might be seeking to launder money or transmit funds for the purposes of funding terrorism whilst not necessarily acting in a manner which has a negative impact on the licensee. This will be dealt with in more detail in section 9 which covers transactions that have no lawful or economic purpose.

Even those in technical and non-customer facing roles have a part to play in the fight against money laundering and the funding of terrorism if they come across something that arouses suspicion. They too will be under the general obligations under the Disclosure Law and Terrorism Law that attach to all employees to report their suspicions and should receive appropriate training.

Senior management have an important role to play in that they need to be fully involved in all aspects of the process. They need to lead by example and ensure that they engender a culture of vigilance. They will also have to ensure that appropriate levels of resources are given to the fight against money laundering and countering the financing of terrorism.

1.9 Who is needed?

All licensees are required to have a money laundering reporting officer (MLRO) and a nominated officer (as defined in paragraphs 7(1)(a) and (b) of Schedule 16 of the Regulations). In addition, many licensees may choose to have a deputy money laundering reporting officer. These individuals have a special role to play as they will receive any reports of suspicious transactions or activity and will have to determine whether this suspicion should be reported to the Financial Intelligence Service.

It is therefore important that a licensee's employees know who the MLRO, the deputy MLRO and nominated officer are and how they can be contacted as well as the

internal procedures of the licensee for escalating and for reporting suspicions.[5] Licensees are required to ensure that this forms part of the training that they deliver to relevant employees (paragraphs 7 and 8 of Schedule 16 to the Regulations – see Appendix 2).

[5] The ICS will need to highlight those areas where there is human involvement and discretion in the decision making process and how the risks that are posed by that involvement are mitigated. The way in which a Licensee demonstrates their vigilance in this respect should be explained. The ICS will also need to identify how the roles of MLRO, Deputy MLRO and Nominated Officer are structured, funded and publicised within the organisation as well as the training that will be given to employees. For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

2. Internal Control System and Business Risk Assessment

What is a business risk assessment and how does it differ from an ICS?

2.1 Introduction

2.1.1 Internal Control System

The Internal Control System ("ICS") is a detailed description of a licensee's entire control environment. Preparation of an ICS will, of necessity, involve thorough risk assessments of all relevant business areas. The ICS is used by the Commission to assess the procedures put in place by an operator prior to the operator being permitted to commence operations in order to comply with the legislation and also to evaluate the operator's ongoing performance with regard to these processes. It should not be confused with a business risk assessment which is required specifically in relation to procedures relating to money laundering and the funding of terrorism.

An Internal Control System is defined as "a **system of controls and administrative and accounting procedures used by an eGambling licensee for the conduct of eGambling**" (section 30(1) of the Ordinance).

The ICS needs to be documented and submitted to the Commission for approval in accordance with the provisions of regulations 175 and 176 and the detail of the application form is set out in Schedule 11 of the Regulations.

The Commission requires licensees to operate pursuant to robust, well documented and auditable internal controls (see regulations 175 and paragraph 9A(1)(a) of Schedule 16 to the Regulations – Appendix 2). The Commission undertakes regular on-site inspections and off-site supervisory activities of the licensee's operations to assess whether the licensee is conducting its business in a controlled manner, in conformity with law and regulation, and to assess the correct application of the procedures documented in the approved ICS, and whether the licensee's current approved ICS remains relevant and appropriate to the business. The licensee must

therefore ensure all operational changes are addressed in the ICS, and secure the Commission's formal approval prior to implementing any such change.

An ICS must include the policies, procedures and controls as are appropriate and effective for the **purposes of forestalling, preventing and detecting money laundering and terrorist financing, and necessary in order to comply with the money laundering and terrorist financing provisions under Schedule 16 and the associated regulations** of the Regulations including the following policies, procedures and controls –

(a) policy for reviewing at appropriate intervals its compliance with the money laundering and terrorist financing provisions;

(b) arrangements to manage compliance;

(c) screening practices when recruiting relevant employees;

(d) ongoing employee training programme;

(e) audit function to test its systems;

(f) measures taken to keep abreast of and guard against the use of technological developments and new methodologies in money laundering and terrorist financing schemes;

(g) customer identification and verification systems (in relation to a Category 1 eGambling licensee only); and

(h) procedures relating to ongoing customer due diligence and monitoring of the customer relationship (in relation to a Category 1 eGambling licensee only).

2.1.2 Business Risk Assessment

The business risk assessment must be undertaken prior to the submission of the ICS. eGambling licensees are in the best position to identify those areas of their operations that present the greatest risks of money laundering and terrorist financing and therefore those which should be the focus of their attention. The licensee can determine the most cost effective and proportionate way of managing those risks in a manner that is both flexible and effective. The business risk assessment must be

regularly updated to ensure that it meets the requirements of paragraph 1(2) of Schedule 16 to the Regulations.[6] (See Appendix 2)

2.1.3 ICS Guidelines

For detailed guidance on internal policies, procedures and controls, please refer to the Commission's ICS Guidelines. The Commission's latest ICS guidelines for the submission of an Internal Control System can be downloaded from http://www.gamblingcontrol.org/userfiles/file/ICSG/ICSG%20Version%204_0%20FINAL.pdf (correct as at publication of this guidance)

2.2 What should a Business Risk Assessment contain?

When compiling a Business Risk Assessment an eGambling Licensee should look at the following issues:

- General and specific risks
- Controls that mitigate against risks that have been identified
- The recording of actions taken
- Compliance with the legislation

The drafting of the Business Risk Assessment is a very important task which requires careful consideration. The "further reading" section of this guidance lists a number of sources of material which eGambling licensees should consider as part of the preparation process. A recent additional key document that licensees should refer to is be the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (Moneyval) research report into the use of online gambling for money laundering and the financing of terrorism purposes. This report published in April 2013 provides a helpful description of the risks of money

[6] It is a requirement that the licensee regularly reviews its entire ICS and keeps it up to date to ensure that it accurately reflects the nature of eGambling carried out under the licence (paragraph 1(2) of Schedule 16 to the Regulations – Appendix 2). The licensee must also specifically regularly review and update the Business Risk Assessment. Approval for any changes to the ICS to accommodate variations in the Business Risk Assessment should be sought in the usual way in accordance with Regulation 192.

laundering and terrorist financing in the eGambling sector setting out a number of typologies and "red flag" indicators as well as identifying a number of vulnerabilities in the sector which licensees are expected to familiarise themselves with and ensure that their business risk assessments reflect any relevant risks and their internal controls, policies and procedures effectively mitigate any such risks.

In August, 2014 the Commission concluding a review of the risks of money laundering and terrorist financing in eGambling. This analysis took into account the various reports and methodologies published by FATF and Moneyval together with a number of academic studies, a consultation with the eGambling industry in 2013 and the Commission's own experiences, a review of STRs that relate to eGambling and analysis of requests for Mutual Legal Assistance made to the Guernsey Financial Intelligence Service to compile a list of risks in the industry and then to identify, on a weighted basis, the greatest risks of ML/TF in the eGambling sector. This analysis identified that the five greatest risks in the sector are currently:-

1. **Card Fraud**

   This would include where a criminal gains access to the credit card details and personal data of a large number of victims and uses this information to fund various eGambling accounts in his own name, or in the name of his associates. After nominal gambling activity he then attempts to withdraw these funds or transfer them to an account in his name, or in the name of his associate.

2. **Laundering via illegal and legal betting**

   Criminals collude with participants in sports events attempting to affect the outcome of events and laundering the proceeds of this fraud through placing bets with unsuspecting eGambling operators.

3. **Legal and regulatory risks**

   The eGambling operator must make a decision on accepting players or business associates from new target markets where the legal/regulatory environment may not allow for an adequate level of identity checks or may not provide an adequate audit trail for payments/source of funds.

4. **Ownership and control of casinos**

   This includes –

   - *A launderer, in collusion with an operator of an offshore gambling website, deposits funds obtained from criminal activities in the gambling account and withdraws such funds as winnings. The website operator keeps a percentage of the proceeds as a Commission while the launderer declares the winnings to the tax authorities and then uses the funds for legitimate purposes.*

   - *A launderer sets up a company in an offshore jurisdiction through various front men. The company then applies for an eGambling licence in the offshore jurisdiction. Funds deriving from criminal activity are then laundered through the eGambling website which is controlled by the launderer.*

- *A criminal colludes with other persons who act as beneficial owners of a company which is used to obtain an eGambling licence. Illegally obtained funds are then co-mingled with the legitimate profits of the company and deposited in a bank account*

5. Identify theft and false ID

The eGambling operator suspects that the player is using a false or assumed identity. This is either a fake or false identity or one belonging to another person.

2.2.1. Risk

General Risks

These are the risks that are relevant to the industry in general and its own business in particular.

The Commission requires each licensee to consider general AML/CFT risks in the industry and its business and to demonstrate an appropriate level of vigilance regarding those general risks.

2.2.2. Specific risks

There are a number of specific risks that the Commission has identified as being relevant to a licensee's business. This list is not exhaustive and each licensee may consider that they have other risks specific to their operations.

Risks identified by the Commission include the following:

2.2.2.1 Customers

This includes types and behaviours. For example this might include customers who make regular deposits to their accounts but wager only very small sums before seeking a withdrawal from their account. It could also include customers who are located in jurisdictions which are considered to have AML/CFT regimes that

do not meet international standards. The Commission assists in this regard by publishing Business from Sensitive Sources Notices (BSSN's) on its website. The most recent BSSN's can be found by following the links below.

http://www.gamblingcontrol.org/userfiles/file/BSSN%2019%2018082014.pdf

http://www.gamblingcontrol.org/userfiles/file/BSSN%2018%2018082014.pdf

(links correct at date of publication). When a new BSSN is issued it will be published by the Commission on its website and relevant employees of licensees will be notified by their relationship manager at the Commission.

In addition licensees must ascertain whether any customers are considered to be Politically Exposed Persons (see section 6). In addition, changes to the customer's gambling habits could warrant further investigation.

The Category 1 eGambling licensee's business risk assessment will also need to encompass their customer identification and verification systems and how they deal with the issue of ongoing due diligence of the customer relationship.

2.2.2.2 Products

Slots and bingo may be seen to be lower risk games. However these games are not without risk where money launderers may seek to protect the value of their deposits. This could take the form of the customer placing bets on both red and black on a roulette table to minimise their risks of loss.[7] eGambling licensees should ensure that their systems identify such activity and flag it for monitoring and review (see chapters 8, 9 and 10).

[7] Where a customer bets on both red and black at roulette losses would be limited to those occasions when the "ball" lands on "0". On all other occasions there would be no loss or gain.

In addition there may be occasions when players elect to or allocated seats at the same table in certain games. Where this happens the systems of eGambling licensees should identify such activity for monitoring and review of the transactions.

Poker and other peer to peer games could be seen to be a higher risk games due to the higher risks of collusion and chip dumping by customers and therefore Category 2 eGambling licensees and certificate holders must ensure that they are in a position to identify such activity.

2.2.2.3 Services

Category 1 eGambling licensees may offer facilities for their customers to transfer funds to another customer – commonly known as player to player transfers. Such transfers present a significantly increased risk which will need to be addressed through some additional forms of control. For example, the licensee could require that funds transferred in such a manner must be wagered and cannot be withdrawn or be made the subject of subsequent re-transfer. Category 1 eGambling licensees may consider that the risks of player to player transfers necessitate the implementation of additional customer due diligence procedures in relation to those involved. Category 1 eGambling licensees offering such facilities should explain what controls will be put in place to deal with the risks accompanying these options.

With event based wagering, risks of match or event "fixing" exist and consideration should be given to how this will be dealt with, including how suspicions will be reported and how customers are informed about how information about them will be processed. This should have regard to the Data Protection (Bailiwick of Guernsey) Law, 2001. Regulations 4(n), 6(o), 8(k) and 60(l) of the Regulations must be complied with. In addition eGambling licensees should, at that time, consider their obligations under the Disclosure Law with regards to the filing of a suspicious

transaction report with the Guernsey Financial Intelligence Service.

2.2.2.4 Banking Methods –

Banking methods include media such as credit cards, bank transfers and cheques, and other ewallet solutions for making deposits into and withdrawals from a player's eGambling account with the Category 1 eGambling licensee. Are there risks of these being diverted? The risks of money laundering can be reduced by ensuring that deposits originate from an account with a recognised financial body in the name of the customer. In addition, the risk of money laundering can be further reduced by ensuring that withdrawals are made to the same credit/debit card or account as the original deposit came from. The Alderney eGambling regime does not permit the use of cash[8] or anonymous stored value credit cards. Those Category 1 eGambling licensees who make use of alternative deposit or withdrawal methods (such as third party payment processors) should be aware that this increases the risk of money laundering and their business risk assessments and internal policies, procedures and controls must address this factor.

2.2.2.5 Geographical areas of operation

Some countries are deemed to present greater risks than others for money laundering and the financing of terrorism. These countries typically do not have legislation which meets FATF standards or have legislation which insufficiently applies the FATF recommendations. Licensees must therefore focus on money being received from and remitted to such jurisdictions. It may also be harder to verify the identity of a customer under the required customer due diligence ("CDD") (including enhanced CDD) procedures in countries where there are fewer appropriate resources such as credit reference agencies or creditable databases,

[8] See Regulation 230(2) – Appendix 2.

e.g. electoral roll information. Licensees are required to take note of non-compliant countries and territories as published by the FATF as well as those insufficiently applying the FATF recommendations. The Commission will endeavour to provide assistance in this respect wherever possible. In addition information can also be obtained from the website of the Guernsey Financial Services Commission at http://www.gfsc.gg/The-Commission/Pages/Legislation-and-Guidance.aspx

2.2.2.6 Employees

Employees, including relevant staff of third party providers, with access to the eGambling system of the licensee and/or customer data and funds present a considerable risk. Accordingly, licensees must identify staff positions that present a higher risk and introduce screening processes during the recruitment of employees filling these positions as required by paragraph 8(1) of Schedule 16 of the Regulations (see Appendix 2). In addition licensees must train relevant employees in relation to AML/CFT as set out in paragraph 8 of Schedule 16 and maintain records of such training as required under paragraph 9 of Schedule 16 of the Regulations (see Appendix 2).

2.2.3 Red Flag Indicators

The recent Moneyval Research Report identified the following as being "red flag indicators" of possible laundering through eGambling –

- *Information provided by the player contains a number of mismatches (eg email domain, telephone or postcode details do not correspond to the country);*
- *The registered credit card or bank details do not match the player's registration details;*
- *The player is situated in a higher-risk jurisdiction or is identified as being listed on the international sanctions list;*
- *The player is identified as a politically exposed person;*

- *The player seeks to open multiple accounts under the same name (licensees should also note that this may raise issues with regards to player protection);*
- *The player opens several accounts under different names using the same IP address;*
- *The withdrawals from the account and not commensurate with the conduct of the account, such as for instance where the player makes numerous withdrawals without engaging in significant gambling activity;*
- *The player deposits large amounts of funds into his online gambling account;*
- *The source of funds being deposited into the account appears to be suspicious and it is not possible to verify the origin of the funds;*
- *The customer logs into the account from multiple countries;*
- *A deposit of substantial funds followed by very limited activity;*
- *The player has links to previously identified accounts; Different players are identified as sharing banks accounts from which deposits or withdrawals are made.*

These indicators arise from both general industry and specific business risks. Licensees should ensure that (a) they are vigilant in relation to these "red flag indicators" and (b) these "red flag indicators" are effectively integrated within their internal controls, policies and procedures for the purposes of forestalling, preventing and detecting money laundering and terrorist financing.

2.2.4 Controls to mitigate risks

Each licensee needs to consider the design and implementation of internal controls, policies and procedures to manage and mitigate risks according to their category of licence. Appropriate controls could include, for example, player tracking systems to track changes in play and spending over a period of time, or manual procedures involving regular checks by licensee's staff. Automated systems are likely to be helpful in providing analysis, but it is the responsibility of the MLRO

to identify those instances when a STR may need to be made. Controls and systems will help licensees to identify instances of collusion, and may also identify customers coming from jurisdictions which are deemed to present greater risks in respect of money laundering or the financing of terrorism. The following issues must be addressed by the licensee:-[9]

- individual or linked transactions which are complex or unusually large with no apparent or lawful economic purpose including those relative to a relationship;

- unusual patterns of transactions with no apparent economic or lawful purpose including those relative to a relationship;

- transactions which exceed certain limits with no apparent economic or lawful purpose including those relative to a relationship;

- transactions arising from a country or territory that does not apply or insufficiently applies the FATF Recommendations;

- very high account turnover inconsistent with the balance;

- transactions which are outside of the customer's regular transaction activity.

Category 1 eGambling licensees must describe how they will identify and deal with accounts which are funded but where no gambling takes place prior to a request to withdraw funds.

Category 2 eGambling licensees and Category 2 associate certificate holders must describe how they will monitor for collusion and how they will detail those findings in writing and communicate those findings to the Category 1 eGambling licensee who had registered the

[9] The ICS must deal with how the licensee might link transactions together, especially those planned to thwart AML/CFT safeguards (e.g. the trigger points for enhanced customer due diligence). For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

customer as required by paragraph 6(4) of Schedule 16 of the Regulations (see Appendix 2).

The Category 1 eGambling licensee must engage in ongoing monitoring of:

- customer identity, due diligence and identification data
- customer financial habits and behaviours, to ensure that the transactions are consistent with the licensee's knowledge of the customer's risk profile
- customer gambling habits and behaviours to ensure that the transactions are consistent with the licensee's knowledge of the customer's risk profile.

2.2.5 Recording what action has been taken

Licensees need to outline how they will comply with the requirement that they record what actions are taken and the reasons for such action being taken. Effectively they are being asked to demonstrate how they record their vigilance. The record keeping requirements are set out in paragraph 9 of Schedule 16 of the Regulations (see Appendix 2) and are further discussed in section 9 of this Guidance.

2.2.6 Compliance with the law

Licensees must record and be able to demonstrate how they achieve full compliance with the laws applicable in the Bailiwick of Guernsey. Details of these laws can be found in the dedicated AML/CFT Resources section of the licensee's area of the Commission's website.

The licensee will be liable and responsible for compliance with the various AML/CFT laws within the Bailiwick even if it relies upon services or assurances from third parties, associates or consultants.[10]

[10]. The ICS must deal with how Category 1 eGambling licensees would assimilate and process information received from a Category 2 eGambling licensee/ associate certificate and outline the steps it would take to comply with its obligations under the Disclosure Law and the Terrorism Law. For

In addition licensees must also check the UN/EU sanctions section of the Commission's website for further details of sanctions imposed by the United Nations and the European Union. This can be found at http://www.gamblingcontrol.org/licensees10.php (see Chapter 13 of this Guidance)

In addition information can be found on the website of the Guernsey Financial Services Commission at http://www.gfsc.gg/FCA/Pages/Sanctions.aspx

There is no set format for a business risk assessment; each licensee has the freedom to present their business risk assessment in the manner which best reflects their operations. However, the Commission expects each licensee to address each of the issues set out in section 2.2 of this Guidance. The Commission will assess each business risk assessment. The Commission considers this approach to be appropriate given that the business of each licensee is different and the licensee is best placed to identify and prioritise the risks it faces. Given the differences in products offered by licensees the adoption of a prescribed format might not accurately focus the attention of the licensee on *their* business and the risks *it* faces.

2.3 What comes after the business risk assessment?

2.3.1 Review of business risk assessment.

Licensees are required to consider their business risk assessment at regular intervals to ensure that it has not become susceptible to new methodologies of money laundering or the financing of terrorism (paragraph 1(2) of Schedule 16 to the Regulations – see Appendix 2).

There is also a requirement that the ICS is generally kept under regular review. The review period has to take into account the size, nature and

---

detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

complexity of its gambling offering; in the case of a Category 1 eGambling licensee its registered customers; and the way it provides its services.

Licensees are also required to maintain an independent audit function to test its compliance with their AML/CFT obligations. The audit function must be adequately resourced and independent (see paragraph 9A(1)(c) of Schedule 16 to the Regulations– Appendix 2). For large licensees who have an independent audit committee that committee's remit could be extended. For smaller licensees there are many ways this regulatory requirement can be met.

2.3.2 Individual Risk Assessment

In addition to their general business risk assessment Category 1 eGambling licensees must also undertake an individual risk assessment of each customer either at the time of registration or as soon as reasonably practicable thereafter (regulation 227(2) of the Regulations – see Appendix 2). There is no fixed time for doing this but the ICS will need to explain the steps that will be taken to meet this requirement and the timescale involved. It is a requirement that this risk assessment must also be regularly reviewed (regulation 229 of the Regulations – see Appendix 2). The review period is for the Category 1 eGambling licensee to set but it should take into account the factors applicable to business risk assessment reviews such as changing technology, any developments in the field of money laundering or terrorist financing, and the territory in which the customer may be based which either increase or lower risk.

2.3.3 Failure of customer due diligence

Category 1 eGambling licensees must identify in their internal controls, policies and procedures how they will deal with instances when customer due diligence measures cannot be completed. This includes when someone seeks to become a customer or when during

the course of an ongoing customer relationship it becomes necessary to terminate the customer relationship together with considering whether a disclosure must be made pursuant to Part 1 of the Disclosure Law or section 12 of the Terrorism Law.[11]

2.4 Typologies

Licensees are under a duty to take appropriate measures to keep abreast of and guard against the use of new and emerging technological developments and new methodologies in money laundering and terrorist financing (see paragraph 9A(1)(b) of Schedule 16 to the Regulations – Appendix 2). The recent Moneyval Research Report identified a number of various potential typologies for money laundering in the eGambling sector. For ease of reference, these are set out below:-

- *A money launderer, in collusion with an operator of an offshore gambling website, deposits funds obtained from criminal activities in the gambling account and withdraws such funds as winnings. The website operator keeps a percentage of the proceeds as a commission while the launderer declares the winnings to the tax authorities and then uses the funds for legitimate purposes.*

- *A money launderer sets up a company in an offshore jurisdiction through various frontmen. The company then applies for an online gambling licence in the offshore jurisdiction. Funds deriving from criminal activity are then laundered through the online gambling website which is controlled by the launderer.*

- *A criminal colludes with other persons who act as beneficial owners of a company which is used to obtain an online gambling licence. Illegally obtained funds are then co-mingled with the legitimate profits of the company and deposited in a bank account.*

[11] References in this Guidance to the Disclosure Law means the Disclosure (Bailiwick of Guernsey) Law, 2007, as amended and references to the Terrorism Law mean the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002, as amended.

- *A money launderer sets up an online gambling website without registering the website or obtaining a licence. The website is not made available to the public but is used to place funds obtained from criminal activities which are then distributed as winnings to various frontmen. The website is then disconnected citing failure to make a profit as the primary reason for the disconnection.*

- *A money launderer colludes with professional gamblers to place illegally obtained funds on online gambling websites. The gamblers keep a commission from any winnings made before transferring the remaining funds to the launderer.*

- *Illegally obtained funds are deposited into an online gambling account using a false identity. The player engages in minimal gambling activity which is sufficient to make the account appear genuine. After incurring minimal losses the funds are then transferred from the gambling account to a legitimate bank account.*

- *A money launderer deposits funds derived from criminal activities into an e-wallet through a money service business. The funds are then deposited into an online gambling account by frontmen. The winnings are remitted back to the e-wallet account and used for other legitimate purposes on other websites.*

- *A money launderer deposits funds into an online gambling account by using a stolen identity to avoid detection.*

- *Peer-to-peer games such as e-poker, where value transfers can occur between both electronic and human players as a result of deliberate losses, at a relatively low cost to the players. Players will make large bets on very bad hands expecting to lose to the accomplice. This is generally known as chip-dumping and is considered to mainly pose a risk of terrorist financing.*

Licensees should ensure that (a) they consider each of these typologies and (b) effectively integrate safeguards against the occurrence of each of these typologies within their internal controls, policies and procedures for the purposes of forestalling,

preventing and detecting money laundering and terrorist financing in accordance with paragraph 9A(1)(b) of Schedule 16 to the Regulations.

BUSINESS RISK ASSESSMENTS AND INTERNAL CONTROL SYSTEMS
• **Key Legislative Provisions:**
• Regulation 175 (Internal Control System) • Paragraph 1 of Schedule 16 to the Regulations (Business Risk Assessment)
To summarise: Licensees must (according to their category of eGambling licence or certificate)[12] assess the risks posed by: • the industry (all) • customers (1) • products and services (all) • payment methods (1) • location (all) • employees (all) • new and emerging technologies (all) Licensees must design controls or processes to manage risks and identify • complex transactions (all) • unusual transactions (all) • transactions outside a customer's normal pattern of activity (all) • transactions arising from a country which does not apply or insufficiently applies FATF recommendations. (all) Licensees must monitor:

[12] References in parenthesis refer to category of licence or certificate.

- the information they hold (all)
- customers' financial habits (1)
- customers' gambling habits (all)

Licensees must record in writing and detail

- the actions they take (all)
- how they achieve compliance with Bailiwick laws (all)

3. CORPORATE GOVERNANCE

Fighting money laundering and the financing of terrorism are areas in which licensees' senior management need to be fully and actively involved. This means engaging and participating in the decision making process which generates the policies adopted by the licensee. The legislation provides for criminal sanctions in the event that the law and procedures are not followed properly. It is vital therefore that licensees undertake proper and considered risk assessments, ensure that any relevant discussions and decisions taken are properly and accurately recorded, take a careful, strict and considered approach to the Regulations, a proper consideration of the risks, together with a consideration of the way in which risks can be mitigated, and ensure that established internal controls, policies and procedures are followed and regularly reviewed.

In addition, as senior managers are required to approve high risk customer relationships (i.e. those where the customer is subject to enhanced customer due diligence procedures), it is imperative that they are fully aware of their responsibilities and are appropriately trained in all aspects of the legislation and AML/CFT controls and procedures.

It is a requirement under the legislation that all licensees establish and maintain internal policies, procedures and controls that are appropriate and effective for the purposes of forestalling, preventing and detecting money laundering and terrorist financing (see paragraph 9A(1)(a) of Schedule 16 to the Regulations – Appendix 2).

In addition appropriate measures must be taken to keep abreast of and guard against the use of new and emerging technological developments and new methodologies in money laundering and terrorist financing (see paragraph 9A(1)(b) of Schedule 16 to the Regulations – Appendix 2).

Furthermore policies and procedures must be established and maintained to address specific risks associated with non face-to-face customer relationships and transactions, in particular before registering customers and when performing the ongoing monitoring of the customer relationship (see paragraph 9A(1)(c) of Schedule 16 to the Regulations – Appendix 2)..

A licensee's Board of Directors must take responsibility for the maintenance and establishment of an effective policy for the review of compliance with the associated regulations and the requirements of Schedule 16 to the Regulations. The policy established must include the provision as to the extent and frequency of reviews, and the requirement to maintain an adequately resourced and independent audit function to test compliance with such requirements. In addition the directors will need to ensure that the review of compliance of Schedule 16 to the Regulations and the associated regulations is discussed and minuted at Board meetings taking place at appropriate intervals and when determining what an appropriate interval is regard shall be had to risk taking into account the size, nature and complexity of eGambling conducted and in respect of Category 1 eGambling licensees its registered customers, products and services as well as the ways in which those products and services are provided (see paragraph 9A(1)(d) and (e) of Schedule 16 to the Regulations – Appendix 2).

Licensees must also have regard to and meet the requirements of any relevant guidance, notice instruction, and countermeasures issued by the Commission relating to anti-money laundering and counter-terrorist financing which are designed to alert and advise of weaknesses in the AML or CFT systems in other countries (see paragraph 9A(1)(f) of Schedule 16 to the Regulations – Appendix 2).

CORPORATE GOVERNANCE **Key legislative provisions:**
• Paragraph 9A of Schedule 16 to the Regulations (Ensuring Compliance, Corporate Responsibility and Related Requirements)
To summarise: Senior management must • be involved in the decision making processes • record the decisions made • implement the procedures appropriately • appropriately trained. Board of Directors must –

- ensure that an effective policy is established and maintained in order to review the compliance with the AML/CFT requirements
- ensure that the review of compliance with the AML/CFT requirements is discussed and minuted at Board Meetings at appropriate intervals.

4. CUSTOMER DUE DILIGENCE

4.1 Introduction

It is necessary for a Category 1 eGambling licensee to undertake customer due diligence and where necessary, enhanced (additional) customer due diligence, in order to identify and verify every customer prior to allowing eGambling to commence (paragraphs 2 and 3 of Schedule 16 to the Regulations – see Appendix 2). Transactions involving customers who are not fully identified and verified can pose real risks. These risks are increased when it is not possible to deal with customers on a face to face basis. No eGambling can take place face to face.

In addition customer due diligence measures must be undertaken –

- when a customer deposits €3000 or cumulative deposits in a 24 hour period reach or exceed €3000;
- when a licensee has suspicions or cause to suspect a customer is engaged in money laundering or terrorist financing;
- where a licensee doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification of a customer.

Customer due diligence measures are specified in paragraph 10(1) of Schedule 16 to the Regulations.[13]

Why is CDD needed?

Category 1 eGambling licensees must have sound CDD procedures for a number of reasons. Firstly they form an essential part of their risk management strategy helping them to identify, assess mitigate and manage risk. They will also help the Category 1 eGambling licensees' business as well as the whole eGambling sector by reducing the chances of the business and the sector being a vehicle for or victim of financial crime or terrorist financing.

[13] The ICS must detail the procedures that will be carried out to comply with these requirements. For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

When carrying out CDD the Category 1 eGambling licensee will be able to take comfort that their customers are who they say they are and that it is appropriate to offer them the services they seek. Lastly the Category 1 eGambling licensee will be assisted during the course of the business relationship in identifying factors which are unusual and which may lead them to knowing or suspecting or having reasonable grounds for knowing or suspecting that their customers may be involved in money laundering or terrorist financing.

4.2 What steps need to be take place

4.2.1 Customer risk assessment

Category 1 eGambling licensees are required to undertake individual risk assessments of each customer in accordance with their ICS. This can take place either at the time of registration or as soon as is reasonably practicable thereafter (regulation 227(2) of the Regulations – see Appendix 2).[14]

4.2.2 Obligation to Identify and Verify Identity

The Category 1 eGambling licensee must establish that –

(1) their customer exists on the basis of appropriate identification data (*identification data are documents, data or information relating to identification which are from a reliable and independent source*) and;

[14] The ICS must therefore define this process. The ICS must define the processes that ensure that no anonymous accounts can be set up and should also outline how it will ensure that accounts are not set up in names which the Category 1 eGambling Licensee knows to be fictitious or has reasonable cause to suspect are fictitious (regulation 228 of the Regulations – see Appendix 2). In addition this individual risk assessment must be regularly reviewed taking into account factors which come to light during the reviews of the business risk assessment which take place. The ICS must define when customer due diligence measures will be carried out. In the event that verification cannot take place at registration, the ICS must explain what policies, procedures and controls will manage this risk. The Regulations permit the verification of the identity of the customer to be completed after registration when the need to do so is essential so as not to interrupt the normal conduct of the licensee's business. Category 1 eGambling Licensees would need to explain in the ICS why it cannot be carried out at registration and what the timescale for carrying it out would be. For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

(2) that customer, beneficial owner or underlying principal is the person they say they are by verifying from identification data satisfactory confirmatory evidence of appropriate components of their identity.

This means that the Category 1 eGambling licensee must have suitable policies procedures and controls in place which provide the scope to identify and verify the identity of the customer to a depth appropriate to the assessed risk of the customer relationship.

The policies, procedures and controls must be risk based so as to differentiate between what is expected in standard risk situations and what is expected in higher risk situations (where enhanced CDD would be required, for example when dealing with a customer in a territory or jurisdiction which fails to or inadequately applies FATF recomendations). Within the eGambling industry on Alderney there are only standard risk and high risk customer relationships as the concept of a low risk relationship does not feature in the eGambling sector.

The Category 1 eGambling licensee must determine, in accordance with the risk based approach set out in its Business Risk Assessment the extent of the identification and verification information to ask for, what to verify and how this information is to be verified in order to be satisfied as to the identity of its customer, beneficial owner or underlying principal.

Where the customer is a legal person as opposed to a living individual (natural person) the legal status of the legal person or legal arrangement must be verified and information must be obtained about the name of the customer, its legal form, its address, its directors and provisions relating to the power of the entity to enter into eGambling arrangements. In addition the Category 1 eGambling licensee must be satisfied that it knows who the beneficial owner or underlying principal is, including, in the case of a legal person, trust or other legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement. Where the individual or business relationship presents a high risk then the eGambling licensee must consider the extent of additional verification required (see section 5).

Category 1 eGambling licensees should note that when undertaking customer due diligence measures they should comply with the terms of the Data Protection (Bailiwick of Guernsey) Law, 2001.

4.2.3 Identification and Verification of Customers who are Individuals

The identification and verification of customers is a two stage process. Firstly the customer must identify himself to the Category 1 eGambling licensee by the provision of a range of personal information. Secondly, this personal information is then verified by the Category 1 eGambling licensee through the use of identification data.

4.2.3.1 Identification data for individuals

The nature of the personal information to be collected by the Category 1 eGambling licensee on an individual will include legal name, address, date of birth, place of birth, nationality and unique identifiers contained within official documents such as driving licences, passports or identity cards. In addition obtaining occupation information will assist in respect of making the determinations necessary regarding politically exposed people.

4.2.3.2 Verification of identity: the individual

The personal information must be verified. Verification may take the form of obtaining copies of documents which would confirm the identity of the customer such as a current passport, driving licence, armed forces identity card or other government issued identity card.

The examples set out above are not the only possibilities. Depending on where the customer is based other forms of documentation may be available and suitable in order to evidence the identity of the individual.

4.2.3.3 Verification of identity: the address

Verification of the customer's address is most likely to come from the use of commercial electronic databases but can come from the possession of a driving licence, a bank or credit card statement or a utility bill. In addition electoral roll information can be used in the verification process.

Where the eGambling licensee is not familiar with the form of evidence forming the identification data it must take reasonable measures to satisfy itself that the evidence is genuine. For example, if a document is not in English they may need to be translated and they should be considered by an employee familiar with the nature of documentation from that jurisdiction.

4.2.4 Identification and Verification of Customers who are not living individuals

In the event that the customer is not a living individual the checks to be performed will be different. These will include the identification and verification of the legal body[15] or legal arrangement as well as verifying the legal status of the legal body or legal arrangement. This will include the name, number, date and country of incorporation together with the registered office and principal place of business.

There will also need to be the identification and verification of individuals ultimately holding a 25% or greater interest in the capital or net assets of the legal body as well as the identification and verification of the individuals including beneficial owners, underlying principals, directors, authorised signatories or the equivalents with ultimate effective control over the capital assets of the legal body.

Verification of the legal status of the legal body may be made through the use of the following documents:-

- a copy of the certificate of incorporation (or equivalent);
- a company registry search;
- a copy of the most recent audited financial statements;
- a copy of the Memorandum and Articles of Association;
- a copy of the Directors' register;
- a copy of the shareholders' register;

[15] For the purposes of this guidance a legal body is a legal person as set out in the legislation and references to legal person and legal body are used interchangeably.

- independent information sources including electronic business information sources; or
- a copy of the Board resolution authorising the opening of the account and recording account signatories.

Where the documents provided are copies of the originals the Category 1 eGambling licensee must ensure that they are certified by the company secretary, director, manager or equivalent officer.

The Category 1 eGambling licensee must also consider whether additional checks are necessary given the non face-to-face nature of the business relationship, for example where the documents may be in a different format to those they are familiar with due to local differences

4.2.5 Identification and Verification Systems

Under paragraph 5A of Schedule 16 to the Regulations (see Appendix 2). Category 1 eGambling licensees must ensure that their customer identification and verification systems –

- incorporate robust and effective client identification methods and measures in order to adequately manage and mitigate the specific risks of non face-to-face customer relationships or transactions inherent in the eGambling industry; There can be no occasional transactions in the eGambling industry.
- supplement identification verification software with additional forms of CDD and identity verification procedures in circumstances which are appropriate and effective for the purposes of managing and mitigating the risks of non face-to-face customer relationships and transactions and forestalling, preventing and detecting money laundering and terrorist financing. As eGambling is not face-to-face Category 1 eGambling licensees must take adequate measures to mitigate the risks that when the customer is not present. This includes a requirement that additional documents are provided when necessary;
- are approved by the Commission and integrated in their ICS. Category 1 eGambling licensees must identify in their internal control system

what forms of identification and verification will be considered to be acceptable. This means that the identification verification software and additional or alternative identification methods must be first approved by the Commission and should they wish to make changes they will need to seek an amendment to their approved ICS.

Category 1 eGambling licensees can make use of third party suppliers when undertaking customer due diligence measures. The methods of identification and verification utilised by the Category 1 eGambling licensee may be electronic although the value of these will depend on the number of sources used including both positive and negative information sources. Category 1 eGambling licensees are liable for any errors and omissions which lead to breaches of the CDD requirements so it is vital that they ensure that they obtain their information from reliable sources.

In addition paragraph 5A of Schedule 16 to the Regulations requires that Category 1 eGambling licensees have these methods and sources approved by the Commission.

4.2.6 Other Customer Due Diligence Measures

Regulation 227(4) of the Regulations (see Appendix 2) requires that a Category 1 eGambling licensee makes a determination as to whether the customer is acting on behalf of another person. A Category 1 eGambling licensee should ensure that those potential customers entering the registration process are required to confirm that they are acting as principal and that they are not acting on behalf of another person in order to complete the customer registration process.

In addition customer due diligence includes identifying the beneficial owner or underlying principal. Where there is a beneficial owner of underlying principal who is not the customer, that beneficial owner or underlying customer must be identified and the identification verified using identification data and where the beneficial owner or principal is a legal person or legal arrangement measures must be taken to understand the ownership and control structure of that entity.

There is also a requirement that a determination is to be made as to whether or not the customer, beneficial owner or underlying principal is a politically exposed person (regulation 227(2) of the Regulations – see section 6 and Appendix 2).

In addition there is a requirement that information shall be obtained on the purpose and intended nature of the business relationship (paragraphs 2 and 10(1) of Schedule 16 to the Regulations – see Appendix 2).

4.2.7 Timing of Identification and Verification

These identification processes must be undertaken prior to commencing the relationship with the customer. However under paragraph 4 of Schedule 16 to the Regulations (see Appendix 2) the verification of the identity of the customer may, subject to there being appropriate and effective policies, procedures and controls in place to mitigate the risk, be completed following the establishment of the business relationship provided that it is completed as soon as reasonably practical thereafter and the need to do so is essential not to interrupt the normal conduct of the Category 1 eGambling licensee's business.

4.2.8 Anonymous or fictitious accounts

Within the eGambling sector in Alderney there can be no anonymous accounts or accounts in fictitious names. In addition all accounts must be maintained in a manner which facilitates the meeting of the obligations placed on the Category 1 eGambling licensee by the Regulations (regulation 228 of the Regulations – see Appendix 2).

4.3 Failure to complete or comply with Client Due Diligence Procedures

Where a Category 1 eGambling licensee finds themselves unable to comply with the provisions set out in paragraphs 2 or 3 of Schedule 16 of the Regulations (see Appendix 2) they must, if there is already a customer relationship, terminate that relationship and where there is no existing customer relationship, not enter into the proposed customer relationship. Further in either case consideration must be given as to whether a disclosure must be made to the FIS under the Terrorism Law or the Disclosure Law.

4.4 The ongoing nature of CDD

Licensees also need to be aware that CDD is not a one off obligation. The performance of CDD measures must be undertaken at various stages during the currency of the customer relationship. This can be at certain stages during the relationship based on time or can be in response to trigger events.

For example, a Category 1 eGambling licensee must undertake CDD on registered customer –

- if the customer makes a deposit of or exceeding €3000, or
- where the value of deposits in any period of 24 hours reaches or exceeds €3000.

In this scenario, a Category 1 eGambling licensee may revert to the CDD previously undertaken to confirm that it is still satisfied that the information it holds is correct. Where a Category 1 eGambling licensee outsources player verification to a third party provider whose data is updated on a periodic basis, and the Category 1 eGambling licensee requires updated or revised player verification, further due diligence checks via that third party may be necessary where the Category 1 eGambling licensee or the third party provider cannot confirm the continuing accuracy of the verification information previously provided. Where a Category 1 eGambling licensee has grounds to suspect that the information it holds may no longer be correct then it should, as a matter of course, undertake customer due diligence measures again.

Category 1 eGambling licensees are also under an obligation to perform ongoing and effective monitoring of identification data in order to ensure that it is kept up to date and relevant, particularly in relation to high risk customers (paragraph 6(1) of Schedule 16 to the Regulations – see Appendix 2).

4.5 Examples of when CDD must be performed

4.5.1 Deposit based verification.

For example if a customer makes a deposit of €2950 and subsequently makes a further deposit of €100 23 hours later then CDD must be performed. A customer who deposits €2950 and deposits a further €100 25 hours later would not automatically trigger CDD (however, the licensee may consider the transactions to be linked for other reasons, which would trigger CDD).

4.5.2 Intelligence based verification.

At other times the vigilance of the Category 1 eGambling licensee may lead them to undertake CDD measures at a time when they would not automatically be required to do so. This intelligence may be in the form of a written record being received by a Category 1 eGambling licensee from the Category 2 eGambling licensee effecting the gambling transaction. This may provide sufficient grounds or information to submit an STR to the FIS.

4.5.3 Suspicion based verification.

CDD measures must also be undertaken if the Category 1 eGambling licensee suspects, or has reasonable grounds for suspecting, that a person is engaged in money laundering or terrorist financing or where it has concerns about the adequacy of documents, data or information previously obtained.[16]

CUSTOMER DUE DILIGENCE **Key Legislative Provisions:**
• regulations 226, 227, 229 (customer registration) • regulation 228 (customer accounts) • Paragraph 2 of Schedule 16 to the Regulations (customer due diligence) • Paragraph 4 of Schedule 16 to the Regulations (Timing of Identification and Verification) • Paragraph 5 of Schedule 16 to the Regulations (Non Compliance with Customer Due Diligence Measures)

[16] The ICS must define when CDD will be carried out and where applicable explain the frequency with which this information is updated. For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

- Paragraph 5A of Schedule 16 to the Regulations (Customer Identification and Verification Systems)
- Paragraph 10 of Schedule 16 to the Regulations (Definitions – including Customer Due Diligence Measures, Customer Due Diligence Information, Identification Data)

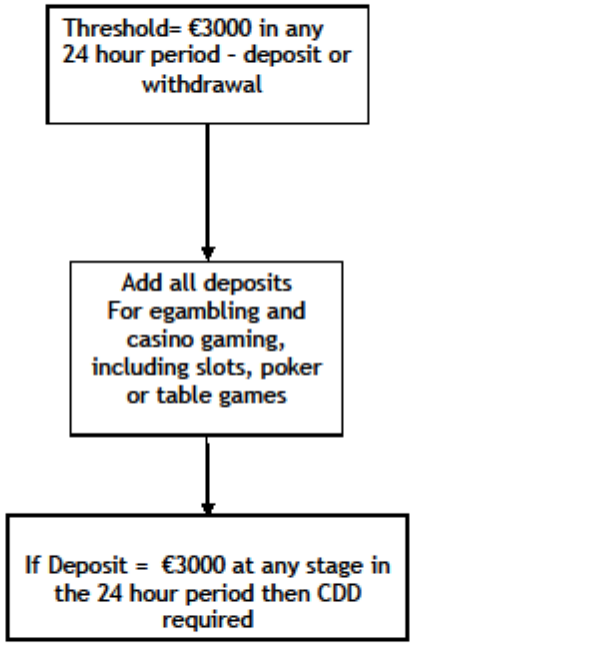
To summarise:

CDD must be performed by a Category 1 eGambling licensee

- prior to registration
- when a customer deposits €3000 or cumulative deposits in a 24 hour period reach or exceed €3000
- when a licensee has suspicions or cause to suspect a customer is engaged in money laundering or terrorist financing
- where it doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification of a customer
- In line with the Category 1 eGambling licensees Business Risk Assessment in respect of ongoing CDD.

The table below sets out a flowchart for Category 1 eGambling licensees to follow in respect of customer deposits.

Determining when thresholds are reached - remote casinos
Depositing eGambling account funds



Note 1: The casino operator can set its own 24 hour period, for example the same hours as the business day, as appropriate to its business model

Note 2: Risk-based approach-
Operator analysis of spending behaviours at each site and an objective assessment made of the likelihood of customers reaching either threshold. Measures then put in place needed to capture all customers likely to hit either threshold

5. Enhanced customer due diligence

5.1 Introduction

There will be circumstances where the standard level of customer due diligence measures may not be sufficient and additional measures will be required. These are called enhanced customer due diligence measures. These will include instances where the individual risk assessment of the customer results in the Category 1 eGambling licensee considering the customer to be a high risk. They will also include those relationships where the customer, beneficial owner or underlying principal is a Politically Exposed Person (See section 6 below) as well as those instances where the customer is established or situated in a country or territory which does not apply, or insufficiently applies, the FATF Recommendations.

5.2 What is involved in enhanced customer due diligence?

Enhanced customer due diligence involves procedures above and beyond those measures employed during standard customer due diligence.[17] On those occasions where customers are asked to provide further information to meet enhanced customer due diligence measures they should not feel they are being treated unfairly or are being labelled as a money launderer. Instead they may wish to consider that the licensee is being vigilant and so helping the fight against money laundering and the financing of terrorism as well as potentially preventing customer details from being used fraudulently.

[17] In relation to enhanced customer due diligence measures, the ICS will need to address the following items:

- the additional identification information to be obtained and, obtaining such data.
- the additional aspects of the identity of the customer needing to be verified and, verifying these aspects.
- taking reasonable measures to establish the source of funds and wealth of the customer, any beneficial owner or underlying principal.
- the carrying out of more frequent and more extensive ongoing customer monitoring.

For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

Under paragraph 3 of Schedule 16 to the Regulations (see Appendix 2), where a Category 1 eGambling licensee undertakes CDD it must undertake enhanced CDD in relation to customer relationships where:-

- The customer is established or situated in a country or territory that does not apply, or insufficiently applies, the FATF recommendations on money laundering;
- The Category 1 eGambling licensee considers the customer relationship to be a high risk relationship pursuant to regulation 227(2) or 229 or taking into account any notices issued by the Commission pursuant to Section 22(3) of the Ordinance; or
- The customer or any beneficial owner or underlying principal is a politically exposed person.

Enhanced CDD is defined in paragraph 10 of Schedule 16 to the Regulations (see Appendix 2) and means that the Category 1 eGambling licensee will need to:-

- Obtain senior management approval to establish the customer relationship;
- Obtain senior management approval to continue a customer relationship with a politically exposed person;
- Take reasonable measures to establish the source of any funds and of the wealth of the customer, beneficial owner or underlying principal;
- Carrying out more frequent and more extensive ongoing monitoring in accordance with paragraph 6 of Schedule 16 of the Regulations;
- Take such steps as are necessary to the customer relationship namely
    - Obtaining additional identification data;
    - Verifying additional aspects of the customer's identity; and/or
    - Obtaining additional information to understand the purpose and intended nature of each customer relationship.

5.3 Source of funds and source of wealth

The source of funds refers to the activity which generates the funds for the customer relationship.

The source of wealth is distinct from the source of funds, and it describes the activities which have generated the total net worth of a person.

It is important for the Category 1 eGambling licensee to understand the customer's source of funds and source of wealth – particularly in relationships with PEPs.

ENHANCED CUSTOMER DUE DILIGENCE

Key Legislative Provisions

- Paragraph 3 of Schedule 16 to the Regulations (additional customer due diligence)
- Paragraph 10 of Schedule 16 to the Regulations (definitions including "enhanced customer due diligence"

To summarise Category 1 eGambling licensees must note that:

Enhanced customer due diligence is necessary for:

- high risk customers (pursuant to regulation 227(2) or 229 or taking into account any notices issued by the Commission pursuant to Section 22(3) of the Ordinance)
- politically exposed persons
- customers in certain jurisdictions (i.e. countries or territories that do not or insufficiently apply the FATF Recommendations and other high risk countries or territories)

Enhanced due diligence measures to be undertaken by the Category 1 eGambling licensee include:

- considering what additional information is needed
- obtaining further information
- obtaining senior management approval
- taking further steps to verify customers' identities
- carrying out more frequent monitoring

6. Politically Exposed Persons

6.1 Introduction

A Politically Exposed Person ("PEP") is defined in paragraph 10 of Schedule 16 of the Regulations (see Appendix 2) as an individual who has, or has had at any time, a prominent public function or who has been elected or appointed to such a function in a country or territory outside the Bailiwick of Guernsey. This makes the definition very wide ranging. PEP's include:-

- Heads of state or heads of government;
- Senior politicians and other important officials of political parties;
- Senior government officials;
- Senior members of the judiciary;
- Senior military officers; and
- Senior executives of state owned body corporates.

In addition immediate family members of people in the above list are PEP's. Immediate family includes spouses, partners, children, siblings, parents in law, and grandchildren. Close associates of people in the above list are also classed as PEP's. Close associates include someone who is widely known to maintain a close business or professional relationship with such a person and people who are in a position to conduct substantial financial transactions with such a person.

The fact that a person is a PEP does not automatically mean that they are involved in money laundering or terrorist financing. It is however something that results in an alteration to that person's risk profile and causes them to be subject to additional customer due diligence measures (paragraph 3 of Schedule 16 to the Regulations – see Appendix 2). Category 1 eGambling licensees are required to carry out enhanced CDD on customers who are PEP's and in order to do so they must first ascertain whether a customer is a PEP (regulation 227 (2) of the Regulations – see Appendix 2).

6.2 Examples of PEPs

By way of examples, the following people would, during their lifetime, have been a PEP as defined by the legislation. It covers people from a number of walks of life and

some of these names will be familiar, others less so and it is this that highlights the problems that can be faced in identifying those that this term applies to.

Examples of people who would have been a PEP in the politician category are Ted Heath, Ronald Reagan, Benazir Bhutto and Gwyneth Dunwoody, because they had been elected to a prominent public function outside the Bailiwick of Guernsey.

Denis Thatcher would also have fallen into the category of PEP through being immediate family of someone elected to a prominent public function outside the Bailiwick of Guernsey.

Examples of PEP's in other categories would be Creighton Abrams, Lord Hussey of North Bradley and Sir Peter Parker. Abrams, or to give him his full title, General Creighton Williams Abrams Jr, was the Commander of US forces in Vietnam, a former senior military officer. Lord Hussey was the former chairman of the BBC and Sir Peter Parker was the former chairman of British Rail: both would have been a PEP by virtue of having been senior executives of state owned bodies outside of the Bailiwick of Guernsey.

6.3 What steps need to be taken?

The Category 1 eGambling licensee must consider how they will identify a new customer as being a PEP and how they will screen for such people on an ongoing basis. If a PEP is to be accepted as, or is to continue as a customer there must be approval from the Category 1 eGambling licensees' senior management and they must therefore define how such approvals will be sanctioned, the measures that will be taken to establish the source of wealth and funds of the individual and how the customer relationship will be monitored on an ongoing basis. The Category 1 eGambling licensee must also explain what steps they will take to identify PEPs during the registration process. There must be systems in place to ensure that a PEP is not allowed to become a customer on an automatic basis.[18] This area does pose a significant risk for operators. There is a real risk of PEPs registering and playing

[18] If the PEP is not present during registration, i.e. when Senior Management approval takes place, then the ICS should specify the measures the Category 1 eGambling licensee will take on a risk-sensitive basis to recognise the risks when carrying out customer due diligence measures and the monitoring of that customer relationship.

without the appropriate levels of senior management approval and customer due diligence taking place. This is why systems must be in place to manage such risk.

Establishing whether a person is a PEP is not straightforward and may require a number of different processes to be involved. Licensees must describe the processes employed to screen for and identify PEPs, both amongst existing customers and new customers. This could include the use of internet search engines or subscriptions to suitable commercial databases. The databases used for customer due diligence may be able to assist in this regard.[19] The Transparency International Corruption Perceptions Index may also be of use. This is available to download from

http://www.transparency.org/policy_research/surveys_indices/cpi.

and will help licensees establish which countries pose greater risks of corruption and establishing who are the current and former holders of prominent public functions in those countries and determining, as far as reasonably practicable, whether or not customers, beneficial owners or underlying principals have any connections with such individuals.

Category 1 eGambling licensees must also address how they will monitor the status of their customers as existing customers may over time become PEPs. It should be noted that under the legislation in place in the Bailiwick, once a person has been identified as a PEP they will always continue to be considered as one and therefore subject to the appropriate levels of monitoring and due diligence.[20]

[19] The ICS should specify the steps that will be taken by the Category 1 eGambling licensee to ensure that PEPs are not allowed to register and play on an automated basis. For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

[20] The ICS should explain what steps will be taken by the Category 1 eGambling licensee to screen for PEPs both during the registration process and thereafter to identify those people who subsequently become PEPs. For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

POLITICALLY EXPOSED PERSONS

Key Legislative Provisions:

- Regulation 227 (2) (identification of PEPs)
- Paragraph 3 of Schedule 16 to the Regulations (additional customer due diligence measures required for PEPs)
- Paragraph 10 of Schedule 16 to the Regulations (definitions, including definition of "politically exposed person").

To summarise:

Politically exposed persons are:

- elected or appointed politicians outside the Bailiwick
- people holding a prominent public function outside the Bailiwick
- the immediate families and close associates of such people

Politically exposed persons require:

- senior management approval to become a customer
- additional customer due diligence
- additional monitoring
- establishment of the source of wealth and funds

7. FAILURE TO COMPLETE CUSTOMER DUE DILIGENCE.

There may be occasions where it is not possible for customer due diligence measures to be completed. This could be for any number of reasons.[21] In such instances there needs to be a mechanism in place to ascertain what issues have arisen and to bring about a resolution to the situation. Under paragraph 5 of Schedule 16 to the Regulations (see Appendix 2), in all cases –

- Where CDD cannot be completed for a person applying to be a customer, the Category 1 eGambling licensee **must not register** that person as a customer.

- Where CDD cannot be completed in relation to a person that is an existing customer, the Category 1 eGambling licensee **must terminate** the customer relationship.

- In both cases (where the registration is not concluded or the existing customer relationship is terminated) consideration must be given to whether a disclosure should be made and is required pursuant to the Disclosure Law or Terrorism Law.

FAILURE TO COMPLETE CUSTOMER DUE DILIGENCE

Key Legislative Provisions:

- Paragraph 5 of Schedule 16 to the Regulations (Non-Compliance with customer due diligence measures)

To summarise:

The Category 1 eGambling licensee must:

[21] The ICS will need to explain the measures that will be taken by the operator should this occur. In particular the ICS will need to detail the processes that will be taken not to register a prospective customer and to terminate the customer relationship where the failure relates to an existing customer. In addition the ICS should highlight the steps that will be taken to ensure that the obligations of the operator with regard to Part I of the Disclosure Law and section 12 of the Terrorism Law are met as to whether the circumstances warrant the making of a disclosure. For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

- Where CDD cannot be completed for a person applying to be a customer, the Category 1 eGambling licensee must not register that person as a customer.
- Where CDD cannot be completed in relation to a person that is an existing customer, the Category 1 eGambling licensee must terminate the customer relationship.
- explain the processes to be followed when CDD or enhanced CDD fails
- consider its disclosure obligations in such cases

8. MONITORING TRANSACTIONS AND OTHER ACTIVITY

8.1 Objective

Category 1 eGambling licensees are required to monitor the relationships they have with their customers. Category 2 eGambling licensees and associate certificate holders must monitor the activity they facilitate. This must be ongoing and effective. This monitoring can have an impact upon the risk profiles that might be assigned to the customers of a Category 1 eGambling licensee. This will help to identify things which are unusual. This has benefits both in terms of ensuring compliance with AML/CFT obligations but can also help with fraud protection generally.[22]

The monitoring requirements for licensees can be found in paragraph 6 of Schedule 16 of the Regulations (see Appendix 2).

8.2 Obligation to Monitor

Category 1 eGambling licensees

[22] The ICS will need to explain what monitoring the Category 1 eGambling licensee will undertake and on what basis and frequency bearing in mind that it must as a minimum cover the following:

- Identification data – is it up to date and relevant? This is a particular requirement to those customers who have been identified as being high risk. How often is it checked?
- The storage of identification data. Does the way this is stored facilitate the ongoing monitoring of the customer relationship? Can it be easily accessed by those who might need to refer to it?
- Transactions. These must be scrutinised to ensure that they are consistent with the knowledge that the Licensee has of the customer and the customer's individual risk profile. Particular attention should be paid to those transactions that are:
    - complex
    - both large and unusual
    - part of an unusual pattern
    - arising from a country or territory that does not apply or insufficiently applies the FATF Recommendations

  And which have no apparent economic or lawful purpose.

The ICS must also define how the licensees' written findings in these respects will be stored. Again can these be easily accessed if needed?

For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

Category 1 eGambling licensees are required to monitor all existing customer relationships which includes –

(i) the review of identification data in order to ensure that it is kept up to date and relevant (particularly in relation to high risk customers);

(ii) ensure the way in which identification data are recorded and stored is such as to facilitate the ongoing monitoring of each customer relationship;

(iii) scrutinise transactions in order to ensure that they are consistent with the licensee's knowledge of the registered customer and its risk profile, paying particular attention to –

- complex transactions,
- transactions which are both large and unusual,
- unusual patterns of transactions, and
- transactions arising from a country or territory that does not apply or insufficiently applies the FATF Recommendations,

which have no apparent economic purpose or no apparent lawful purpose.

Scrutiny of transactions and activity must be undertaken throughout the course of the business relationship to ensure that the transactions and activity being conducted are consistent with the Category 1 eGambling licensees' knowledge of the customer, their source of funds and the source of their wealth.

It is likely that the monitoring undertaken by licensees will include the following:-

- new customer registrations
- deposit activity
- gambling history
- account access (time and location)
- account detail changes
- withdrawal activity
- registration data

Licensees will need to look at the following:-

- Customer identity, CDD and identification data

- Customer financial habits and behaviours to ensure that the transactions are consistent with the licensee's knowledge of the customer's risk profile
- Customer gambling habits and behaviours to ensure that the transactions are consistent with the licensee's knowledge of the customer's risk profile
- Individual and linked transactions which are complex or unusually large with no apparent economic or lawful purpose
- Unusual patterns of transactions with no apparent economic or lawful purpose
- Transactions which exceed certain limits with no apparent economic or lawful purpose
- Very high account turnover inconsistent with the account balance
- Transactions which are outside the customer's regular transaction activity.

Category 2 eGambling licensees and Category 2 Associate Certificate holders

Category 2 eGambling licensees and Category 2 associate certificate holders must monitor gambling transactions, paying particular attention to –

- complex transactions,
- transactions which are both large and unusual,
- unusual patterns of transactions, and

which have no apparent economic purpose or no apparent lawful purpose.

The Category 2 eGambling licensee or Category 2 associate certificate holder must scrutinise gambling transactions to ensure that the customers of the Category 1 eGambling licensee are not acting in a suspicious manner in respect of their activity.

General obligations

eGambling licensees will be looking for activity or patterns of activity which are inconsistent with the expected pattern of activity within that business relationship. This could indicate money laundering or terrorist financing activity where the transactions or activity have no apparent economic or visible lawful purpose.

This monitoring must be conducted in line with a risk based approach and should factor in greater monitoring of high risk relationships (i.e. those where enhanced CDD measures have been applied) to normal customer relationships. Consideration will need to be given to matters such as the frequency of monitoring and how monitoring is to be effective.

Monitoring requirements are likely to be greater in respect of customers based in or transactions originating from jurisdictions specified in Business from Sensitive Sources Notices (BSSN's) issued by the Commission.

eGambling licensees must examine the background and purpose of complex, unusual and large transactions as well as unusual patterns of transactions (and in the case of Category 1 eGambling licensees, those transactions arising from countries and territories which do not apply or insufficiently apply FATF recommendations) and must record such findings in writing. Where a Category 2 eGambling licensee or Category 2 associate certificate holder records such findings in writing it shall as soon as reasonably practicable communicate such findings to the MLRO of the Category 1 eGambling licensee who allowed its customer to gamble with or through it to effect the gambling transaction.

In order to undertake monitoring licensees will need to ensure that their staff receive training to monitor effectively – so they can recognises potential money laundering and terrorist financing and other suspicious activity including matters relating to attempts to influence event based wagering.

MONITORING TRANSACTIONS AND OTHER ACTIVITY

Key Legislative Provisions:

- paragraph 6 of Schedule 16 to the Regulations (monitoring transactions and other activity)

To summarise:

For Category 1 eGambling licensees there needs to be monitoring of:

- identification data
- recording and storage of identification data
- transactions, in particular those that are
  - complex
  - large and unusual
  - part of an unusual pattern
  - arise from a country that does not or insufficiently applies FATF Recommendations

which have no apparent economic purpose or no apparent lawful purpose.

For Category 2 eGambling licensees or Category 2 associate certificate holders there needs to be monitoring of gambling transactions, in particular those that are –

- complex
- large and unusual
- part of an unusual pattern

which have no apparent economic purpose or no apparent lawful purpose.

Licensees and certificate holders shall examine as far as reasonably possible the background and purpose of the above transactions and set out its findings in writing.

The extent and frequency of monitoring must be determined on a risk-sensitive basis (including whether or not a customer relationship is high risk or not).

Where a Category 2 eGambling licensee or Category 2 associate certificate holder sets out in writing the findings of its monitoring it must communicate those findings to the relevant Category 1 eGambling licensee.

9. RECORD KEEPING

It is a requirement that records are kept for a number of reasons. The primary reason is to ensure that there is an audit trail available in the event that a financial or other investigation is undertaken by a law enforcement body. It is essential that records are kept to assist in any investigation and to ensure that criminal funds are kept out of the industry, or if not, that they may be detected and confiscated by the appropriate authorities.

Unlike the terrestrial gaming sector, a Category 1 eGambling licensee will always enter into a business relationship with a customer. Therefore there can be no occasional or one off transactions. Category 2 eGambling licensees and Category 2 associate certificate holders are required to keep records in order to ensure that there is a full audit trail in respect of the gambling transactions made by the customer of the Category 1 eGambling licensee.

The requirements for record keeping are set out in paragraph 9 of Schedule 16 of the Regulations (see Appendix 2).

9.1 General Requirements

Licensees must retain the following information –

- **transaction documents** (defined as a document which is a record of a transaction carried out by an eGambling licensee or Category 2 associate certificate holder with a registered customer and which, as a minimum, identifies the customer (in the case of a Category 1 eGambling licensee only), the nature and date of the transaction and the type and amount of the currency involved and the identifying number of any account involved in the transaction),

- **customer due diligence information** (information obtained by the Category 1 eGambling licensee during the CDD (or enhanced CDD) procedure relating to the identification and verification of the customer) and any other information relating to the customer relationship,

- **any findings relating to unusual or suspicious transactions (including the background and purpose of any such transactions)**,
- **any reports made to the MLRO under the Disclosure or Terrorism Law,**
- **any training** carried out in relation to AML/CFT matters, and
- **documents prepared pursuant to paragraphs 1(2) and 9A(1)(e)** of Schedule 16 to the Regulations **,**
- **policies, procedures and controls** that are required pursuant to the Regulations.

To ensure that the record keeping requirements of the Regulations are met, a licensee must have appropriate and effective policies, procedures and controls in place to require that records are prepared, kept for the stipulated period and are in retrievable form so as to be available in a timely basis by the Financial Intelligence Service as well as other domestic competent authorities. [23]

9.2 Retention Periods

The Regulations set out certain retention periods for certain documents and information.

Transaction documents, or a copy thereof, must be kept for 5 years from the date of the transaction or the date of completion of any related transaction.[24] Customer due diligence information, or copies thereof, must also be kept for a minimum of 5 years[25] from the date the person concerned ceases to be a registered customer. There is scope for these to be held in a number of formats.[26]

---

[23] The ICS must address the procedure that will be used to ensure this. For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

[24] Unless the Commission, The Financial Intelligence Service or an officer of the police has directed that the retention period should be longer.

[25] Unless the Commission, The Financial Intelligence Service or an officer of the police has directed that the retention period should be longer.

[26] The ICS should set out how these will be kept, the security arrangements that will apply and processes for retrieval. For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

The licensee should note that the Commission, the Financial Intelligence Service or an officer of police can direct that records be kept for a period greater than 5 years.[27] The production of these could be required as a result of a court order, an enactment or rule of law and the operator must be in a position to respond to such demands.

Where a Category 1 eGambling licensee has, as a result of monitoring transactions, discovered transactions that are complex, both large and unusual, part of an unusual pattern, or arising from a country or territory that does not apply or insufficiently applies the FATF Recommendations and which have no apparent economic or lawful purpose, it must maintain the written record of its findings for 5 years from the date the record was created.[28]

Where a Category 2 eGambling licensee or Category 2 associate certificate holder has, as a result of monitoring transactions, discovered gambling transactions that are complex, both large and unusual, or part of an unusual pattern and which have no apparent economic or lawful purpose, it must maintain the written record of its

[27] The ICS should address the capability of the licensee to deal with that eventuality. The ICS should also address how the licensee will provide this information during the retention period should it be called upon to do so. The ICS should also set out how the licensee will maintain a register of the transaction documents and due diligence information that it can provide, as may be required to during this period, and how it will ensure that it maintains a copy of the transaction document or customer due diligence information until either the original is returned or the retention period ends, depending on which occurs first. For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

[28] The ICS should outline the procedures that will be followed in the event that the MLRO makes a report to the Financial Intelligence Service and should also outline the procedures followed in the event that a disclosure is made other than by a report to the MLRO. It must also provide details of how such reports will be stored for 5 years from the date that the person concerned ceased to be a registered customer. Licensees may also consider dealing with those occasions where a prospective customer has, for whatever reason, failed to become a registered customer. The ICS must provide information about the processes to be followed in recording the training that employees receive to meet the licensee's training obligations under these Regulations. These records must be kept for 5 years starting from the date the training took place. Discretion exists as to how this information can be stored. In addition, the licensee's ICS must detail how and in what form minutes and other documents prepared pursuant to Regulation 188 will be kept for the period of 5 years from being finalised, or such time as they are superseded by later minutes prepared under that regulation, whichever is the later. In addition the ICS must outline how the policies, procedures and controls established as a result of the money laundering amendment regulations are to be retained for a period of 5 years starting from the date that they cease to be operative. This includes previous iterations of the relevant sections of the ICS. Licensees have discretion as to the format or medium in which these are retained. For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

findings for 5 years from the date the record was created. Where a Category 2 eGambling licensee or Category 2 associate certificate holder sets out such findings in writing it shall as soon as reasonably practicable communicate such findings to the MLRO of the Category 1 eGambling licensee who had allowed its customer to gamble with or through it in order to effect a gambling transaction.

RECORD KEEPING

Key Legislative Provisions:

- paragraph 9 of Schedule 16 to the Regulations (record keeping)

To summarise:

Relevant documents must be kept for at least 5 years. These include:

- transaction records
- customer due diligence information
- suspicious transaction reports
- AML/CFT training records
- Any findings relating to unusual or suspicious transactions
- Documents prepared pursuant to paragraphs 1(2) and 9A(1)(e) of Schedule 16 to the **Regulations,**
- policies, procedures and controls that are required pursuant to the Regulations,

Information stored must be easily retrievable

10. SUSPICIOUS TRANSACTIONS

10.1 Obligation to Report

It is a legal obligation that those who work for a licensee know that they are under a duty to report suspicious transactions. These include instances:

- where they know; or
- where they suspect; or
- where they have reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing.

These three instances are referred to as “grounds for knowledge or suspicion”.

A suspicion may be based on a transaction or activity which is inconsistent with a customer's normal known activity. It follows that it is essential that a licensee knows enough about the customer relationship or pattern of gambling activity to recognise that a transaction or activity is unusual. Such knowledge would principally arise from complying with the monitoring and ongoing client due diligence requirements set out in paragraph 6 of Schedule 16 of the Regulations – see section 8 of this Guidance.

Licensees must ensure that appropriate training is provided in respect of the relevant enactments as set out in paragraph 10 of Schedule 16 of the Regulations (see Appendix 2). There is specific requirement that licensees train their staff regarding their obligations and the requirement to make reports to their MLRO or nominated officer.

Certain employees of a licensee will be relevant employees (as defined in the Regulations and includes any employee whose duties relate to eGambling). Such employees are more likely to be in positions where their duties could result in them having to make reports and disclosures. However it should be recognised that all employees have a part to play in the fight against money laundering and the financing of terrorism.

A licensee must establish appropriate and effective policies, procedures and controls in order to facilitate compliance with the reporting requirements of the Regulations. Licensees will need to therefore demonstrate how such reports can be raised and considered. They must provide a framework for how this is to be done.

10.2 Internal reporting to the MLRO

The relevant legislative provisions which relate to this paragraph are set out in paragraph 7(1) of Schedule 16 to the Regulations (see Appendix 2).

Licensees must ensure that their employees report to the money laundering reporting officer (MLRO) or in his absence their nominated officer when they have grounds for knowledge or suspicion that a person or customer is engaged in money laundering or terrorist financing. Licensees should be aware that their obligations in this respect extend beyond their customer base, but should also encompass contractors, business contacts and the like.

The MLRO or nominated officer must consider each report made to determine whether it gives rise to grounds for knowledge or suspicion.

In addition, as it is a requirement that the MLRO or nominated officer takes into account all relevant information prior to making a report, the ICS must address how the MLRO or nominated officer will be made aware of all relevant information. It is also a requirement that this information be provided promptly to the MLRO or

nominated officer.[29] Licensees will need to address how their employees refer matters to the MLRO or Nominated Officer [30]

10.3 Reporting to the FIS

The relevant legislative provisions which relate to this paragraph are set out in paragraphs 7(1) and 7(2) of Schedule 16 to the Regulations (see Appendix 2).

Where the MLRO or nominated officer determines that there are grounds for knowledge or suspicion, the matter must be reported to the Guernsey FIS as soon as is practicable in accordance with Part I of the Disclosure Law or Section 12 of the Terrorism Law. [31,] The Guernsey Financial Intelligence Service maintains a website at www.guernseyfis.org which can be a valuable source of information on AML and CFT generally as well as on some specific topics. It is through this website that the MLRO or nominated officer should access THEMIS, a dedicated online reporting portal maintained by the Guernsey Financial Intelligence Service for the reporting of suspicious transactions. All MLROs and nominated officers must obtain THEMIS credentials from the Guernsey Financial Intelligence Service.

Appendix 1 of this guidance contains a form for making a report to the Financial Intelligence Service. This form should only be used in the event that THEMIS is unavailable and may be subject to alteration and therefore the form should always be downloaded from the relevant section of the Financial Intelligence Service Website.

A copy of any suspicious transaction report must be submitted to the Alderney Gambling Control Commission. There is a dedicated email address for this – STR@agcc.gg – or the licensee can deliver it by post to The Alderney Gambling

[29] The ICS must address the systems that will ensure this takes place. For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.
[30] The ICS must also address the procedure that will take place in order to ensure that the Commission and the Financial Intelligence Service are notified of the name and title of the officer appointed as the Money Laundering Reporting Officer as soon as is practicable and in any event within 14 days starting from the date of that person's appointment. For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

[31] The ICS must also detail the procedure that will be adopted when a report is made to the Financial Intelligence Service under Part I of the Disclosure Law or Section 12 of the Terrorism Law to ensure that the Commission is provided with a copy either at the same time or as soon as practicable thereafter. For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

Control Commission, St Anne's House, Queen Elizabeth 2 Street, Alderney, GY9 3TB.

The FIS will acknowledge receipt of a suspicious transaction report in writing.

Licensees should always remember that failure to make an STR is a criminal offence. If you think an STR may be necessary then one should be submitted.

SUSPICIOUS TRANSACTIONS

Key Legislative Provisions:

- Paragraph 7 of Schedule 16 to the Regulations (reporting suspicion)

To summarise:

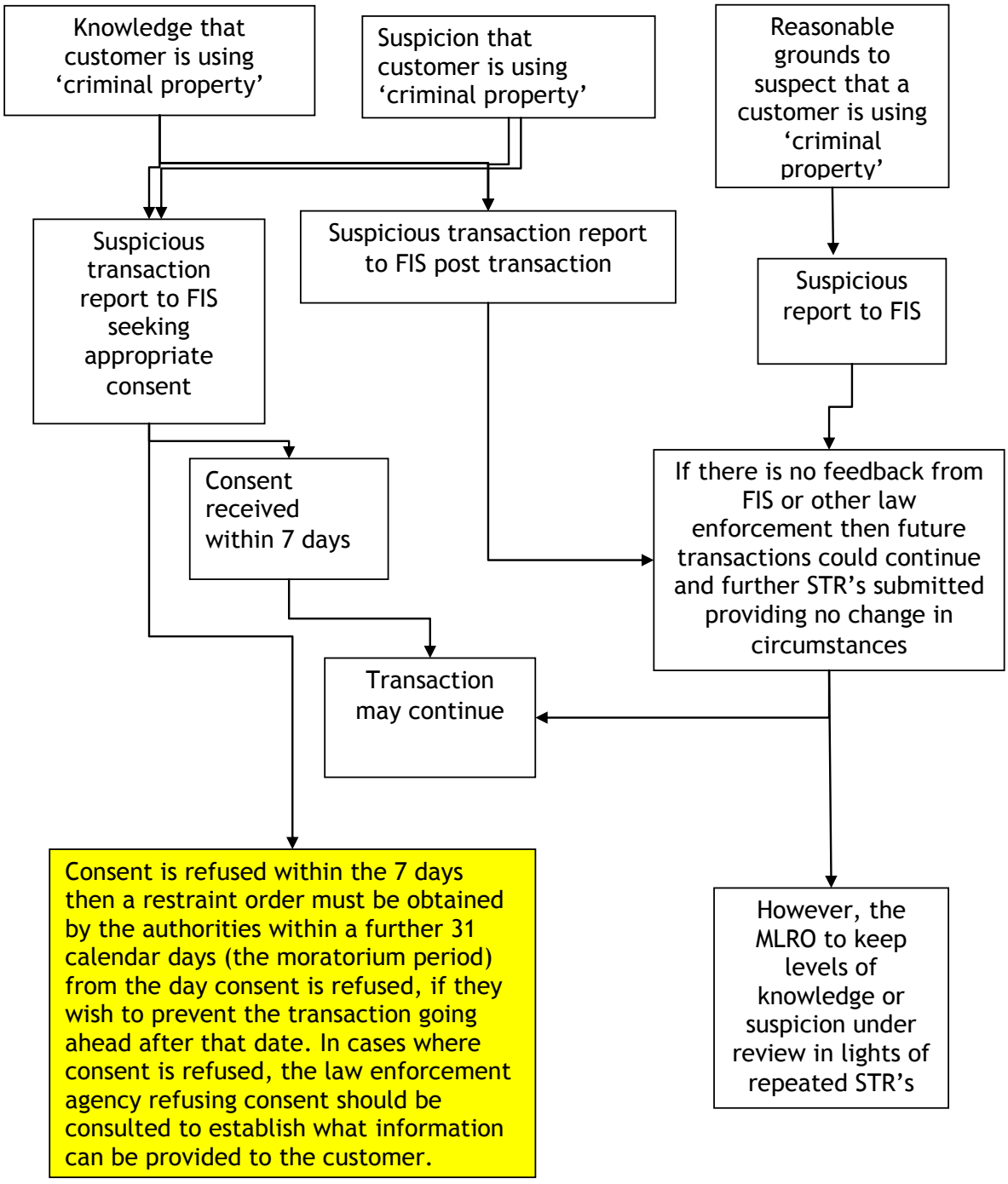
Reports of suspicious transactions must be made

- when employees know
- when employees suspect, or
- when employees have reasonable grounds for suspecting a person is engaged in money laundering or funding terrorism

Suspicious transaction reports must be:

- made to the Guernsey FIS
- in the form specified by the GFSC
- copied to the Commission

The table on this page sets out the process where consent may be given to a Category 1 eGambling licensee to conduct a financial transaction with a customer.



11. EMPLOYEE SCREENING AND TRAINING

11.1 Employee Screening

Dishonest staff present a fraud and business risk to licensees.[32]

In order for a licensee to ensure that employees are of a high standard of probity and competence, licensees must maintain and have effective policies, procedures and controls in place when hiring employees (paragraph 8(1)(a) of Schedule 16 to the Regulations – see Appendix 2).

11.2 Training

Poorly trained and untrained staff also pose a business risk to licensees. It is a requirement that relevant employees receive comprehensive ongoing training in a number of areas (paragraph 8(1)(b) of Schedule 16 to the Regulations – see Appendix 2). Licensees could address this issue through the use of training plans or schedules. These plans could be individual to members of staff. The application of a risk based approach allows licensees to tailor the training to the functions being undertaken by employees and the likelihood of their encountering suspicious activities.

All licensees must ensure that **relevant employees** (see paragraph 11.3) receive training in relation to - :[33]

[32] The ICS must outline the procedures adopted during the recruitment process to ensure high standards of employee probity and competence. This could include what checks are made, such as references, credit record checks and other vetting measures, verification of information given during the recruitment phase, and confirmation of identity. For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

[33] The ICS must also address which employees, by virtue of their responsibilities, should receive additional training in respect of the above topics and how that training is provided and the details recorded. For detailed guidance on internal policies, procedures and controls, please refer to the AGCC's ICS Guidelines.

- relevant enactments, the Gambling (Alderney) Law, 1999, the Ordinance, the Regulations and relevant guidance issued by the Commission which relates to AML/CFT.

- the personal obligations of employees and their potential criminal liability under the relevant enactments and the Ordinance

- the implications of employee non-compliance with guidance issued by the Commission

- the licensees' policies, procedures and controls for the purposes of forestalling, preventing and detecting money laundering and terrorist financing

- The identity and responsibilities of the MLRO

- The detection of unusual or suspicious transactions

- The principle vulnerabilities of the products and services offered by the licensee,

- New developments including information on current money laundering and terrorist financing techniques, methods, trends and typologies

  In addition relevant employees of Category 1 eGambling licensees must receive comprehensive ongoing training in CDD requirements (paragraph 8(2) of Schedule 16 to the Regulations – see Appendix 2).

Training must be provided to all new employees prior to their being actively involved in day to day operations. Thereafter the frequency of training should be determined in line with a risk based approach. Those employees with responsibility for the handling of customer relationships or transactions should receive more frequent training.

11.3 Relevant employees

The definition of relevant employees is set out in regulation 265 of the Regulations (see Appendix 2).

The definition is wide and relevant employees includes employees whose duties relate to eGambling. By way of illustration, relevant employees will include (this list is not exhaustive) –

- employees who organise or effect gambling transactions. Therefore those employees who have direct contact with customers or those handling or being responsible for the handling of customer relationships or financial or gambling transactions,
- employees supporting those employees that have direct contact with customers or those handling or being responsible for the handling of customer relationships or financial or gambling transactions,
- Relevant employees also include any member of the licensee's management or board of directors. It follows that the management and board of directors should receive comprehensive training in the areas identified in paragraph 11.2 above.

11.4 The MLRO

The MLRO, nominated officer and any deputies should receive training in:-

- The handling and reporting of internal suspicion reports;
- The handling and production of restraining orders;
- Liaising with law enforcement agencies; and
- The management of the risk of tipping off.

11.5 Bribery and corruption

Licensees should ensure that staff receive suitable training in respect of the risks of bribery and corruption. In addition there should be suitable processes and controls within the Internal Control System to mitigate against staff being involved in bribery and corruption, including through the manipulation of event based wagering or in respect of the activities of the corporate entity.

EMPLOYEE SCREENING AND TRAINING

Key Legislative Provisions

- Paragraph 8 of Schedule 16 to the Regulations (employee screening and training)

To summarise:

Employees must:

- be identified and verified
- be screened to ensure their probity including checking references and checks of criminal convictions.
- receive appropriate ongoing AML/CFT training

12. Bribery and corruption.

12.1 What is bribery and corruption?

Bribery and corruption are the terms used for when an entity or person makes a secret agreement with another person or entity to secure a favour of some description, usually to influence a transaction. The agreement could (and frequently does) involve a financial inducement. Frequently when people talk of bribery and corruption they consider public officials to be involved. Within the eGambling sector bribery and corruption can also take other forms particularly with regards to the manipulation of events[34] upon which wagering is taking place or in respect of the awarding of contracts for goods and services by employees of the eGambling licensee (see Chapter 11 which deals with staff risks).

eGambling licensees should ask themselves what risk they consider to be associated with:-

- the products and services that they offer or administer;
- the underlying purpose to which those products and/or services are put;
- their customers and their geographical origin; and
- their exposure to PEP's.

In addition eGambling licensees are expected to take the necessary steps to ensure that their monitoring assists them in mitigating the risks specified above having regard to:-

- any commission structures and whether these are reasonable, proportionate and transparent;
- political and charitable donations as well as sponsorships;
- instructions to effect payments for advisory and consulting activities with no apparent connection to the known activities of the business;

[34] The primary focus here is sports betting however any event upon which betting takes place and which can be influenced by external forces such as elections or televised "talent" shows.

- payments to unknown third parties;
- effecting transactions through cash payments and money orders; and
- transactions which do not appear to offer "best value" or good value for money.

12.2 Examples

12.2.1 Corrupt staff member (1)

A member of staff accepts an inducement from a supplier to place an IT contract. In this instance the eGambling licensee pays an excessive price to the supplier and the member of staff receives some form of financial or other inducement which the licensee is not aware of.

This results in the eGambling licensee spending more money than it otherwise would on goods and services and the employee receives an incentive from the suppliers.

12.2.2 Corrupt staff member (2)

A member of staff accepts an inducement to circumvent CDD processes. In this instance an employee with the ability to over-ride computer systems accepts an inducement to ensure that a person is not subjected to levels of CDD that would result in suspicions being aroused which ultimately enable the fraudster or launderer to effectively launder the proceeds of crime without arousing the suspicion of the licensee and triggering a STR.

12.2.3 Manipulated events

The licensee has concerns about an event upon which wagers are being taken as the values being staked do not correspond to what it would expect of such an event. The licensee has concerns that efforts are being made to manipulate the result of the event.

12.3 Action to be taken

Where there are concerns that relate to an attempt to manipulate an event upon which wagers are being taken a notification as prescribed in Regulations 4(n), 6(o), 8(k) and 60(l) of the Regulations must be made to the Commission.

In addition, in any case where an eGambling licensee, or an employee of a licensee, has concerns regarding bribery and corruption and/or event manipulation, it should consider whether a report should be made under the Disclosure Law or Terrorism Law.

13. UN and EU SANCTIONS

The Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011("Terrorist Law") implements the United Nations Security Council Resolution 1373 and Council Regulation (EC) No. 2580/2001.

The EU Regulation imposes restrictive measures directed against certain persons and entities (known as designated persons) with a view to combatting terrorism. In the Bailiwick, the Al-Qaida (Restrictive Measures) (Guernsey) Ordinance, 2013, the Al-Qaida Restrictive Measures) (Alderney) Ordinance, 2013 and the Al-Qaida (Restrictive Measures) (Sark) Ordinance, 2013 ("Al-Qaida Ordinance") implements the United Nations Security Council Resolution 1267 and Council Regulation (EC) No. 881/002 as amended by EU Regulation 754/2011. The EU regulation imposes restrictive measures directed against persons designated by the United Nations Sanctions Committee.

In the Bailiwick, the Afghanistan (Restrictive Measures) (Guernsey) Ordinance, 2011, the Afghanistan (Restrictive Measures) (Alderney) Ordinance, 2011 and the Afghanistan (Restrictive Measures) (Sark) Ordinance, 2011 ("Afghanistan Ordinance") implements the United Nations Security Council Resolutions 1988 (2011) and 1989 (2011) and Council Regulation (EC) No. 753/2011.

When determining whether a particular individual or entity is a designated person, licensees must consult the full list of financial sanctions targets which may be found in the HM Treasury website at https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets .

Licensees must ensure that they comply with the requirements under the Terrorist Law, Al-Qaida Ordinance, and the Afghanistan Ordinance which prohibit licensees from dealing with, or making available funds, financial services or economic resources, to designated persons.

MLROs and Nominated Officers from eGambling licensees should ensure that they are registered users of THEMIS, the online reporting portal used for reporting suspicious transactions as the Guernsey FIS will use this as a means of distribution for relevant information in relation to sanctions. In addition Notices and Instructions issued by the Commission in addition to BSSN's will be used to deliver information to eGambling licensees.

In addition useful information can be found at on the Guernsey government website at http://www.gov.gg/sanctions

14. FURTHER READING

The FATF 40 Recommendations:

http://www.fatf-gafi.org/topics/fatfrecommendations/documents/the40recommendationspublishedoctober2004.html

The FATF 9 Special Recommendations on Terrorist financing:

http://www.fatf-gafi.org/topics/fatfrecommendations/documents/ixspecialrecommendations.html

The FATF Guidance on the risk-based approach to combating money laundering and terrorist financing:

http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatfguidanceontherisk-basedapproachforcasinos.html

FATF Guidance in relation to the casino industry : Vulnerabilities of Casinos and Gaming Sector.

http://www.fatf-gafi.org/media/fatf/documents/reports/Vulnerabilities%20of%20Casinos%20and%20Gaming%20Sector.pdf

The FATF Guidance on money laundering and terrorist financing typologies

http://www.fatf-gafi.org/topics/methodsandtrends/documents/moneylaunderingandterroristfinancingtypologies2004-2005.html

The FATF report on money laundering through the football sector

http://www.fatf-gafi.org/topics/methodsandtrends/documents/moneylaunderingthroughthefootballsector.html

Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (Moneyval) research report into the use of online gambling for money laundering and the financing of terrorism purposes

http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL%282013%299_Onlinegambling.pdf

The Financial Crimes Enforcement Network SAR Activity review. Trends, Tips and Issues.

http://www.fincen.gov/news_room/rp/sar_tti.html

Good Practice Guidelines for the online gambling industry

http://www.rga.eu.com/data/files/rga_aml_guidance_2010.pdf

APPENDIX 1

DISCLOSURE FORM (Only to be used in the event that THEMIS is unavailable)

STRICTLY PRIVATE AND CONFIDENTIAL		
Your ref:	Our ref:	Date:

Guernsey FIS, Ozanne Hall, Mignot Plateau, Cornet Street, St Peter Port, Guernsey, GY1 1LF

Tel: + 44 (0)1481 714081 Fax: +44 (0)1481 710466 E-mail: director@guernseyfis.org

Legislation under which this disclosure is made (*please tick one of the following*):

Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 □

Disclosure (Bailiwick of Guernsey) Law, 2007 □

Subject's full name(s)			
Gender			
Date(s) of birth		Place(s) of birth	
Passport or ID number(s)			
Nationality(ies)			
Address(es)			
Telephone	Home:	Work:	Mobile:
Occupation/employer			
Associated company: *e.g. company registration number, date and place of incorporation, etc.*			
Account name			
Account/product number			

Date account/product opened	
Details of any intermediary	
Other relevant information: *e.g. additional details of identification and/or references taken, associated parties, addresses, telephone numbers, etc.*	

DISCLOSURE (CONTINUED)

Reasons for suspicion:

Current status of business relationship:

When submitting this report, please provide a covering letter which includes contact information and append any additional material that you may consider relevant and which may be of assistance to the recipient, e.g. bank statements, vouchers, international transfers, inter-account transfers, telegraphic transfers, details of associated accounts and products, etc.

APPENDIX 2 RELEVANT AML/CFT LEGISLATION

EXTRACTS FROM THE ALDERNEY EGAMBLING ORDINANCE, 2009 AND THE ALDERNEY EGAMBLING REGULATIONS, 2009 (AS AMENDED).

For ease of reference, this appendix contains extracts from the Alderney eGambling Ordinance, 2009 and the Alderney eGambling Regulations, 2009 referred to in this Guidance. These extracts are neither exhaustive not authoritative. eGambling licensees must familiarise themselves with the original legislation as enacted.

THE ALDERNEY EGAMBLING ORDINANCE, 2009.

Section 3A.

In this Ordinance and any Regulations made thereunder, "**licensing objectives**" means the objectives of-

(a) protecting and enhancing the reputation of Alderney as a well regulated eGambling centre,
(b) ensuring that eGambling is conducted honestly and fairly and in compliance with good governance,
(c) preventing eGambling from being a source of crime, being associated with crime or being used to support crime, including preventing the funding, management and operation of eGambling from being under criminal influence, and
(d) protecting the interests of young persons and other vulnerable persons from being harmed or exploited by eGambling.

Section 3B.

(1) Without prejudice to any existing functions assigned to the Commission by the Law, or by any Ordinance made thereunder (including any provisions under this Ordinance), the functions of the Commission in relation to eGambling include –

(a) taking such steps as the Commission considers necessary or expedient –
    (i) For the effective regulation, supervision and control of eGambling in Alderney and pursuant to the Alderney eGambling (Operations in Guernsey) Ordinance, 2006, in Guernsey,

(ii) in order to pursue the licensing objectives,

(iii) for maintaining confidence in, and the safety, soundness and integrity of Alderney's eGambling sector,

(b) the countering of financial crime and of the financing of terrorism in the eGambling sector; and for this paragraph "financial crime" includes any offences involving –

(i) fraud or dishonesty

(ii) misconduct in, or misuse of information relating to, a financial market,

(iii) handling the proceeds of crime

and "offence" includes an act or omission which would be an offence if it had taken place in Alderney.

Section 22(2)(e)

an eGambling licensee and a Category 2 associate certificate holder and, where appropriate, its associates are obliged to take steps to comply with applicable measures in respect of money laundering and terrorist financing, and such regulations shall include, without limitation, the duties and requirements to be complied with by such licensees, certificate holders and associates for the purposes of forestalling and preventing money laundering and terrorist financing.

Sections 22(3), 22(4) and 22(5)

(3) The Commission may –

(a) establish and maintain a website to support the performance of its functions under this Ordinance and regulations made thereunder; and

(b) make such notices, instructions, guidance or other similar instruments as it considers appropriate for the purposes of this Ordinance and regulations made thereunder, including, without limitation, such notices, instructions, guidance or other similar instruments for the purposes of providing information about compliance with the provisions of this Ordinance and regulations made thereunder.

(4) The Commission and any court shall take the notices, instructions, guidance and other similar instruments made under subsection (3) into account in determining whether any person has complied with this Ordinance and the regulations made thereunder.

(5) Paragraphs (a) and (b) of section 27(1) and section 27(2) (general provisions as to regulations) have effect in relation to notices, instructions, guidance and other similar instruments made by the Commission as if references in that section to regulations were references respectively to notices, instructions, guidance and other similar instruments.

THE ALDERNEY EGAMBLING REGULATIONS, 2009

Regulation 4

(b) in no circumstances may cash be accepted from a customer by, or on behalf of, the Category 1 eGambling licensee

(e) the Category 1 eGambling licensee must appoint a money laundering reporting officer in accordance with Schedule 16, who may, but need not be, the compliance officer

(l) the Category 1 eGambling licensee must have regard to, and meet the requirements of, any relevant guidance, notice, instruction and counter-measure issued by the Commission which is necessary or expedient for the regulation, good conduct and control of eGambling, including, without limitation, any such guidance, notice, instruction or counter-measure which relates to anti-money laundering and counter terrorist financing

(n) the Category 1 eGambling licensee must –

(i) take reasonable steps to identify any improper attempts to influence the outcome of any event upon which gambling may take place; and

(ii) where any such activity is identified –

(A) notify the Commission in writing with the details and consequences (if known) of the activity within 24 hours of identifying such activity; and

(B) co-operate with any investigation, regulatory process of legal proceedings arising from such activity

(o) the Category 1 eGambling licensee must at all times comply with the money laundering and terrorist financing provisions under Schedule 16 and the associated regulations to the extent that such provisions are therein stated to apply to the licensee

Regulation 6

(b) in no circumstances may cash be accepted from a customer by, or on behalf of, the Category 2 eGambling licensee

(e) the Category 2 eGambling licensee must appoint a money laundering reporting officer in accordance with Schedule 16, who may, but need not be, the compliance officer

(l) the Category 2 eGambling licensee must have regard to, and meet the requirements of, any relevant guidance, notice, instruction and counter-measure issued by the Commission which is necessary or expedient for the regulation, good conduct and control of eGambling, including, without limitation, any such guidance, notice, instruction or counter-measure which relates to anti-money laundering and counter terrorist financing

(m) the Category 2 eGambling licensee shall not effect gambling transactions on behalf of an operator who is not a category 1 eGambling licensee unless that operator –

(i) has been approved by the Commission as a business associate that is a fit and proper person to be associated with the Category 2 eGambling licensee in accordance with regulation 22; and

(ii) complies with all the requirements set out in paragraph 11(2) of Schedule 16

(o) the Category 2 eGambling licensee must –

(i) take reasonable steps to identify any improper attempts to influence the outcome of any event upon which gambling may take place; and

(ii) where any such activity is identified –

(A) notify the Commission in writing with the details and consequences (if known) of the activity within 24 hours of identifying such activity; and

(B) co-operate with any investigation, regulatory process of legal proceedings arising from such activity

(p) the Category 2 eGambling licensee must at all times comply with the money laundering and terrorist financing provisions under Schedule 16 and the associated regulations to the extent that such provisions are therein stated to apply to the licensee.

Regulation 8

(b) in no circumstances may cash be accepted from a customer by, or on behalf of, the Temporary eGambling licensee

(k) the Temporary eGambling licensee must –

(i) take reasonable steps to identify any improper attempts to influence the outcome of any event upon which gambling may take place; and

(ii) where any such activity is identified –

(A) notify the Commission in writing with the details and consequences (if known) of the activity within 24 hours of identifying such activity; and

(B) co-operate with any investigation, regulatory process of legal proceedings arising from such activity

(m) the Temporary eGambling licensee must appoint a money laundering reporting officer in accordance with Schedule 16, who may, but need not be, the compliance officer

(o) the Temporary eGambling licensee must have regard to, and meet the requirements of, any relevant guidance, notice, instruction and counter-measure issued by the Commission which is necessary or expedient for the regulation, good conduct and control of eGambling, including, without limitation, any such guidance, notice, instruction or counter-measure which relates to anti-money laundering and counter terrorist financing

(p) the Temporary eGambling licensee must at all times comply with the money laundering and terrorist financing provisions under Schedule 16 and the associated regulations to the extent that such provisions apply to a Temporary eGambling licensee

Regulation 60

(a) in no circumstances may cash be accepted from a customer by, or on behalf of, the Category 2 associate certificate holder

(d) the Category 2 associate certificate holder must appoint a money laundering reporting officer in accordance with Schedule 16, who may, but need not be, the compliance officer

(j) the Category 2 associate certificate holder must have regard to, and meet the requirements of, any relevant guidance, notice, instruction and counter-measure issued by the Commission which is necessary or expedient for the regulation, good conduct and control of eGambling, including, without limitation, any such guidance, notice, instruction or counter-measure which relates to anti-money laundering and counter terrorist financing

(l) the Category 2 associate certificate holder must –

(i) take reasonable steps to identify any improper attempts to influence the outcome of any event upon which gambling may take place; and

(ii) where any such activity is identified –

(A) notify the Commission in writing with the details and consequences (if known) of the activity within 24 hours of identifying such activity; and

(B) co-operate with any investigation, regulatory process of legal proceedings arising from such activity

(m) the Category 2 associate certificate holder must at all times comply with the money laundering and terrorist financing provisions under Schedule 16 and the associated regulations to the extent that such provisions are therein stated to apply to the certificate holder.

Regulation 175

(1) The purpose of an internal control system is —

(a) to provide a description by an eGambling licensee or a Category 2 associate certificate holder of the controls and administrative, operational and accounting policies and procedures to which it will adhere when conducting eGambling or operating under its licence or certificate; and

(b) to establish the standards and processes against which an ordinary investigation by the Commission in the form of an inspection in accordance with regulation 251 will be undertaken.

(2) As a minimum, an internal control system shall contain information about and describe having regard to its business risk assessment —

(a) accounting systems and procedures and chart of accounts;

(b) administrative systems and procedures;

(c) computer software;

(d) standard forms and terms;

(e) general procedures to be followed for the conduct of any form of eGambling;

(f) procedures and standards for the maintenance, security, storage and transportation of gambling equipment;

(g) procedures for registering, identifying and verifying customers (in relation to a Category 1 eGambling licensee only), recording gambling transactions and paying winnings to customers (in relation to a Category 1 eGambling licensee only);

(h) positions to be designated as key positions;

(i) its auditors; and

(j) the policies, procedures and controls as are appropriate and effective for the purposes of forestalling, preventing and detecting money laundering and terrorist financing, and necessary in order to comply with the money laundering and terrorist financing provisions under Schedule 16 and the associated regulations.

(3) Without prejudice to the generality of the foregoing, the policies, procedures and controls referred to in paragraph 2(j) shall include the eGambling licensee's or Category 2 associate certificate holder's –

(a) policy for reviewing at appropriate intervals its compliance with the money laundering and terrorist financing provisions;

(b) arrangements to manage compliance;

(c) screening practices when recruiting relevant employees;

(d) ongoing employee training programme;

(e) audit function to test its systems;

(f) measures taken to keep abreast of and guard against the use of technological developments and new methodologies in money laundering and terrorist financing schemes;

(g) customer identification and verification systems (in relation to a Category 1 eGambling licensee only); and

(h) procedures relating to ongoing customer due diligence and monitoring of the customer relationship (in relation to a Category 1 eGambling licensee only).

"THE ASSOCIATED REGULATIONS"

(means regulations 175(2)(j), 175(3), 226, 227, 228, 229, 230, 233 and any other provision in these Regulations associated with the money laundering and terrorist financing requirements under Schedule 16)

Regulation 175(2)(j), 175(3)(2) As a minimum, an internal control system shall contain information about and describe having regard to its business risk assessment —

(j) the policies, procedures and controls as are appropriate and effective for the purposes of forestalling, preventing and detecting money laundering and terrorist financing, and necessary in order to comply with the money laundering and terrorist financing provisions under Schedule 16 and the associated regulations.

(3) Without prejudice to the generality of the foregoing, the policies, procedures and controls referred to in paragraph 2(j) shall include the eGambling licensee's or Category 2 associate certificate holder's –

(a) policy for reviewing at appropriate intervals its compliance with the money laundering and terrorist financing provisions;

(b) arrangements to manage compliance;

(c) screening practices when recruiting relevant employees;

(d) ongoing employee training programme;

(e) audit function to test its systems;

(f) measures taken to keep abreast of and guard against the use of technological developments and new methodologies in money laundering and terrorist financing schemes;

(g) customer identification and verification systems (in relation to a Category 1 eGambling licensee only); and

(h) procedures relating to ongoing customer due diligence and monitoring of the customer relationship (in relation to a Category 1 eGambling licensee only).

Regulation 226

A Category 1 eGambling licensee shall not permit a person to effect a gambling transaction as part of its operations under its eGambling licence unless the person is a customer who has registered in accordance with regulation 227.

Regulation 227

(1) A customer shall register —

(a) directly with a Category 1 eGambling licensee; or

(b) with an associate of a Category 1 eGambling licensee,

by completing an application process as set out in the Category 1 eGambling licensee's approved internal control system.

(2) Prior to registering a customer, or as soon as reasonably practicable thereafter, a Category 1 eGambling licensee, or, when applicable, an associate on the licensee's behalf, shall undertake a risk assessment in respect of that person, in accordance with the terms of the Category 1 eGambling licensee's approved internal control system, to determine if –

(a) the Category 1 eGambling licensee's relationship with the customer is a high risk relationship; or

(b) the customer or any beneficial owner or underlying principal is a politically exposed person.

(3) A person shall not be eligible for registration as a customer in accordance with paragraph (1) unless he is able to produce to the person carrying out the registration process evidence of a type and in a manner set out in the Category 1 eGambling licensee's approved internal control system —

(a) of his identity and place of residence; and

(b) that he is at least 18 years of age.

(4) Subject to paragraph 4 of Schedule 16, the registration of a customer shall not be completed by the person carrying it out until —

(a) the identity of the person wishing to register as a customer has been authenticated;

(b) the person's place of residence has been verified;

(c) the customer has confirmed that he is acting as principal and is not restricted in his legal capacity;

(d) if the customer is not a natural person –

(i) the legal status and legal form of the customer has been verified; and

(ii) the names of the natural persons who have ultimate ownership and/or control of the customer have been determined; and

(e) the customer due diligence measures (as defined in Schedule 16) have been undertaken,

in accordance with the terms of the Category 1 eGambling licensee's approved internal control system and the money laundering and terrorist financing provisions set out in Schedule 16.

(5) Save in such circumstances as are set out in a Category 1 eGambling licensee's approved internal control system an employee of —

(a) a Category 1 eGambling licensee;

(b) the associate carrying out the registration process;

(c) any other associate directly involved in managing any aspect of the Category 1 eGambling licensee's gambling transactions, whether or not he is a key individual, shall not be registered as a customer.

Regulation 228

(1) A Category 1 eGambling licensee, or, when applicable, an associate on the licensee's behalf, shall not set up anonymous customer accounts or accounts in fictitious names.

(2) A Category 1 eGambling licensee, or, when applicable, an associate on the licensee's behalf, shall maintain customer accounts in a manner which facilitates the meeting of the requirements of this Chapter and Schedule 16.

Regulation 229

A Category 1 eGambling licensee, or, when applicable, an associate on the licensee's behalf, shall, in accordance with the terms of the Category 1 eGambling licensee's approved internal control system, regularly review any risk assessment carried out under regulation 227(2) so as to keep it up to date and, where changes to that risk assessment are required, it shall make those changes.

Regulation 230

(1) The funds with which a customer pays for gambling transactions with a Category 1 eGambling licensee may be deposited –

(a) directly with the Category 1 eGambling licensee, or

(b) with an associate of the Category 1 eGambling licensee,

in the manner set out in the Category 1 eGambling licensee's approved internal control system and in accordance with the money laundering and terrorist financing provisions set out in Schedule 16.

(2) For the purposes of paragraph (1), in no circumstances may cash be accepted as funds from a customer by, or on behalf of, the Category 1 eGambling licensee.

Regulation 233

(1) An eGambling licensee, a Category 2 associate certificate holder and, to the extent applicable, other associates shall comply with the money laundering and terrorist financing provisions set out in Schedule 16 to the extent that such provisions are therein stated to apply to such a licensee, certificate holder or associate.

(2) For the purposes of section 24(5) of the Ordinance –

(a) each requirement set out in Schedule 16, and

(b) each requirement under regulations 175(2)(j), 175(3), 226, 227, 228, 229 and 230, is specified as a "money laundering offence".

Regulation 265

"**appropriate resources**" means financial resources —

(a) adequate, in the Commission's opinion, to ensure the financial viability of operations conducted under an eGambling licence or Category 2 associate certificate; and

(b) available from a source that is not, in the Commission's opinion, tainted with illegality, including, for the avoidance of doubt, whether those resources may have been derived from money laundering or terrorist financing;

"**appropriate services**" means the services of persons who have appropriate experience to ensure the proper and successful conduct of eGambling and who have satisfied applicable screening processes relating to money laundering or terrorist financing on recruitment;

"**associated regulations**" means regulations 175(2)(j), 175(3), 226, 227, 228, 229, 230, 233 and any other provision in these Regulations associated with the money laundering and terrorist financing requirements under Schedule 16;

"beneficial owner" means, in relation to a customer relationship —

(a) the natural person who ultimately owns or controls the customer; and

(b) a person on whose behalf the customer relationship is to be or is being conducted and, in the case of a trust or other legal arrangement, this shall mean —

(i) any beneficiary in whom an interest has vested, and

(ii) any other person who appears likely to benefit from that trust or other legal arrangement;

"**business risk assessment**" means an assessment which documents the exposure of the business of an eGambling licensee or a Category 2 associate certificate holder to money laundering and terrorist financing risks, and vulnerabilities, including those that may arise from new or developing technologies that might favour anonymity, taking into account its —

(a) size, nature and complexity; and

(b) customers, products and services and the ways in which it provides those services;

"**customer relationship**" means a continuing relationship between a Category 1 eGambling licensee and a registered customer to enable the organisation and preparation of gambling transactions, and "**customer**" has a corresponding meaning;

"**employee**" means an individual working, including on a temporary basis, for an eGambling licensee or Category 2 associate certificate holder whether under a contract of employment, a contract for services or otherwise

"financial transaction" includes the purchase or cashing in of casinos chips or tokens or the opening of an account or any money or other value transfer or exchange

"**registered customer**" means a customer who has been registered in accordance with regulation 227

"**relevant employee**" includes any –

(a) member of the eGambling licensee's or Category 2 associate certificate holder's board of directors;

(b) member of the management of the eGambling licensee or Category 2 associate certificate holder; and

(c) employees whose duties relate eGambling,

whether or not they hold a key individual certificate or are directly employed by the eGambling licensee or Category 2 associate certificate holder;

"**risk**" means a risk of money laundering or terrorist financing occurring and "**risk assessment**" shall be construed accordingly

Schedule 16

SCHEDULE 16

MONEY LAUNDERING AND TERRORIST FINANCING PROVISIONS

Risk assessment

Business risk assessment.

1. 1. (1) An eGambling licensee or, as the case may be, a Category 2 associate certificate holder, shall carry out a suitable and sufficient business risk assessment before submitting its application for approval of its internal control system in accordance with regulation 176.

(2) An eGambling licensee or, as the case may be, a Category 2 associate certificate holder, shall regularly review its business risk assessment so as to keep it up to date and where, as a result of that review, any change to the business risk assessment is required, it shall seek approval to make any corresponding change to its approved internal control system in accordance with regulations 191 and 192.

Customer due diligence, etc.

Customer due diligence.

2. A Category 1 eGambling licensee shall undertake customer due diligence measures —

(a) subject to paragraph 4, before registering a customer in accordance with regulation 227;

(b) immediately after a registered customer, in accordance with regulation 230, makes a deposit —

(i) of €3,000 or more, or

(ii) that results in the total value of his deposits in the course of any period of 24 hours reaching or exceeding €3,000;

(c) when it knows or suspects or has reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing; or

(d) when it doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification of a registered customer.

Additional customer due diligence.

3. (1) Where a Category 1 eGambling licensee is required to carry out customer due diligence in accordance with paragraph 2, it shall also carry out enhanced customer due diligence in relation to the following customer relationships —

(a) a relationship in which the customer or any beneficial owner or underlying principal is a politically exposed person;

(b) a relationship where the customer is established or situated in a country or territory that does not apply or insufficiently applies the FATF Recommendations;

(c) a relationship which has been assessed as a high risk relationship pursuant to regulation 227(2) or 229, and

(d) a relationship which the Category 1 eGambling licensee considers to be a high risk relationship, taking into account any notices or warnings issued from time to time by the Commission pursuant to regulation 4(l).

(2) Where a customer relationship falls within sub-paragraph (1)(a), a Category 1 eGambling licensee shall —

(a) ensure that senior management approval is obtained for registering the customer,

or, in the case of an existing registered customer, continuing that relationship;

(b) take reasonable measures to establish the source of any funds and of the wealth of the customer and beneficial owner and underlying principal.

(3) Where the customer was not physically present when an activity set out in paragraph 2(a) or (b) takes place, the Category 1 eGambling licensee shall take adequate measures on a risk-sensitive basis to compensate for the specific risk arising as a result —

(a) when carrying out customer due diligence measures; and

(b) when carrying out monitoring of that relationship pursuant to paragraph 6.

Timing of identification and verification.

4. Verification of the identity of the customer and of any beneficial owner and underlying principal may be completed following the registration of the customer provided that —

(a) it is completed as soon as reasonably practicable thereafter;

(b) the need to do so is essential not to interrupt the normal conduct of the Category 1 eGambling licensee's business; and

(c) appropriate and effective policies, procedures and controls are set out in the Category 1 eGambling licensee's approved internal control system so as to manage money laundering and terrorist financing risks.

Non-compliance with customer due diligence measures, etc.

5. Where a Category 1 eGambling licensee is unable to comply with paragraph 2 and, where applicable, paragraph 3, it shall —

(a) in the case of a person wishing to become a registered customer, not register that person as a customer;

(b) in the case of an existing registered customer, terminate that customer relationship; and

(c) consider whether making a disclosure is required pursuant to Part I of the Disclosure Law or section 12 of the Terrorism Law.

Customer Identification and Verification Systems.

5A. The Category 1 eGambling licensee's customer identification and verification systems

shall –

(a) incorporate robust and effective client identification methods and measures in order to adequately manage and mitigate the specific risks of non face-to-face customer relationships or transactions inherent in the eGambling industry;

(b) supplement identification verification software with additional forms of customer due diligence and identity verification procedures in circumstances which are appropriate and effective for the purposes of managing and mitigating the risks referred to in item (a) and forestalling, preventing and detecting money laundering and terrorist financing, including, without limitation, where a Category 1 eGambling licensee is required to carry out enhanced customer due diligence under this Schedule; and

(c) refer only to identification verification software and additional or alternative identification methods that have been approved by the Commission.".

Ensuring compliance and record keeping

Monitoring transactions and other activity.

6. (1) A Category 1 eGambling licensee shall perform ongoing and effective monitoring of any existing customer relationship, which shall include —

(a) reviewing identification data to ensure they are kept up to date and relevant in particular for registered customers in respect of whom there is a high risk;

(b) ensuring that the way in which identification data are recorded and stored is such as to facilitate the ongoing monitoring of each customer relationship; and

(c) without prejudice to the Category 1 eGambling licensee's obligations under regulation 236, scrutiny of any transactions or other activity (including, where necessary, the source of funds) to ensure that the transactions are consistent with the Category 1 eGambling licensee's knowledge of the registered customer and his risk profile, paying particular attention to all —

(i) complex transactions,

(ii) transactions which are both large and unusual,

(iii) unusual patterns of transactions, and

(iv) transactions arising from a country or territory that does not apply or insufficiently applies the FATF recommendations

which have no apparent economic purpose or no apparent lawful purpose and recording its findings thereon in writing.

(1A) A Category 2 eGambling licensee or, as the case may be, a Category 2 associate certificate holder shall perform ongoing and effective monitoring of all gambling transactions, paying particular attention to all –

(a) complex transactions

(b) transactions which are both large and unusual, and

(c) unusual patterns of transactions,

which have no apparent economic purpose or no apparent lawful purpose and recording its findings thereon in writing.

(2) A Category 1 eGambling licensee, a Category 2 eGambling licensee and a Category 2 associate certificate holder shall examine as far as reasonably possible, the background and purpose of the transactions described in sub-paragraphs 1(c) and (1A) and shall set forth its findings in writing.

(3) The extent of any monitoring carried out under sub-paragraph (1) and the frequency at which it is carried out shall be determined on a risk-sensitive basis including whether or not the customer relationship is a high risk relationship.

(4) Where a Category 2 eGambling licensee or Category 2 associate certificate holder sets out its findings in writing in accordance with sub-paragraphs (1A) and (2) it shall as soon as reasonably practicable communicate such findings to the MLRO of the Category 1 eGambling licensee who had allowed its customer to gamble with or through it in order to effect a gambling transaction

Reporting suspicion.

7. (1) A Category 1 eGambling licensee, a Category 2 eGambling licensee, a Category 2

associate certificate holder and a Temporary eGambling licensee (in respect of the activities under its Temporary eGambling licence) shall —

(a) appoint an executive officer as the money laundering reporting officer ("**MLRO**") and provide the name and title of that officer to the Commission and the Financial Intelligence Service as soon as is reasonably practicable and, in any event, within fourteen days starting from the date of that person's appointment;

(b) nominate another person (a **"nominated officer"**) to carry out the functions of the MLRO in his absence and ensure that any relevant employee is aware of the name of that nominated officer;

(c) ensure that where a relevant employee, other than the MLRO, is required to make a disclosure under Part I of the Disclosure Law or section 12 of the Terrorism Law, that this is done by way of a report to the MLRO, or, in his absence, to a nominated officer;

(d) ensure that the MLRO, or, in his absence, a nominated officer, in determining whether or not he is required to make a disclosure under Part I of the Disclosure Law or section 12 of the Terrorism Law, takes into account all relevant information;

(e) ensure that the MLRO, or, in his absence, a nominated officer, is given prompt access to any other information which may be of assistance to him in considering any report; and

(f) ensure that it establishes and maintains such other appropriate and effective procedures and controls as are necessary to ensure compliance with requirements to make disclosures under Part I of the Disclosure Law and section 12 of the Terrorism Law.

(2) Where a Category 1 eGambling licensee, a Category 2 eGambling licensee, a Category 2 associate certificate holder and a Temporary eGambling licensee (in respect of the activities under its Temporary eGambling licence) makes a disclosure under Part I of the Disclosure Law or section 12 of the Terrorism Law, a copy of that disclosure shall be provided to the Commission at the same time or as soon as practicable thereafter

Employee screening and training.

8. (1) A Category 1 eGambling licensee, a Category 2 eGambling licensee, a Category 2

associate certificate holder and a Temporary eGambling licensee (in respect of the activities under its Temporary eGambling licence) shall –

(a) maintain appropriate and effective procedures, when hiring employees, for the purpose of ensuring high standards of employee probity and competence;

(b) ensure that relevant employees receive comprehensive ongoing training in —

(i) the relevant enactments, the Law, the Ordinance and these Regulations;

(ii) the personal obligations of employees and their potential criminal liability under the relevant enactments and the Ordinance;

(iii) the implications of non-compliance by employees with any guidance issued by the Commission in accordance with section 22(3)(b) of the Ordinance;

(iv) its policies, procedures and controls for the purposes of forestalling, preventing and detecting money laundering and terrorist financing;

(v) the identity and responsibilities of the MLRO;

(vi) the detection of unusual or suspicious transactions;

(vii) the principal vulnerabilities of the products and services offered by the eGambling licensee or the associate certificate holder;

(viii) new developments including information on current money laundering and terrorist financing techniques, methods, trends and typologies; and

(c) identify relevant employees who, in view of their particular responsibilities, should receive additional and ongoing training, appropriate to their roles, in the matters set out in item (b) and shall provide such training.

(2)A Category 1 eGambling licensee shall ensure that relevant employees receive comprehensive ongoing training in customer due diligence requirements.

Record-keeping.

9. (1) A Category 1 eGambling licensee, a Category 2 eGambling licensee, a Category 2 associate certificate holder and a Temporary eGambling licensee (in respect of the activities under its Temporary eGambling licence) shall keep such of the following as is appropriate to their licence or certificate —

(a) a transaction document or a copy thereof for five years starting from the date that

both the transaction and any related transaction were completed; and

(b) any customer due diligence information or a copy thereof for five years starting from the date the person concerned ceased to be a registered customer,

or, in either case, for such other longer period as the Commission, the Financial Intelligence Service, or an officer of police may direct.

(2) Where an eGambling licensee or an associate certificate holder is required by any enactment, rule of law or court order to provide a transaction document or any customer due diligence information to any person before the end of the period set out in sub-paragraph (1), the licensee or certificate holder shall —

(a) keep a copy of the transaction document or customer due diligence information until the period has ended or the original is returned, whichever occurs first; and

(b) maintain a register of transaction documents and customer due diligence information so provided.

(3) An eGambling licensee and an associate certificate holder shall (if applicable) also keep records of —

(a) any findings made under paragraphs 6(1)(c) and 6(1A) and/or 6(2) for five years from the date the record was created;

(b) any reports made to its MLRO as referred to in paragraph 7 and of any disclosure made under Part I of the Disclosure Law or section 12 of the Terrorism Law made other than by way of a report to the MLRO for five years starting from the date the person concerned ceased to be a registered customer;

(c) any training carried out under paragraph 8 for five years starting from the date the training was carried out;

(d) any minutes or other documents prepared pursuant to paragraphs 1(2) and 9A(1)(e) until

(i) the expiry of five years starting from the date that they were finalised, or

(ii) they are superseded by later minutes or other documents prepared under those provisions,

whichever occurs later; and

(e) its policies, procedures and controls which it is required to establish and maintain pursuant to these Regulations, including previous iterations of the relevant

sections of its approved internal control system, for five years starting from the date that they ceased to be operative.

(4) Documents and customer due diligence information, including any copies thereof, kept under this paragraph —

(a) may be kept in any manner or form, provided that they are readily retrievable; and

(b) shall be made available on a timely basis –

(i) in respect of customer due diligence information, transaction documents and records relating to sub-paragraphs (3)(a), (3)(c), (3)(d) and (3)(e), -

(A) to any auditor, and

(B) to the Financial Intelligence Service, an officer of police, the Commission, the MLRO, nominated officer or any other person where such documents or customer due diligence information are requested pursuant to these Regulations or any relevant enactment, and

(ii) in respect of records relating to sub-paragraph (3)(b), to the Financial Intelligence Service, a prescribed police officer, the Commission, the MLRO or the nominated officer.

Ensuring compliance, corporate responsibility and related requirements.

9A. (1) An eGambling licensee or Category 2 associate certificate holder must, in addition to complying with the preceding requirements in this Schedule,

(a) establish and maintain such other internal policies, procedures and controls as are appropriate and effective for the purposes of forestalling, preventing and detecting money laundering and terrorist financing;

(b) take appropriate measures to keep abreast of and guard against the use of technological developments and new methodologies in money laundering and

terrorist financing schemes;

(c) establish and maintain policies and procedures to address any specific risks associated with non face to face customer relationships or transactions, in particular before registering a customer in accordance with regulation 227, and when performing its ongoing monitoring of any customer relationship in accordance with paragraph 6;

(d) establish and maintain an effective policy, for which responsibility must be taken by the board of directors, for the review of its compliance with the requirements of this Schedule and the associated regulations, and such policy shall include –

(i) provision as to the extent and frequency of such reviews; and

(ii) the requirement to maintain an adequately resourced and independent audit function to test compliance with such requirements;

(e) ensure that a review of its compliance with this Schedule and the associated regulations is discussed and minuted at a meeting of its board of directors at appropriate intervals, and in considering what is an appropriate interval, the eGambling licensee or Category 2 associate certificate holder shall have regard to the risk taking into account —

(i) the size, nature and complexity of the eGambling it conducts;

(ii) its registered customers (in relation to a Category 1 eGambling licensee only), products and services; and

(iii) the ways in which it provides those products and services; and

(f) must have regard to, and meet the requirements of any relevant guidance, notice, instruction and counter-measure issued by the Commission which relates to anti-money laundering and counter terrorist financing, including, without limitation, any such guidance, notice, instruction or counter-measure (whether described as "Business from Sensitive Sources Notices" or otherwise) designed to alert and advise it of weaknesses in the anti-money laundering and counter terrorist financing systems in other countries or territories where the eGambling licensee or Category 2 associate certificate holder may operate.

Miscellaneous

Interpretation.

10. (1) In this Part, unless the context otherwise requires —

"customer due diligence information" means —

(a) identification data, and

(b) any other files and correspondence relating to the customer relationship;

"customer due diligence measures" means —

(a) identifying the customer and verifying the customer's identity on the basis of identification data,

(b) identifying, where there is a beneficial owner or underlying principal who is not the customer, the beneficial owner or underlying principal and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the Category 1 eGambling licensee is satisfied that it knows who the beneficial owner or underlying principal is, including, in the case of a legal person, trust or other legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement,

(c) identifying any person purporting to act on behalf of a customer and verifying that identity on the basis of identification data and the authority of the person so acting, and

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

"**Disclosure Law**" means the Disclosure (Bailiwick of Guernsey) Law, 2007[35];

"document" includes information recorded in any form (including, without limitation, in electronic form);

"enactment" includes a Law, an Ordinance or any subordinate legislation and any provision or portion of a Law, an Ordinance or any subordinate legislation and, for the purposes of this definition, **"subordinate legislation"** means any statutory instrument, regulation, rule, order, notice, rule of court, resolution, scheme, warrant, byelaw or other instrument made under any enactment and having legislative effect;

"enhanced customer due diligence" means steps in relation to identification and verification in addition to customer due diligence measures, including taking the following steps —

(a) obtaining senior management approval for establishing a customer relationship,

(b) obtaining senior management approval for, in the case of an existing customer relationship with a politically exposed person, continuing that relationship,

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

(d) carrying out more frequent and more extensive ongoing monitoring in accordance with paragraph 6, and

(e) taking one or more of the following steps as would be appropriate to the particular customer relationship –

(i) obtaining additional identification data,

(ii) verifying additional aspects of the customer's identity, and

(iii) obtaining additional information to understand the purpose and intended nature of each customer relationship;

"FATF Recommendations" means the Financial Action Task Force Recommendations on Money Laundering and the Financial Action Task Force Special Recommendations on Terrorist Financing as revised or reissued from

[35] Order in Council No. XVI of 2007; Ordinance XXXIX of 2008.

time to time;

"Financial Intelligence Service" means the division of the Financial Investigation Unit, comprising those officers of police and other persons assigned to the division for the purpose of the receipt, analysis and dissemination within the Bailiwick of Guernsey, and elsewhere, of disclosures under Part I of the Disclosure Law or Section 12 of the Terrorism Law, which are more commonly known or referred to as suspicious transaction reports or suspicious activity reports,

"Financial Investigation Unit" means that branch of the Customs and Immigration Service responsible for the investigation of financial and economic crime,

"high risk relationship" means a customer relationship which has a high risk of involving money laundering or terrorist financing and related terms shall be construed accordingly;

"identification data" means documents, data or information relating to identification which are from a reliable and independent source;

"legal arrangement" means an express trust or any other vehicle whatsoever which has a similar legal effect;

"MLRO" shall be construed in accordance with paragraph 7(1)(a);

"nominated officer" shall be construed in accordance with paragraph 7(1)(b);

"**politically exposed person**" means —

(a) a person who has, or has had at any time, a prominent public function or who has been elected or appointed to such a function in a country or territory other than the Bailiwick of Guernsey including, without limitation —

(i) heads of state or heads of government,

(ii) senior politicians and other important officials of political parties,

(iii) senior government officials,

(iv) senior members of the judiciary,

(v) senior military officers, and

(vi) senior executives of state owned body corporates,

(b) an immediate family member of such a person including, without limitation, a spouse, partner, child, sibling, parent-in-law or grandchild of

such a person and, for the purposes of this definition, **"partner"** means a person who is considered by the law of the country or territory in which the relevant public function is held as being equivalent to a spouse, or

(c) a close associate of such a person, including, without limitation —

(i) a person who is widely known to maintain a close business or professional relationship with such a person, or

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

"prescribed police officer" means an officer of police who is a member of the Financial Intelligence Service,

"**subsidiary**" has the meaning given to it by paragraph 1 of Schedule 4 of the Companies (Alderney) Law, 1994[36], as amended;

"**relevant enactments**" means —

(a) [deleted]

(b) the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999,

(c) the Drug Trafficking (Bailiwick of Guernsey) Law, 2000,

(d) the Terrorism (United Nations Measures) (Channel Islands) Order 2001[37],

(e) the Al-Qaida and Taliban (United Nations Measures) (Channel Islands) Order 2002[38],

(f) the Terrorism Law,

(g) the Disclosure Law,

(h) the Transfer of Funds (Alderney) Ordinance, 2007[39],

and such enactments relating to money laundering and terrorist financing as may be enacted from time to time in, or in respect of, the Island of Alderney;

"transaction document" means a document which is a record of a transaction carried out by an eGambling licensee or Category 2 associate certificate holder with a

registered customer and which, as a minimum, identifies the customer(in the case of a Category 1 eGambling licensee only), the nature and date of the transaction and the type and amount of the currency involved and the identifying number of any account involved in the transaction;

"underlying principal" means, in relation to a customer relationship, any person who is not a beneficial owner but who —

(a) is a settlor, trustee or protector of a trust which is the customer or the beneficiaries of which are the beneficial owners, or

(b) exercises ultimate effective control over the customer or exercises or is to exercise such control over the customer relationship,

and, for the purposes of this definition, **"protector"** means a person other than a trustee who, as the holder of an office created by the terms of the trust, is authorised or required to participate in the administration of the trust.

(2) A reference to an enactment is to that enactment as from time to time amended, repealed and replaced, extended or applied by or under any other enactment.

Application to associates, foreign branches and subsidiaries.

11. (1) A reference to an eGambling licensee or a Category 2 associate certificate holder in this Schedule shall include a reference to the following –

(a) an associate which an eGambling licensee or a Category 2 associate certificate holder has arranged to perform on its behalf any activity required to be carried out in accordance with this Schedule;

(b) any other associate which the Commission requires by written notice to comply with this Schedule;

(c) branches and subsidiaries of the eGambling licensee or Category 2 associate certificate holder dealing with eGambling which are situated in a foreign country or territory, to the extent that the laws of that foreign country or territory allow; and

(d) a business associate which contracts with a Category 2 eGambling licensee in an arrangement whereby the Category 2 eGambling licensee effects gambling transactions on behalf of that business associate.

(2) Subject to sub-paragraph (3) an eGambling licensee or a Category 2 associate certificate holder shall ensure that an associate, foreign branch or subsidiary in a

country or territory outside the Island of Alderney to which sub-paragraph (1) applies complies with —

(a) the applicable requirements of this Schedule, regulations 4(d), 4(f), 6(d), 6(f), 8(d), 8(l), 60(c), 60(e) and the associated regulations; and

(b) the requirements under the law in that country or territory which are consistent with the FATF Recommendations,

provided that, where requirements under items (a) and (b) differ, the licensee or certificate holder must ensure that the requirement which provides the highest standard of compliance, by reference to the FATF Recommendations is complied with.

(3) The obligation under sub-paragraph (2) applies to the extent that the law of the relevant country or territory allows and if the law of that country or territory does not so allow in relation to any requirement of these Regulations, the licensee or certificate holder shall notify the Commission accordingly.