



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 Regulations, 2009 came into force on 1st January, 2010 and replaced the Alderney eGambling Regulations, 2006 (as amended). The 2009 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 Alderney eGambling Regulations, 2009 and should therefore be read in conjunction with those regulations. The Regulations and the Alderney eGambling Ordinance, 2009 set out the legal framework and requirements applicable to licensees and players.

In addition, licensees should refer to the published AGCC guidelines when preparing their Internal Control System. 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 during the course of every on-site inspection undertaken by the Commission.

1. INTRODUCTION

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 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. It is no longer acceptable to turn a blind eye and hope for the best.

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.

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 System¹ 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 Alderney eGambling Regulations, 2009. Part of the ICS must address the procedures and processes a licensee² will adopt in relation to the area of anti-money laundering and countering the financing of terrorism.³ The Commission maintains that the fight

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 Note that references to licensees means Category 1 eGambling licensees, Category 2 eGambling licensees and Foreign Gambling Associate Certificate holders.

³ When preparing the section of the ICS that relates to AML and CFT, a Licensee must conform to Regulations 175(3) and (4) and 233, and Schedule 16 of the Alderney eGambling Regulations, 2009 as amended.

against money laundering and countering the financing of terrorism (collectively known for the purposes of this guidance as AML) 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. The Commission also requests that customers appreciate that these checks and controls have been introduced for good reasons even if they may, on the face of matters, appear to seem burdensome.

Unfortunately a “tick box” approach in this area is no longer 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

In certain spheres of business activity, there are generally perceived to be three levels of risk, ranging from low/non-existent 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.

For standard risk customer due diligence measures are required and for higher risk transactions 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 people who might be using criminal funds.

Under the Alderney eGambling Ordinance, 2009 it is a criminal offence for a person to fail to comply with any regulations regarding anti money laundering. This guidance

has therefore been written to assist those involved in ensuring compliance with the relevant regulations. 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 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 employees⁴ 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 eGambling Regulations) There will be few employees 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 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

⁴ As defined in Regulation 265 of the Alderney eGambling Regulations, 2009 and includes any member of the licensee’s board of directors, member of the management of the licensee; and employees whose duties relate to the organising or effecting of gambling transactions, including arranging payments in respect of such transactions, or collecting customer due diligence, whether or not they hold a key individual certificate

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.

1.8 Who is needed?

All licensees are required to have a money laundering reporting officer (MLRO) and a nominated officer (as defined in Section 7(1)(b) of Schedule 16 of the 2009 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.

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.

2. 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 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.

2.1.2 Business Risk Assessment

The business risk assessment must be undertaken prior to the submission of the ICS.⁶ eGambling Licensees are in the best position to identify those areas of their operations that present the greatest risks 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 Regulation 175(3) of the Alderney eGambling Regulations, 2009.⁷

⁶ A defined term – Regulation 265(1). This specifically defines Business Risk Assessment as being an assessment which documents the exposure of the business of an eGambling licensee to money laundering and terrorist financing risks, and vulnerabilities, including those which may arise from new or developing technologies that might favour anonymity taking into account its (a) size nature and complexity; and (b) customers and services and the ways in which it provides those services.

⁷ 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. 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.

2.1.3 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%20Version%203_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

2.2.1. Risks

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 may 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. 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, requiring minimal, if any, AML/CFT risk mitigation beyond those applied at the customer level.

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 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.

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. 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 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”) procedures in countries where there are fewer appropriate resources such as credit reference agencies or creditable databases, 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/content.asp?pageID=211>

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 Alderney eGambling Regulations, 2009. 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 Alderney eGambling Regulations, 2009.

2.2.3 Controls to mitigate risks

Each licensee needs to consider the design and implementation of controls 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. A fully automated system is probably unlikely to provide the necessary analysis, and in any event, 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:-⁸

- 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.
- 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.

⁸ 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).

Category 2 eGambling licensees 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 customer as required by paragraph 6(4) of Schedule 16 of the Alderney eGambling Regulations, 2009.

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.

2.2.4 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 Alderney eGambling Regulations, 2009 and are further discussed in section 9 of this Guidance.

2.2.5 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, as well as some of the relevant UK specific 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.⁹

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>

In addition information can be found on the website of the Guernsey Financial Services Commission at <http://www.gfsc.gg/content.asp?pageID=639>

There is no set form 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. There is a requirement that the ICS is generally kept under regular review. The review period has to take

⁹. The ICS must deal with how Category 1 eGambling licensees would assimilate and process information received from a Category 2 eGambling licensee/foreign gambling associate certificate and outline the steps it would take to comply with its obligations under the Disclosure Law and the Terrorism Law.

into account the size, nature and 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 now also required to have an independent audit function to test its compliance with these requirements. The audit function must be adequately resourced and independent. 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. 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. 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 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.¹⁰

¹⁰ 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.

To summarise:

Licensees must (according to their category of eGambling licence or certificate)¹¹ assess the risks posed by:

- the industry (all)
- customers (1)
- products and services (all)
- payment methods (1)
- location (all)
- employees (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 (1)
- transactions arising from a country which does not apply or insufficiently applies FATF recommendations. (all)

Licensees must monitor:

- the information they hold (1)
- 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)

¹¹ References in parenthesis refer to category of licence or certificate.

3. RESPONSIBILITIES

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. However this risk can be minimised by undertaking proper and considered risk assessments and ensuring that any decisions taken are properly and accurately recorded. Whilst the consequences of failure could be high, licensees and those who work for them can reduce their personal risks by a careful and considered approach to the regulations. If there is a proper consideration of the risks, together with a consideration of the way in which they can be mitigated, with discussions and decisions being properly recorded and established procedures actually being followed then there is little for those involved to fear.

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.

To summarise:

Senior management should

- be involved in the decision making processes
- record the decisions made
- implement the procedures appropriately
- appropriately trained.

4. CUSTOMER DUE DILIGENCE

4.1 Introduction

It is necessary for a Category 1 eGambling licensee to undertake customer due diligence in order to identify and verify every customer prior to allowing eGambling to commence. Transactions involving customers who are not fully identified and verified can pose certain 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 it 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 Schedule 16 of the Alderney eGambling Regulations, 2009.¹²

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 changes of the business and the sector being a vehicle for or victim of financial crime or terrorist financing.

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

¹² The ICS must detail the procedures that will be carried out to comply with these requirements.

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.¹³

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 and;
- (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

¹³ 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. 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.

higher risk situations (where enhanced CDD would be required). 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. 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.

Category 1 eGambling licensees must identify in their internal control system what forms of identification and verification will be considered to be acceptable. 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 could include a requirement that additional documents are provided.

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 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 as well as verifying the legal status of the legal body. 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;
- 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

It is a regulatory requirement that a Category 1 eGambling licensee's identification and verification systems incorporate robust methods and measures in order to manage and mitigate the risks posed by the fact that eGambling transactions are not conducted face-to-face. There can be no occasional transactions in the eGambling industry.

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 Regulation 175(5) requires that Category 1 eGambling licensees have these methods and sources approved by the Commission.

4.2.6 Other Customer Due Diligence Measures

Where someone is not acting as a principal the person acting on behalf of the customer must be identified, his identity verified and in addition his authority to act in such a capacity must be verified.

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 (see section 6).

In addition there is a requirement that information shall be obtained on the purpose and intended nature of the business relationship.

4.2.7 Timing of Identification and Verification

These processes must be undertaken prior to commencing the relationship with the customer. However 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 Alderney eGambling Regulations, 2009.

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 Schedule 16 of the Alderney eGambling Regulations, 2009 they must, if there is already a business relationship, terminate that relationship and where there is no existing business relationship, not enter into the proposed business or 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 licences 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.

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.¹⁴

To summarise:

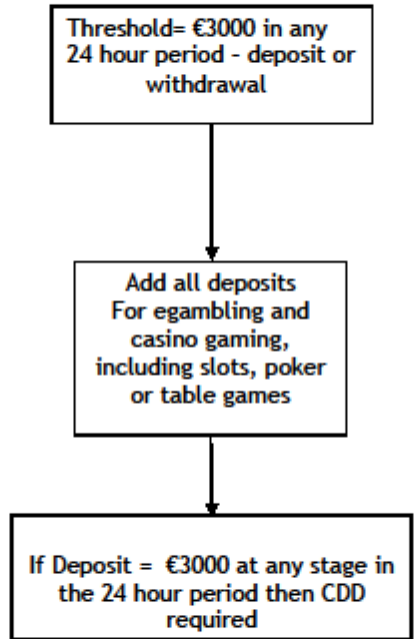
CDD must be performed by a Category 1 eGambling licensee

- 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.

¹⁴ The ICS must define when CDD will be carried out and where applicable explain the frequency with which this information is updated.

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. Additional 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 may also be 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 in a country or territory which does not apply, or insufficiently applies, 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.¹⁵ 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.

Where a Category 1 eGambling licensee undertakes CDD it must undertake enhanced CDD in relation to business relationships where:-

¹⁵ When enhanced customer due diligence measures are called for 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

- 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 Alderney eGambling Ordinance, 2009;or
- The customer or any beneficial owner or underlying principal is a politically exposed person.

Enhanced CDD 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 business 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 client's source of funds and source of wealth – particularly in relationships with PEPs.

To summarise Category 1 eGambling licensees must note that:

Enhanced customer due diligence is necessary for:

- high risk customers
- 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 Alderney eGambling Regulations, 2009 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. 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.

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.¹⁶ This area does pose a significant risk for operators. There is a real risk of PEPs registering and playing

¹⁶ 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.¹⁷ 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.¹⁸

¹⁷ 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.

¹⁸ 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.

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.¹⁹ 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.

To summarise:

The Category 1 eGambling licensee must:

- explain the processes to be followed when CDD or enhanced CDD fails
- consider its disclosure obligations in such cases

¹⁹ 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.

8. MONITORING TRANSACTIONS

8.1 Objective

Category 1 eGambling licensees are required to monitor the relationships they have with their customers. Category 2 eGambling licensees and foreign gambling 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.²⁰

The monitoring requirements for licensees can be found in paragraph 6 of Schedule 16 of the Alderney eGambling Regulations, 2009.

²⁰ 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?

The Licensee is free to determine the frequency of the monitoring it carries out. The ICS should explain the frequency of this on a risk sensitive basis regardless of whether or not the customer relationship has been assessed as high risk (in relation to a Category 1 licensee only).

8.2 Obligation to Monitor

Category 1 eGambling licensees

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;
- (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.

Category 2 eGambling licencees

Category 2 eGambling licensees and foreign gambling 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.

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.

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 or jurisdictions that do not or insufficiently apply the FATF Recommendations.

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.

The Category 2 eGambling licensee or foreign gambling 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.

eGambling licensees must examine the background and purpose of complex, unusual and large transactions as well as unusual patterns of transactions and must record such findings in writing. Where a Category 2 eGambling licensee or foreign gambling 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 recognise potential money laundering and terrorist financing 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 foreign gambling associate certificate holders there needs to be monitoring of gambling transactions, in particular those that are -

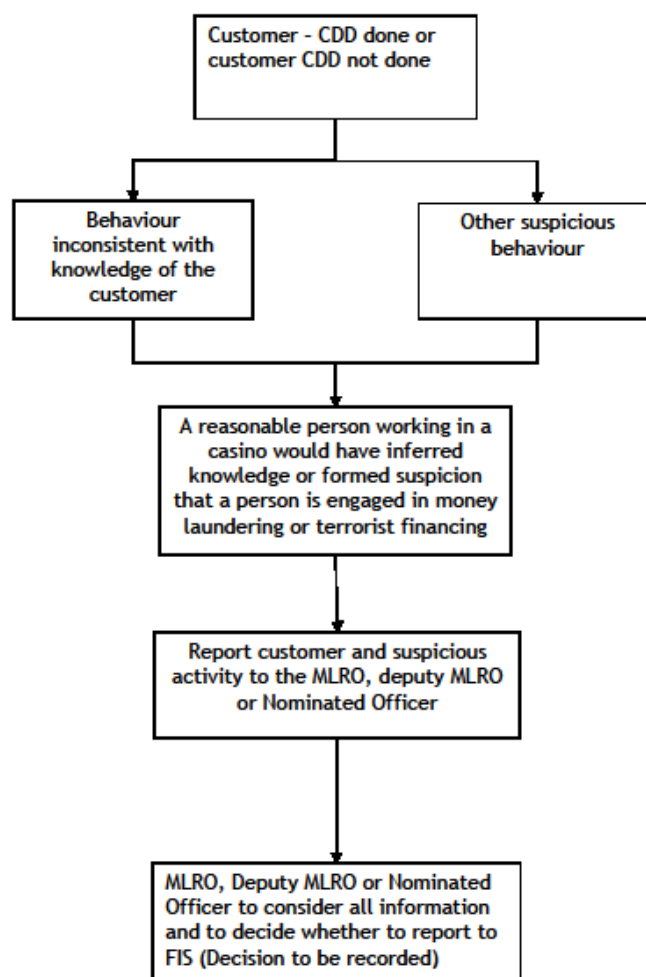
- complex
- large and unusual
- part of an unusual pattern

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

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

This table below sets out a flowchart for the objective test to be used by a Category 1 eGambling licensee.

Reasonable grounds to suspect (the objective test)



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 foreign gambling 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.

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 foreign gambling 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,**
- **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 **Regulation 188,**
- **policies, procedures and controls** that are required pursuant to the Alderney eGambling Regulations, 2009.

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.²¹

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. Customer due diligence information, or copies thereof, must also be kept for a minimum of 5 years 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.²²

The licensee should note that the Commission can direct that records be kept for a period greater than 5 years.²³ The production of these could be required as a result of

²¹ The ICS must address the procedure that will be used to ensure this.

²² The ICS should set out how these will be kept, the security arrangements that will apply and processes for retrieval.

²³ 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.

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.²⁴

Where a Category 2 eGambling licensee or foreign gambling 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 findings for 5 years from the date the record was created. Where a Category 2 eGambling licensee or foreign gambling 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.

²⁴ 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.

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 Regulation 188
- policies, procedures and controls that are required pursuant to the Alderney eGambling Regulations, 2009

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.

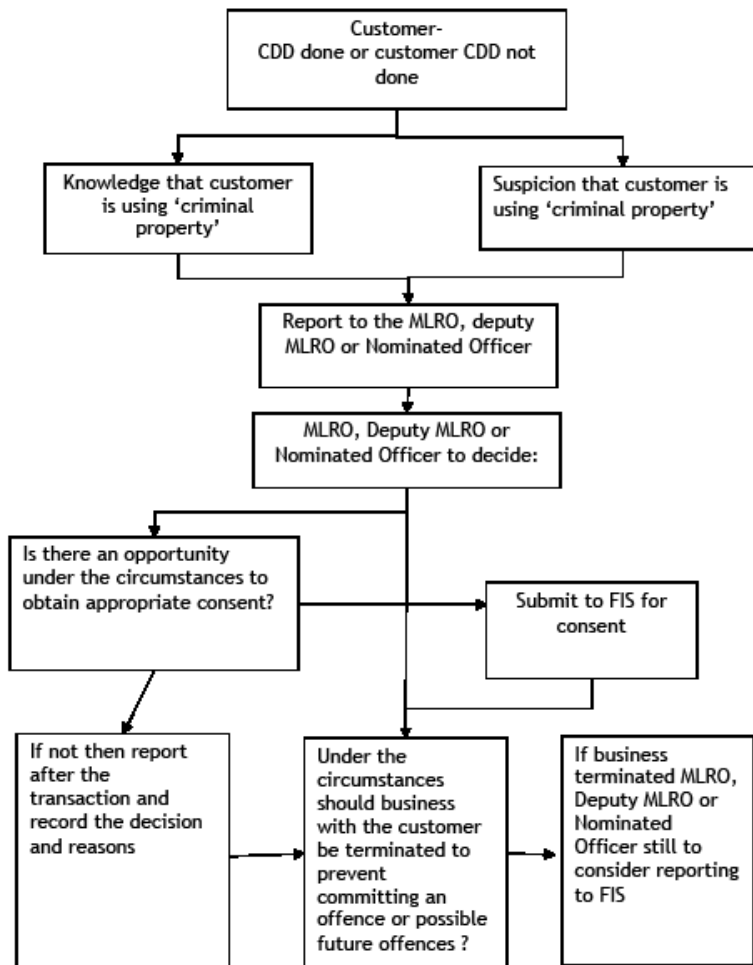
These three instances are referred to as “grounds for knowledge or suspicion”.

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 Alderney eGambling Regulations, 2009. There is specific requirement that licensees train their staff regarding their obligations and the requirement to make reports to their MLRO or nominated officer.

The table on the next page sets out a helpful flow chart for a Category 1 eGambling licensee to consider if a STR should be made.

Knowledge or suspicion of money laundering or terrorist financing
(the subjective test)



Certain employees of a licensee will be relevant employees (as defined in the regulations). 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 is to be done.

10.2 Internal reporting to the MLRO

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.²⁵ Licensees will need to address how their employees refer matters to the MLRO or Nominated Officer²⁶

²⁵ The ICS must address the systems that will ensure this takes place.

²⁶ 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.

10.3 Reporting to the FIS

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.²⁷ 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.

Appendix 1 of this guidance contains the current form for making a report to the Financial Intelligence Service. This form may be subject to alteration and therefore the form should always be downloaded from the relevant section of the Financial Intelligence Service Website located at

<http://www.guernseyfis.org/disclosureServices.asp>

It is a legal requirement that any disclosure report is made in accordance with the form located at Appendix D2 of the Guernsey Financial Services Commission (GFSC) Handbook. A link to the GFSC handbook can be found below:

[http://www.gfsc.gg/UserFiles/File/CFC/FSB%20June10\(clean\)\(2\).pdf](http://www.gfsc.gg/UserFiles/File/CFC/FSB%20June10(clean)(2).pdf)

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 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.

²⁷ 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.

To summarise:

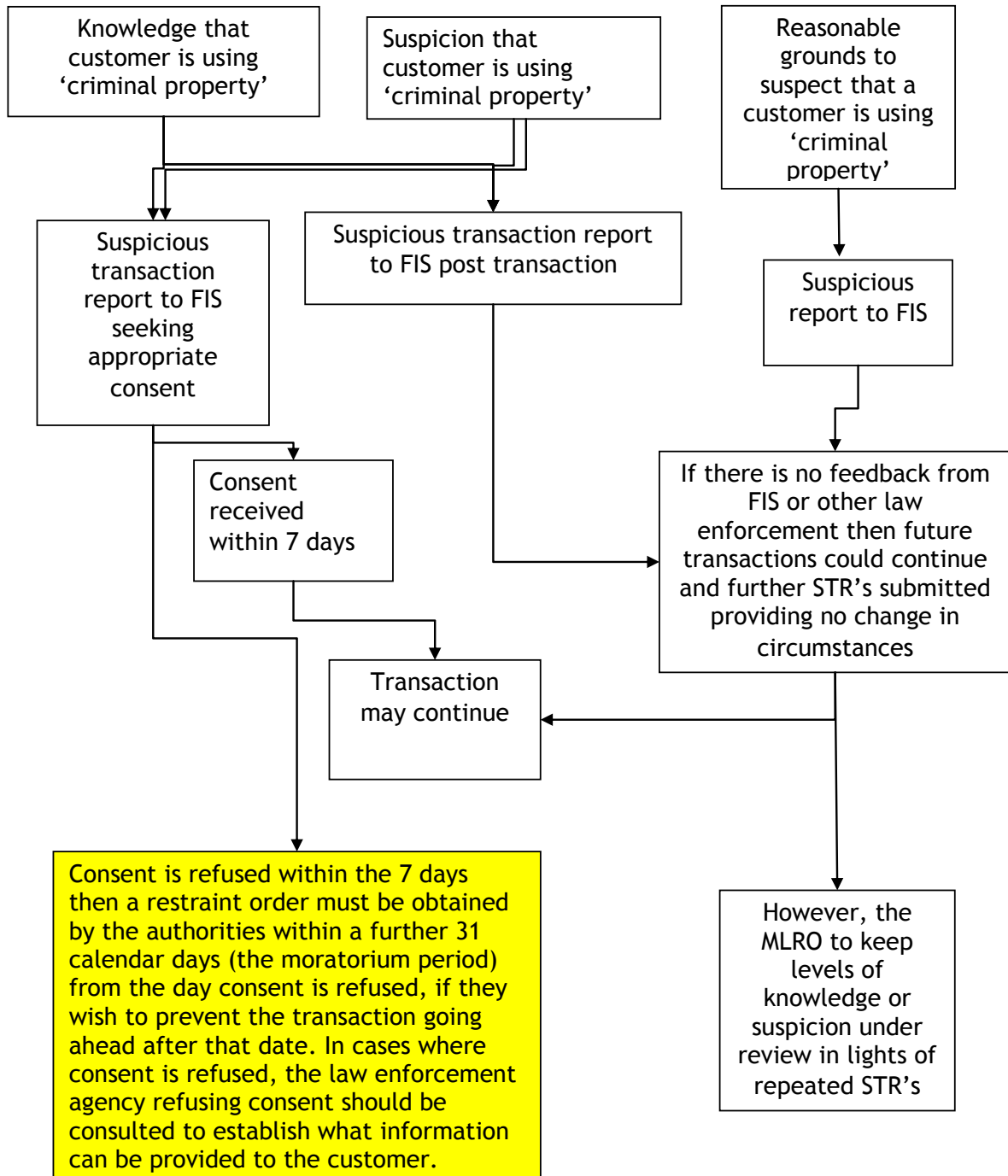
Reports of suspicious transactions must be made

- 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.²⁸

In order for a licensee to ensure that employees are of the required standard of competence they must have effective policies, procedures and controls in place.

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. 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 receive training in relation to - :²⁹

- relevant enactments, the Law, the Ordinance and these Regulations.
- 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

²⁸ 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.

²⁹ 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.

- 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 training in CDD requirements.

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

Relevant employees would include those 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 will be relevant employees. In addition those employees supporting those employees having direct contact with customers or those handling or being responsible for the handling of customer relationships or financial or gambling transactions will also be considered as relevant employees.

Relevant employees also include any member of the licensee's management or board of directors.

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 The Board and Senior Management

The Board and senior management should receive training in:-

- The relevant enactments, the regulations and information on the offences and the related penalties including those relating to key individuals;
- The CDD and record keeping requirements; and
- The internal and external suspicion reporting procedures.

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 training

12. UN and EU SANCTIONS

12.1 The Terrorism Order

- The Terrorism (United Nations Measures) (Channel Islands) Order 2001 (“**Terrorism Order**”), which implements UN Resolution 1373, makes it a criminal offence for any person to make any funds or financial services available to or for the benefit of any person “involved with terrorism” as per Article 3 of the Terrorism (UN Measures) Order 2001 and link to which can be found at <http://www.opsi.gov.uk/si/si2001/20013365.htm>.
- Article 3 of the Terrorism (United Nations Measures) Order 2001 makes it a criminal offence for any person to make any funds or financial services available to or for the benefit of any of the following persons -
 - (a) commit, attempt to commit, facilitate or participate in the commission of terrorism,
 - (b) are controlled or owned directly or indirectly by persons referred to in paragraph (a) above, or
 - (c) are acting on behalf of, or on the direction of, persons referred to in paragraph (a) above.

Category 1 eGambling licensees need to have criteria in place to trigger checks as to whether players fall under the definitions of the Terrorism Order.

- In order to meet the requirements of the Terrorism Order, a Category 1 eGambling licensee must ensure that they do not make any funds and/or financial services available to or for the benefit of any particular individual, entity or group which is provided for in the Terrorism Order.

When determining whether a particular individual or legal person falls into any of those categories, licensees must consult the full list of financial sanctions targets in the HM Treasury website (http://www.hm-treasury.gov.uk/fin_sanctions_index.htm).

12.2 The Al-Qa'ida Order

- The Al-Qa'ida and Taliban (United Nations Measures) (Channel Islands) Order 2002 (“**Al-Qa'ida Order**”), which implements UN Resolution 1267, contains requirements similar to those of the Terrorism Order in respect of the provision of funds to designated persons as per Article 2 of the Al-Qa'ida (UN Measures) Order 2002 which can be found at <http://www.opsi.gov.uk/si/si2002/20020111.htm>.

- A listed person under Article 2 of the Al-Qa'ida Order is –
 - (a) members of the Al-Qa'ida organisation, or
 - (b) members of the Taliban, or
 - (c) individuals, groups, undertakings or entities associated with the persons covered by (a), (b)(i) or (ii) above.

- While the presence of individuals and entities on either of the above lists is a strong indication that such persons respectively fall within the definitions in the Terrorism and Al-Qa'ida Orders, there are likely to be legal or natural persons who come within those definitions but are not on the lists.

13. FURTHER READING

The FATF 40 Recommendations:

http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html

The FATF 9 Special Recommendations on Terrorist financing:

http://www.fatf-gafi.org/document/9/0,3343,en_32250379_32236920_34032073_1_1_1_1,00.html

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

<http://www.fatf-gafi.org/dataoecd/43/46/38960576.pdf>

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

<http://www.fatf-gafi.org/dataoecd/47/49/42458373.pdf>

The FATF Guidance on money laundering and terrorist financing typologies

<http://www.fatf-gafi.org/dataoecd/16/8/35003256.pdf>

The FATF report on money laundering through the football sector

<http://www.fatf-gafi.org/dataoecd/7/41/43216572.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

It should be noted that references, citations, links, and re-directions to other bodies are correct as at 30th July, 2010..

©TheAlderneyGamblingControlCommission2010

APPENDIX 1

DISCLOSURE FORM

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: <i>e.g. company registration number, date and place of incorporation, etc.</i>			
Account name			
Account/product number			

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

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.