mha
Financial Crime Support

The threat of money laundering and terrorist financing through the online gambling industry

A Report prepared for the Remote Gambling Association by MHA Consulting

June 2009

The threat of money laundering and terrorist financing through the online gambling industry

A report prepared for the Remote Gambling Association

1 Executive summary

Whilst, historically, the measures to guard against money laundering and terrorist financing had been directed towards the financial sector, in December 2001 the Second European Money Laundering Directive[1] extended the provisions to a range of non-financial sector businesses, including casinos, and set an implementation deadline of June 2003[2]. Whilst the scope of the Directive was extended to the gaming sector because of the perceived vulnerabilities of land-based casinos, there continues to be a perception that remote casinos are also similarly vulnerable. Consequently, both the perception and the money laundering risks have needed to be managed by the remote gambling industry.

The imposition of money laundering and terrorist financing requirements on remote casinos is therefore relatively new, and application of industry standards and regulations that had been designed primarily for the heavily regulated and significantly vulnerable financial sector has provided a significant challenge. In October 2005, the Second European Directive was replaced by a Third Directive[3] which added a further set of challenges.

However, regardless of these challenges, there appears to be a strong commitment across the industry to prevent and detect money laundering and terrorist financing, to comply with the various legislative and regulatory requirements and to co-operate with the authorities.

The jurisdictions within which RGA members operate are subject to the Financial Action Task Force (FATF) international standards relating to the prevention of money laundering and countering terrorist financing. Specific guidance has also been drawn up for the gambling industry to supplement these generic standards. In addition, all EEA member states are bound by the European Money Laundering Directives. Specific AML/CFT regulations and

[1] Directive 2001/97/EC of the European Parliament and Council

[2] The Second European Money Laundering Directive was implemented in the UL by the Money Laundering Regulations 2003 which became effective on 1 April 2004.

[3] Directive 2005/60/EC of the European Parliament and Council

guidance therefore apply to remote gambling within all of the jurisdictions within which RGA members operate.

However, as is the case with all financial and non-financial businesses that come within the scope of the European Directives and the international standards to counter money laundering and terrorist financing, the strength and application of the regulatory measures varies. The industry is also truly cross-border, and operators must work across the requirements of a number of jurisdictions when devising their policies and procedures. As the regulations start to bite, this could provide a temptation for some less scrupulous operators outside of the EU to locate themselves in the least well regulated centres. Nevertheless, the fact that the regulators must also work to international standards against which their success will be measured, limits the scope for regulatory arbitrage. There is also evidence that the International Association of Gaming Regulators is working on the development of common standards and guidelines that will further limit the scope for such regulatory arbitrage and should provide the opportunity for a proportionate approach that limits the current variations.

The application of a risk-based approach to money laundering and terrorist financing through the Third Directive and the FATF Recommendations places significant responsibilities on senior management to assess, manage and mitigate the risks. To assist senior management in this respect, all remote gambling operators have appointed a money laundering reporting officer/nominated officer to establish internal controls and procedures, to monitor compliance with the relevant legislation, regulations and guidance and to provide a central point of contact for reporting suspicious activity.

Undertaking customer due diligence and monitoring customer activities as prescribed by the Directives and international standards is not a new requirement for the remote gambling industry and the application of electronic identification measures strengthens the process. The industry also undertakes age verification, and gaming surveillance to guard against underage and problem gambling.

Evidence suggests that the strong fraud prevention measures in place within all remote gambling operators are being used successfully to prevent and detect money laundering, in particular the risk of identity theft and fraud through the use of stolen credit cards. However the money laundering and terrorist financing risks are different and operators need to work together and with their regulators and law enforcement to ensure that the risks are adequately understood and managed.

However, the extension of customer due diligence and identification measures that work for the remote gambling industry need to be further developed taking an industry wide approach. Benefit could be gained from discussions with regulators and law enforcement agencies and the development of specific cross-border practices that are tailored to the needs and practices of the industry. In the absence of practical guidelines developed by the industry itself in consultation with its regulators, remote gambling operators and their trade associations will not be best placed to influence consultation on standardisation and new best practice recommendations as they emerge from the regulators, the FATF or other international standard setting bodies. Standard guidelines and procedures will also assist in the formulation of effective training programmes across the industry.

2 Introduction and background

2.1 Background to the report

The Remote Gambling Association (the RGA) represents the world's largest licensed and stock market-listed remote gambling companies and provides the industry with a single voice on all the issues of importance to regulators, legislators and key decision makers around the world.

The RGA is aware that there has been much speculation as to whether online/remote gambling is more susceptible to money laundering and terrorist financing than other comparable services. As the online gambling industry is an inherently international one where electronic payments methods are the norm, fears have been expressed in some quarters that it provides a particularly attractive opportunity for money laundering and terrorist financing. An additional factor is the perception that the industry is lacking in regulation.

The RGA has refuted these points and believes that the threat of money laundering generally has been greatly diminished by the industry's own efforts and increased regulation flowing from various initiatives.

Accordingly, the RGA has commissioned MHA Consulting, a recognised anti-money laundering and financial crime subject matter expert, to consider the existing situation and practices as applied to online gambling operations within the EEA (including Gibraltar and Malta) and the Channel Islands and prepare a report which:

- Provides a reliable definition of what constitutes money laundering through the online gambling industry
- Determines a threat assessment of the risks of money laundering and terrorist financing through online gambling.
- Reviews money laundering legislation and regulations as they apply to online gambling.
- Provides a summary of best practice within the online gambling industry.
- Compares the situation in the online gambling industry with other industries, notably those in the financial services sector.

3 Definition of online gambling

Section 4 of the UK Gambling Act 2005 defines remote gambling as "gambling in which people participate by the use of "remote communication". Remote communication means communication using the internet, telephone, television, radio "any other kind of electronic or other technology for facilitating communication". This is designed to cover all forms of gambling where players are not face to face.

Remote gambling includes the following forms:

- Remote Wagering on Horse Races
- Remote Lottery Play
- Online Telephone Race and Sports Books
- Multi-Player Online Poker through interactive poker rooms
- Online Casinos offering online gambling through games such as blackjack
- Betting Exchanges – peer-to-peer betting exchanges by which individual bettors can place wagers against one another on opposing outcomes of a future event
- Interactive Gambling - including traditional betting wagering forms as diverse as traditional betting to fixed odds gambling, live and interactive bingo betting and interactive betting on live sporting events."

3.1 RGA members assisting with the project

As part of the research undertaken by MHA a number of operators were chosen by the RGA as providing a reasonable cross section of the industry in terms of both product ranges and jurisdictional bases..

Meetings were held with them to discuss their approach to managing their money laundering and terrorist financing risks and copies of their current policies and procedures were obtained.

3.1.1 Types of gaming/betting offered and jurisdiction of licensing

Of the operators assisting with the project, two provide land based facilities although RGA members primarily provide remote gambling facilities only. Operators are licensed in a variety of jurisdictions including Alderney, Antigua, Australia Malta, Gibraltar and the UK. Head office and customer service staff are located in a number of jurisdictions including the UK, Malta, Bulgaria and the Philippines.

RGA members basically offer four types of online gambling:

1) Sports Book
2) Casino
3) Poker
4) Bingo
5) Interactive games.

Sports Book and betting exchanges are not covered by the UK or Gibraltar Money Laundering Regulations.

4 What is money laundering and terrorist financing?

4.1 Money laundering

The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source.

Illegal arms sales, smuggling and the activities of organised crime, including for example drug trafficking and prostitution, rings, can generate huge amounts of proceeds. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to "legitimise" the ill-gotten gains through money laundering.

When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved, Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.

Law enforcement advises[4] that Cash remains the preferred currency of criminals primarily because it is anonymous and leaves no audit trail and a significant proportion of criminal funds is generated in cash. However, in non-cash based societies such as the UK large amounts of cash cannot be disposed of safely without raising suspicion and must therefore be integrated into the economy through conversion into other forms of currency e.g. cheques or other forms of payment from respectable institutions.

As large unexplained sums of cash can no longer be placed into the financial system through banks and other financial services businesses without raising suspicion, laundering through retail businesses and other establishments which accept cash payments is a principal means of laundering the criminal funds through the initial placement stage of money laundering.

In the context of remote and non-remote gambling, money laundering has been described [5] as:

"*including three methodologies, each based on those initiating the actual money laundering (the customers) 'knowing' the funds are illegitimate. From a customer's perspective, these are:*

i) The 'conversion' of illegally obtained funds into funds whose source appears legitimate, i.e. conventional 'washing of dirty money'

ii) The disguise of 'illegally obtained funds, i.e. misrepresenting dirty money to a recipient.

iii) *The 'disposal' of illegally obtained funds, i.e. 'spending or receiving dirty money'."*

[4] SOCA UK Threat Assessments

[5] Gibraltar Regulatory Authority: Gambling Commissioner - Consultation Document on a Proposed AML/CFT Code of Practice for the Gambling Industry

Consequently, as is the situation in the UK, the Commissioner has emphasised that "the simple spending of dirty money, including depositing, wagering, winning or losing arising from that money, amounts to money laundering by the customer".

Within the UK, money laundering is defined in section 340 of the Proceeds of Crime Act 2002 and covers wide ranging circumstances involving any activity concerning the proceeds of crime. This includes:

- Acquiring, possessing, transferring or converting the proceeds of crime
- Handling the benefit of acquisitive crimes such as theft, fraud and tax evasion
- Handling stolen goods
- Being directly involved with any criminal or terrorist property, or entering into an arrangements to facilitate the laundering of criminal or terrorist property
- Criminals investing the proceeds of their crimes in any financial product or using the proceeds to buy goods and services.

4.2 Terrorist financing

According to the definition contained in the UN International Convention for the Suppression of the Financing of Terrorism, the primary objective of terrorism is "to intimidate a population or to compel a Government or an international organisation to do or abstain from doing any act". This is in contrast to other forms or criminal activity where financial gain is generally the ultimate objective.

Since the events of 11th September 2001, action to combat terrorism and terrorist financing has been placed on an equal footing to preventing money laundering, international conventions and standards are now in place requiring countries to take the necessary action.

Whilst there is a difference in goals between terrorism and other criminal activity, terrorists still require financial support in order to achieve their aims and a successful terrorist group, like any criminal organisation, is therefore one that is able to build and maintain an effective financial infrastructure.

Terrorists and their organisations need finance for a wide variety of purposes – recruitment, training, weapons, travel, material and safe haven protection. The intelligence that can be gained in to terrorist networks through knowledge of their financial transactions and dealings is vital in protecting national and international security and upholding the integrity of national and international financial systems.

Terrorists often control funds from a variety of sources around the world and employ increasingly sophisticated techniques to move these funds between jurisdictions. As with other criminal activity, a significant proportion of the terrorist funding originates in cash which must then be laundered. Detecting the transmission of money to finance terrorist activity as it moves through the finance and business sectors is challenging, especially before a terrorist attack takes place. Nevertheless, disrupting the financial support for terrorism does make it harder for terrorists to operate. Tracking the flow of funds also provides

information on links, profiles and movements, which help to build up an intelligence picture of the way terrorists and terrorist organisations operate.

4.3 Measures to prevent money laundering and terrorist financing

No business sector is immune from being targeted by criminals and all businesses are open to a variety of criminal risks. Domestic and international measures to guard against laundering the proceeds of crime have historically focused on the traditional banking and financial sector. However, as defensive measures have been put in place by the financial sector, the criminal have turned their attention to a range of non-financial sectors and businesses to assist in their laundering operations. Law enforcement have identified a number of business sectors where investigations have highlighted money laundering or terrorist financing vulnerabilities and these sectors have now been brought within the scope of domestic and international legislation and standards. Casinos, including remote casinos, fall within the list of non-financial businesses now subject to anti-money laundering legislation together with other comparable services.

The AML/CFT legislation, regulations and standards affecting the online gambling industry are set out in the Appendix to this report.

4.3.1 The application of a risk-based approach

International efforts to prevent and detect money laundering have now been in place for the past 18 years, and in respect of terrorist financing for the past 7 years. Consequently, compliance with money laundering and terrorist financing laws and regulations is not new for the financial sector. However, the extension of these requirements to non-financial businesses such as remote casinos is relatively new in AML regulatory terms, having been introduced through the Second European Directive in 2001 and into the UK Money Laundering Regulations in 2003.

The requirement for a risk-based approach to managing and mitigating money laundering and terrorist financing risks is a new concept for all businesses, including those within the financial sector. Whilst the concept was recognised by the FATF recommendations in 2003 and, introduced by the UK in 2004 it was not generally applied until it was included in the Third European Directive in 2005 for implementation by December 2007.

By adopting a risk-based approach, it is possible to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This allows resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention. The alternative approaches are that resources are either applied evenly, or that resources are targeted, but on the basis of factors other than risk. This can inadvertently lead to a “tick box” approach with the focus on meeting regulatory requirements rather than on combating money laundering or terrorist financing efficiently and effectively. A risk-based AML/CFT regime should help to ensure that honest customers can access the services provided by remote casinos, but creates barriers to those who seek to misuse these services.

Because the concept of risk assessment is new and subjective, there is, as yet no acknowledged right or wrong way to its application. Many legislators, regulators and supervisors have themselves struggled to understand the concept and to determine how it should be applied to combat money laundering and terrorist financing. In recognition that both public authorities and the private sector companies needed assistance in this respect, the FATF set up an Electronic Advisory Group in 2005. The outcome was Guidance consisting of high level principles and procedures which included guidance for public authorities and financial institutions that was adopted by the FATF at its June 2007 Plenary meeting. The meeting also endorsed a proposal to develop guidance on the risk-based approach for the non-financial businesses and professions that are covered by the FATF Recommendations. Separate working groups comprising public and private sector members were established and at its October 2008 Plenary, RBA Guidance for Casinos, including remote casinos, was adopted.

The purpose of the Guidance is stated as being to:

- Support the development of a common understanding of what the risk-based approach involves.
- Outline the high-level principles involved in applying the risk-based approach.
- Indicate good practice in the design and implementation of an effective risk-based approach.

The Guidance is written at a high level to cater for the differing practices of remote casinos in different countries, and the different levels and forms of supervision that may apply. However, the primary target audience for the Guidance is the remote casinos themselves. The wider audience for the Guidance includes countries and regulators which are considering how to apply AML/CFT measures to casinos. The guidance advises counties that they need to identify the most appropriate regime tailored to address individual country risks, and which take into consideration the idiosyncrasies and activities of casinos in their countries.

The Guidance includes the observation that Internet casinos vary significantly to land-based and internet casinos in a number of key areas, including customer contact e.g. whether the operator has other web sites or whether the operator's server is in a different country from other parts of its business.

The Guidance also recognises that both types of casinos are generally subject to a range of regulatory requirements, commercial considerations and security measures, which can complement AML and CFT measures, for example:

- Age verification.
- Financial crime controls.
- Social responsibility provisions.
- Security controls.
- Gaming surveillance, e.g. to deal with problem gambling.

4.4 The money laundering and terrorist financing risks and threats within the on-line gambling industry

4.4.1 Purpose of the section

The purpose of this section is to explain the perceived vulnerabilities that need to be addressed. The policies and procedures that have been put in place by the Gambling regulators and the remote gambling industry to manage and mitigate these vulnerabilities are contained in section 5.

The United States has published the results of official government studies[6] concluding that online gambling is not a likely accessible avenue for money laundering because:

- the identities of the gamblers are known;
- the financial transactions between the bettors and operators are all in electronic format; and
- all of the wagering is recorded.

4.4.2 The Financial Action Task Force RBA Guidance for Casinos

The Financial Action Task Force (FATF) RBA Guidance for Casinos advises[7] that the following money laundering and terrorist financing risks can arise from the operation of remote casinos i.e. products, services, games and account activities. Whilst the report focuses on remote casinos, many of the vulnerabilities are those that apply universally to all e-commerce businesses that use a variety of payment methods across a range of markets and jurisdictions.

- **Proceeds of crime**

As with all retail businesses, however money is transferred to a casino, there is a risk that this money will have arisen from illegal activities such as cheque fraud, credit/debit card fraud, drug trafficking, theft from employer etc.

- **Cash**

The majority of payments to Internet casinos are made directly from financial institution accounts. However, Internet casinos can operate as part of mixed gambling chains which also include betting shops and/or land-based casinos. It may be possible for customers to provide land-based outlets with cash which can then be credited to Internet casino accounts.

- **Transfers between customers**

Internet casinos may permit, or be aware of, customers transferring money between themselves without using their casino's account.

- **Improper use of third parties**

Criminals may use third parties or anonymous or identified agents to gamble amounts on their behalf to avoid customer due diligence being undertaken on

[6] United States General Accounting Office – Internet Gambling: an Overview of the Issues , GAO-03-89 (2 December 2002)

[7] FATF RBA Guidance for Casinos 23 October 2008

them. Third parties may be used to buy chips, or to gamble on behalf of others with minimal play.

- **Use of casino deposit accounts**

Without satisfactory internal controls, customers may use such accounts casino deposit accounts to deposit and withdraw without gambling or with minimal play

- **Multiple casino account or casino wallets**

An internet operator may own and control multiple web sites. Single web sites can also offer a range of different types of gambling. Customers may wish to separate different types of gambling they are conducting with the same operator, or through the same web site for legitimate reasons, e.g. to monitor their performance in different areas. However, customers may open multiple accounts or wallets for dishonest or inappropriate reasons, including attempting to obscure their spending levels, or to avoid checks undertaken at a threshold level.

- **Changes to financial institution accounts**

Casino customers commonly use their accounts with financial institutions to gamble over the internet. Customers may hold a number of financial institution accounts, and they may wish to change which of these accounts they use in casinos. This may be for legitimate reasons or may be to confuse the audit trail or to introduce third party transactions without due diligence having been performed.

- **Identity fraud**

Details of financial institution accounts may be stolen and used on web sites. Stolen identities may also be successfully used to open financial institution accounts and such accounts may also be used on web sites. Criminals may then open multiple casino accounts using these stolen identities.

- **Pre-paid cards**

Using cash to fund a pre-paid card poses similar risks as cash. Internet casinos cannot make the same level of cross reference checks on some types of pre-paid cards as they are able to perform on financial institution accounts.

- **Electronic wallets (e-wallets)**

Not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits However, e-wallets which only accept money from financial institution accounts in the customer's name will not usually pose any greater or lesser money laundering or terrorist financing risk than if funds are received directly from the financial institution. Nevertheless, when customers make payments into e-wallets from their financial institution accounts, the statements issued by their financial institutions may only record the payment to the e-wallet, not the transaction to the Internet casino. This may be useful for dishonest customers who wish to disguise their gambling.

- **Games involving multiple operators**

Internet poker games often take place on platforms (i.e. a central computer system that links electronic gambling devices for purposes of game selection, operation, monitoring, security, and auditing) shared by a number of different casino operators. The platform is likely to play a key role in monitoring the patterns and values of play for potential money laundering activities e.g. chip

dumping. However, without clear operator and platform policies in relation to respective roles and actions, this advantage can be lost.

4.4.3 Variables which affect the money laundering and terrorist financing risks

The FATF goes on to advise that the following range of variables will impact the level of AML/CFT risks that casinos face:

- Whether a casino's business model centres upon either or both of the following options:
  - attracting a large number of customers who gamble relatively small amounts of money; or
  - attracting a small number of customers who gamble relatively large amounts.
- Speed and volume of business.
- Types of financial services offered to customers.
- Types of payment and payment methods accepted from customers.
- Types of gambling offered e.g. table games, card games, and electronic games (live or automated).
- The nature of the customers – whether they are regular/frequent customers or irregular/occasional customers.
- Whether the casino forms part of a bigger organisation owned by the same operator, for example:
  - whether the casino operator owns and manages other land-based and/or Internet casinos;
  - whether the casino, or its operator, offers different types of gambling e.g. sports book, premium players;
  - for internet casinos, whether the operator has other web sites.
- Whether the casino is wholly based in one country, or has a presence in multiple countries, e.g. whether an Internet operator's server is in a different country from other parts of its business.
- Staffing numbers, turnover rate and experience levels.
- Type and effectiveness of existing supervision mechanisms e.g. electronic and/or physical loyalty clubs which monitor gaming activity.

Another important variable is the level of general regulation of the casino, whether this occurs at a national or state/provincial level and whether they are subject to a comprehensive regulatory and supervisory regime that ensures they have effectively implemented the necessary AML/CFT measures. An important aspect of such regulation is to ensure the honesty and integrity of casino staff.

5 Managing and mitigating money laundering and terrorist financing risks within the remote gambling industry

5.1 Regulatory advice on the application of the FATF's good practice guidance

Application of a risk-based approach to money laundering and terrorist financing is not straightforward in that it requires subjective judgements and decisions to be made. Consequently assessing and mitigating the risks will lead to different results across the industry both within and between jurisdictions.

FATF paragraphs 34-35: Challenges of the risk-based approach states that

"Implementing a risk-based approach requires that casinos have a sound understanding of the risks and are able to exercise sound judgement. This requires the building of expertise including for example, through training, recruitment, taking professional advices and 'learning by doing"….Attempting to pursue a risk-based approach without sufficient expertise may lead to flawed judgements. Casinos may over-estimate risk, which could lead to wasteful use of resources or they may under-estimate risk, thereby creating vulnerabilities.

"Casinos may find that some staff members are uncomfortable making risk-based judgements. This may lead to overly cautious decisions, or disproportionate time spent documenting the rationale behind a decision. This may also be true at various levels of management. However, in situations where management fails to recognise or underestimates the risks, a culture may develop that allows for inadequate resources to be devoted to compliance, leading to potentially significant compliance failures".

With a view to assisting the remote gambling industry to implement a risk-based approach, regulators in each of the relevant jurisdictions have published guidance and best practice advice. Examples of this best practice advice, based on the principal requirements of the FATF standards and the European Directive, are set out in sub-sections 5.1.1 – 5.1.7 below.

The practice that the remote gambling industry has adopted to manage and mitigate its risks and to apply the regulatory guidance is set out in section 5.2.

5.1.1 Senior management responsibilities

A risk-based approach places specific requirements on senior management to assess the type and nature of money laundering and terrorist financing risks that an operator faces.

The UK Gambling Commission Guidance advises that:

"Senior management should be fully engaged in the processes around an operator's assessment of risks for money laundering and terrorist financing, and should be involved at every level of the decision making to develop the operator's policies and processes to comply with the regulations".

The guidance goes on to suggest that in addressing risks in the context of how an operator is most likely to be involved in money laundering or terrorist financing, a number of questions should be asked, including:

- *What risk is posed by the business profile and customers using the casino?*

- *Is the business high volume consisting of many low spending customers?*
- *Is the business low volume with high spending customers, perhaps who use and operate within their cheque cashing facilities?*
- *Is the business a mixed portfolio, i.e. customers are a mix of high spenders and lower spenders and/or a mix or regular and occasional customers?*
- *Are procedures in place to monitor customer transactions and mitigate any money laundering potential?*
- *Is the business local with regular and generally well known customers?*
- *Are there a large proportion of overseas customers using foreign currency or overseas based bank cheque or debit cards?*
- *Are customers likely to be individuals who hold public positions in countries which carry a higher exposure to the possibility of corruption, ie a politically exposed person (PEP)?*
- *Are customers likely to be engaged in a business which involves significant amounts of cash?*
- *Are there likely to be situations where the source of funds cannot be easily established or explained by the customer?*
- *Are there likely to be situations where the customer's purchase or exchange of chips is irrational or not linked with gaming?*
- *Is the majority of business conducted in the context of business relationships?*

Alderney eGambling Control Regulations require that eGambling Licensees prepare a Business Risk Assessment "which documents the exposure of the business 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 (a) its size, nature and complexity; and (b) customers and services and the ways in which it provides those services"

The Gibraltar Regulatory Authority – Gambling Commissioner is also proposing that licence holders undertake a formal risk assessment of the business. Paragraph 3.3. of the January 2009 Consultative Document states that:

"The Nominated Officer will be required to ensure that the licence holder undertakes or reviews any existing formal risk assessment in respect of their relevant gambling products, customers, areas of operation and transaction methods, and their susceptibility to the differing types of money laundering, and review, develop or implement corresponding policies. The commissioner is aware that whereas some games, bets, stakes and transaction methods have already established a reputation as being open to certain lower level money laundering typologies, other elements of gambling have proved unproblematic, and licence holders' policies, procedures and systems should reflect these differences. The risk assessment process is likely to be a substantial and ongoing process for operators and should include an annual report to the Board/directors".

5.1.2 Internal controls

Paragraphs 134 – 138 of the FATF Guidance cover the need for internal controls, policies and procedures as also required by the Third Directive. However the following guidance is of particular relevance:

"When devising internal controls, casinos should consider their overall operation. Senior management should ensure that their ownership of AML/CFT issue is visible at the Board or equivalent level and to all staff and business partners, including acknowledging their personal responsibility to ensure that there are adequate systems and controls in place. Senior management is in a position to influence the culture of their organisation, including encouraging a culture of compliance.

Casinos should conduct independent internal and/or external testing for AML/CFT programmes with a scope and frequency commensurate with the risks of money laundering and terrorist financing they face, as well as the products and services provided, to determine if casinos' procedures are comprehensive enough to detect suspicious activities. Casinos should take corrective actions once becoming aware of weaknesses and deficiencies in their AML/CFT risk-based programmes, or any element thereof, that could or did result in failures to comply with governmental requirements".

As part of the internal control and compliance monitoring procedures, the UK Gambling Commission Guidance requires that:

"*The nominated officer should compile an annual report covering the operation and effectiveness of the operator's policies and procedures to combat money laundering. In practice, senior management should determine the depth and frequency of the information they feel is necessary to discharge their responsibilities. The nominated officer may also wish to report to senior management more frequently than annually, as circumstances dictate".*

The Alderney Gambling Control Commission Guidance stresses that:

"*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".*

Senior management should:

- *be involved in the decision making process*
- *Record the decisions mad*
- *Implement the procedures appropriately".*

5.1.3 Undertaking customer due diligence

Customer due diligence, including verifying the identity of customers, has always played a key role in AML/CFT controls and procedures. International standards now extend the requirement beyond the direct customer to any beneficial owner i.e. the natural person who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted.

In accordance with international standards, customer due diligence must be undertaken in the following circumstances:

- When establishing a business relationship.

- When carrying out occasional transactions amounting to €15,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked.
- When there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold.
- When there are doubts about the veracity or adequacy of previously obtained customer identification data.

In respect of Casinos, the Third European Directive requires that all casino customers be identified and their identity verified if they purchase or exchange gambling chips with a value of €2,000 or more during any period of 24 hours. This differs from the FATF Recommendations which sets the threshold amount at €3,000.

The alternative to the threshold approach is the 'on entry approach which requires casinos to identify and verify the identity of the customer before access is given to remote gaming. Once the customer's identity is verified he may commence gaming.

5.1.3.1 Forming a business relationship

Under Alderney's eGambling Regulations, an eGambling licensee must enter into a business relationship with a customer. The concept of occasional or one-off transactions is not permitted. In respect of the UK, the Gambling Commission guidance advises that:

"*Casinos are likely to form a business relationship when:*

- *the casino starts tracking a customer's drop/win figures;*
- *a customer opens an account with the operator or joins a membership scheme; or*
- *a customer obtains a cheque cashing facility".*

5.1.3.2 Application of the threshold approach

Application of CDD measures when a threshold has been reached can be administratively difficult as activity must be monitored to determine when the threshold has been reached. If CDD measures not applied before the threshold, gambling activity must be suspended once the threshold is reached to enable the checks to be completed.

The UK Gambling Commission Guidance has anticipated these difficulties and provides the following advice:

"If casinos wish to adopt the threshold approach, the following two conditions must be satisfied:

- *It must verify the identity of each customer before, or immediately after, the customer purchases, exchanges, pays or stakes €2000 or more; and*
- *The Commission must be satisfied that the casino operator has appropriate procedures in place to monitor and record the total money paid or staked in connection with facilities for remote gaming by each customer.*

Casino operators will have to satisfy the Commission that they have the mechanisms in place that are appropriate for the spend profile. For example, a

casino with a customer drop/win average considerably below the threshold will need mechanisms in place to monitor customer transactions to be sure that any customer reaching the threshold level is picked up in good time to allow CDD to be completed.

Casinos adopting the threshold approach should think carefully about whether they wish to defer both identification and verification until the threshold is reached, or whether identification will be conducted on entry but verification deferred until the threshold is reached. Remote casinos may require customers to identify themselves (and undertake age verification) on registering with the casino but only require verification of identity if the threshold is reached.

There may be significant advantages in asking customers for their identification on entry, even if verification of this information is deferred until the threshold is reached, for example, identifying customers on entry means it will not be necessary to interrupt the customer's gambling once the threshold is reached and verification becomes necessary.

Casinos using the 'threshold approach' must be sure that they are able to end transactions with a customer who reaches the threshold if they are unable to comply with the CDD requirements".

5.1.3.3 Undertaking the CDD requirements

The Third European directive outlines the following four parts of customer due diligence, including an explicit requirement for ongoing monitoring:

1. Identify the customer and verify the customer on the basis of documents, data or information obtained from a reliable independent source.
2. Identify, where applicable, the beneficial owner and take risk-based and adequate measures to verify his identity so that the operator is satisfied that it knows who the beneficial owner is.
3. Obtain information on the purpose and intended nature of the business relationship.
4. Conduct ongoing monitoring of the business relationship on a risk sensitive basis.

Where CDD cannot be completed, the relationships or occasional transaction must not proceed. The UK Gambling Commission Guidance advises that *"Casinos must therefore have clear policies on how they will manage situations where they are unable to comply with the CDD measures. The casino must stop transactions until the CDD requirements can be achieved"*.

In respect of the requirements to identify and verify identity the UK Gambling Commission Guidance states that:

"Casino operators may identify their customers simply by asking them for personal information, including name, home address and date of birth. Some or all of this information will need to be verified. It may also be helpful to obtain information on customers' source of funds and level of legitimate income e.g. occupation. This information may assist casinos with their assessments about whether a customer's level of gambling is in profile for their approximate income, or whether it is suspicious".

Evidence of identity can be verified with by way of documents obtained from the customer e.g. passport, driving licence, bank statements, utility bills etc, or through electronic evidence.

5.1.3.4 Electronic identification evidence

In addition to the generic CDD requirements that apply to all businesses, paragraphs 121-124 of the FATF Guidance provide the following specific recommendations for Internet casinos:

"In the majority of cases Internet casinos do not meet their clients, except perhaps their high spenders.

Non-face to face business can carry specific risks and requires alternative or additional compliance methods, especially in the area of CDD to compensate for the fact that Internet casinos are therefore unable to verify customer's physical appearance against photographic identification documents. These methods rely upon new technologies, including the deposit and withdrawal methods offered on the website, and checks on the customer's IP address.

If casinos use software systems to assist with CDD the software should access a range of positive and negative checks. Although not available in all countries, public source data can be particularly valuable in identifying PEPs and individuals subject to various sanctions, as well as identifying associations with organised crime and/or terrorist financing activities. In addition, casinos may wish to do Internet searches in an effort to obtain additional information about a customer.

Where available, and where permitted by domestic law, casinos may wish to:

- Subscribe to a national and/or international reporting agency that provides on-line or telephonic searching of customer identification, which often can provide historical information on customers from other subscribing casinos concerning whether (a) an individual applied for credit; and (b) a customer has any outstanding casino debts..
- Use public on-line database search engines that do not require a subscription.
- Subscribe to such data mining agencies that document criminal records, employers, occupations, asset locations, civil actions such as bankruptcies, liens and judgements, relatives and associates and other relative information.
- Subscribe to organisations that provide searches from various business, government, legal and news sources of documents to check on customers in question as well as provide customers' personal information (e.g. name, date of birth, address, place of birth) from commercial databases".

Within the UK, electronic identification (EID) solutions have developed to a relatively sophisticated level and are generally provided by the credit reference agencies (CRAs) Originally EID measures were mistrusted by law enforcement and the regulators as providing insufficient breadth and depth of checks and were only permitted to be used as a supplement to documentary identification evidence. During the past 5 years however, the EID suppliers have worked closely with the financial sector, law enforcement and the regulators and the outcome has been a range of EID systems that can, in many cases provide a more robust means of verifying identity and confirming that the person on whom the checks are being performed is indeed the applicant customer. It is now widely accepted that EID systems can provide additional safeguards where, as with remote gambling, customers are not met face to face and cannot therefore be checked against photographic identification documents.

The Gambling Commission Guidance acknowledges that *"increasingly casinos will use reliable electronic systems to help with verification"* and provides detailed guidance on its application including the following:

"Some external electronic databases are accessible directly by casinos but it is more likely they will be purchased from an independent third party organisation.

The size of the electronic 'footprint' in relation to the depth, breadth and quality of data and the degree of corroboration of the data supplied by the customer may provide a useful basis for an assessment of the degree of confidence in the product.

A number of commercial agencies which access many data sources are accessible online by operators, and may provide operators with a composite and comprehensive level of electronic verification through a single interface. Such agencies use databases of both positive and negative information, and may also access high-risk alerts that utilise specific data sources to identify high-risk conditions, for example, known identity frauds or inclusion on a sanctions list.

Positive information relating to full name, current address, date of birth) can prove that an individual exists, but some can offer a higher degree of confidence than others. Such information should include data from more robust sources – where an individual has to prove their identity, or address, in some way in order to be included, as opposed to others where no such proof is required.

Negative information includes consideration of lists of individuals known to have committed fraud, including identity fraud, and registers of deceased persons. Checking against such information may be appropriate where other factors suggest an increased risk of impersonation fraud"

Where EID systems are to be used, an operator is required to be satisfied that the data provider is "extensive reliable and accurate". An operator must also ensure that the process of electronic verification meets the standard level of confirmation that has been laid down by legislation and the regulators before it can be relied upon. In respect of the UK this means:

- One match on an individual's full name and current address, and
- A second match on an individual's full name and either his current address or his date of birth.

Operators are required to understand the depth and breadth of the information accessed and that they understand the basis of the system they use, including any scoring system.

5.1.3.5 Application of enhanced due diligence

The Gibraltar Regulatory Authority currently proposes to require operators to apply enhanced due diligence to all remote gambling customers. Enhanced due diligence in this respect includes undertaking an additional ID check or ensuring that payments from or to the customer are from/to a bank account in the customers name. This proposal will be consistent with the requirement within the Directive for additional identification measures to be applied to non-face to face customers in recognition of the higher risk they pose. However, this is not currently a requirement in other jurisdictions.

Under international standards, enhanced due diligence must be applied to all politically exposed persons (PEPs) because of their added exposure to corruption. This has proved to be a difficult requirement for all financial and non financial companies. The UK Gambling Commission Guidance provides the following helpful advice on how this might be achieved:

"*Establishing whether individuals are PEPs is not always straightforward and can present difficulties. Where operators need to carry out specific checks, they may be able to rely on an internet search engine, or consult relevant reports and*

databases on corruption risk published by specialised national, international, non-governmental and commercial organisations. Resources such as the Transparency International Corruption Perceptions Index, which ranks approximately 150 countries according to their perceived level of corruption, may be helpful in terms of assessing the risk. If there is a need to conduct more thorough checks, or if there is a high likelihood of an operator having PEPs for customers, subscription to a specialist PEP database may be the only adequate risk mitigation tool.

New and existing customers may not initially meet the definition of a PEP, but that position may change over time. Equally, individuals who are initially identified as PEPs may cease to be PEPs, e.g. if thy change their job or retire. The operator should, as far as practicable, be alert to public information related to possible changes in the status of its customers with regard to political exposure.

Although under the definition of a PEP an individual ceases to be so regarded after he has left office for one year, operators are encouraged to apply a risk-based approach in determining whether or when they should cease carrying out appropriately enhanced monitoring of transactions. In many cases, a longer period might be appropriate in order to ensure that the higher risks associated with the individual's previous position have adequately abated.

Each operator's policies and procedures should cover when and how customers will be checked for PEP status".

5.1.3.6 Controls for higher risk situations

The FATF Guidance states that the measures and controls to mitigate higher risk should include:

- Increased awareness and monitoring by casinos of higher risk customers and transactions across each business.
- Escalation for approval of an accountholder relationship with a higher risk customer.
- Increased levels of due diligence e.g. on PEPs. These checks include obtaining information about the individual PEPs business or status, and their source of income in accordance with a country's legal and regulatory requirements. Senior management approval must also be obtained before a casino can do business with a PEP

Implementing controls for higher risk situations can often create perceived problems for senior management who are anxious to ensure that customers are not made to feel that they are automatically being treated as criminals. The following guidance provided by the Alderney Commission is valuable in such circumstances:

"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 funding or terrorism as well as potentially preventing customer details from being used fraudulently".

5.1.3.7 Application of CDD to existing customers

Under the FATF recommendations and the Directive, operators are required to apply CDD to existing customers taking a risk-based approach.

The Gibraltar proposals handle this in the following way:

"*The Commissioner believes that the known reputation and standing of an existing customer should be taken into account when assessing their risk and any further measures to be applied. This means that whilst identified customers with consistent and established accounts are not exempt from ongoing due diligence procedures, priority should be given to those who are less well established, or whose pattern of gambling or spending profile is outside the expected parameters".*

The UK Gambling Commission Guidance suggests the application of trigger events for updating CDD information relating to existing customers:

"*A trigger event for refreshing and extending CDD may be if a customer returns to a casino after a period of non-attendance. Refreshing information about existing customers will ensure that matters such as change of address, or a customer being appointed into a role which attracts PEP status, will be picked up. Keeping information up to date is also a requirement under the Data Protection Act. How these issues will be dealt with in practice should be covered in a casino's policies and procedures".*

In respect of transfers between customers, the Alderney Commission Guidance provides the following advice:

"*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. 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".*

The Alderney Commission guidance also provides the following advice to operators for reducing their money laundering risks through the banking/payment methods used:

"Banking methods include media such as credit cards, wire transfers and cheques, and other ewallet solutions for making deposits into and withdrawals from a player's eGambing account. 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 reduced by ensuring that withdrawals are made to the same credit/debit card or account as the original deposit came from. Those licensees who make use of alternative deposit or withdrawal measures (such as third party payment processors) should be aware that this increases the risk of money laundering and their business risk assessments should address this factor."

5.1.4 Monitoring of customers and transactions

Monitoring customers and their gambling activities is essential to ensure effective application of AML/CFT policies, procedures, internal controls and automated systems. Casinos are also likely to undertake monitoring for other reasons, including their commercial exposure.

With regard to Internet casinos, Paragraphs 128-130`of the FATF Guidance provide the following advice:

"Checks may be made on the location of the computer used when casino accounts are opened, or during gambling, including IP checks (in that Internet Service Providers can elaborate on IP addresses and traffic route) IP addresses provide information about the country where the computer being used is located

It may be helpful to cross reference IP number information about jurisdictions with i) personal data provided by the player and the data provided by the Internet service provider; ii) the information the customer provides about their postal address and iii) if payment is made to the casino from a financial institution account the country where the financial institution account is held, which may be ascertainable from a BIN check.

Internet casinos are dependent upon IT systems. These IT systems should be adapted to ensure accurate monitoring of accounts and customers and to ensure that adequate records are kept and retained. Decisions may need to be made about the necessary level of details of the transaction records which are retained. A risk-based approach cannot solely rely on IT, there must also be an element of human supervision and staff levels should be proportionate to risk levels".

The UK Gambling Commission Guidance indicates that drop/win data needs to be maintained to ensure that occasional transactions can be monitored to determine when they are linked and to create a rolling 5 year history of each customer with whom there is a business relationship.

The Guidance also advises that:

"*Ongoing monitoring of business relationships is a requirement for casino operators and includes scrutiny of transactions undertaken throughout the course of a relationship (including where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, his business and risk profile"*

"Casinos are expected to approach this requirement on a risk basis. Dependent on how frequently a casino forms ´business relationships, it may be good practice to apply ongoing monitoring more widely. Regular players should be the subject of closer scrutiny and their level of play should be assessed with reference to the information already known about them, and where necessary, additional information must be collected and retained about the source of their funds".

"*Monitoring customer activity should be carried out using a risk-based approach, with higher risk customers being subjected to an appropriate frequency and depth of scrutiny, which is likely to be greater than may be appropriate for lower risk customers"*

There is a requirement arising out of the UK Regulations that ongoing monitoring must be undertaken for a relationship with a PEP.

The Gibraltar Consultation Document for a proposed Code of Practice states that in respect of "Ongoing due diligence (Ongoing Monitoring)":

"*Licenceholders must be alert to significant changes in the status or practices around customers, games, states or transaction methods. Consequently, all due diligence should be recognised by licence holders as a dynamic process, meaning new and continuing customers should be subject to periodic but proportionate and documented reviews (including negative checks) based on their expected and developing gambling profile, especially where that profile changes substantially or appears unconventional. All information arising from this process should be recorded and retained."*

The most focussed and comprehensive guidance in respect of monitoring for Internet gambling operators is contained in the guidance provided by the Alderney Gambling Control Commission.

"*Licensees are required to monitor the relationships they have with their customers. This must be ongoing and effective This monitoring can have an impact upon the risk profiles that might be assigned to customers. 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".*

Licensees are required to monitor:

- *The information they hold, including identification data*
- *Customers' financial habits*
- *Customer's gambling habits*
- *Transactions, in particularly those that are:*
- *complex*
- *large and unusual*
- *part of an unusual pattern,*

"The ICS (Internal Control System) will need to explain what monitoring will take place 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 customer's individual risk profile".*

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 sensible basis regardless of whether or not the customer relationship has been assessed as high risk."

5.1.5 Suspicious activity reporting

The requirement to report knowledge or suspicion of money laundering is a mandatory one falling on all operators and their staff. In accordance with the

FATF Recommendations and the Third European Directive the subjective test of suspicion has also been supplemented by an objective "negligence" test requiring that reports be made where there are reasonable grounds to suspect money laundering or terrorist financing.

In some countries, such as the UK, failure to report in itself is a criminal offence carrying with it a possible prison sentence (2 years in respect of the UK). It is also an offence to continue with a suspicious transaction without the consent of the financial intelligence unit. Within the UK (but not generally within other jurisdictions) there is a prescribed statutory period within which law enforcement must provide or withhold consent.

Reporting to a nominated officer provides a legal defence for employees against a charge of assisting etc. where they know or suspect, including where there are reasonable grounds to suspect, money laundering or terrorist activity.

The UK Gambling Commission provides the following guidance for operators:

"In order to provide a framework within which suspicion reports may be raised and considered:

- *Each operator must ensure that any member of staff reports to the operator's nominated officer where they have grounds for knowledge or suspicion that a person or customer is engaged in money laundering or terrorist financing.*
- *The operator's nominated officer must consider each such report, and determine whether it gives grounds for knowledge or suspicion".*

"If the nominated officer determines that a report does give rise to grounds for knowledge or suspicion, he must report the matter to SOCA. Under POCA, the nominated officer is required to make a report to SOCA as soon as is practicable if he has grounds for suspicion that another person, whether or not a customer, is engaged in money laundering. Under the Terrorism Act, similar conditions apply in relation to disclosure where there are grounds for suspicion of terrorist financing.

"The operator's nominated officer must consider each report and determine whether it gives rise to grounds for knowledge or suspicion. The operator must permit the nominated officer to have access to any information, including CDD information, in the operator's possession that could be relevant. The nominated officer may also require further information to be obtained, from the customer if necessary. Any approach to the customer, should be made sensitively to minimise the risk of alerting the customer or an intermediary that a disclosure to SOCA may be being considered."

If the nominated officer decides not to make a report to SOCA, the reasons for not doing so should be clearly documented or recorded electronically and retained

The operator's nominated officer must report to SOCA any transaction or activity that, after his evaluation, he knows or suspects, or has reasonable grounds to know or suspect, may be linked to money laundering. Such reports must be made as reasonably practicable after the information comes to the nominated officer."

In respect of cases where a significant suspicion arises during gambling activity, the Gibraltar proposed Code of Practice provides the following useful advice:

"There may be cases of significant internal reports being made orally or technically whilst gambling is taking place or bets are pending. In these circumstances, the nominated manager must consider whether to allow the gambling to continue or intervene. Whilst different considerations will apply in respect of land based and remote facilities (where any winnings or losses are generally frozen for a predetermined period) unless highly unusual and excessive gambling is taking place it will not, normally, be necessary to suspend the gambling. It will, however, be for the nominated manager to apply experience and judgement in these circumstances with a view to protecting the licence holder by not allowing the situation to escalate and knowingly facilitate or permit money laundering".

5.1.6 Vetting, awareness and training

Vetting of employees who are in sensitive roles is a requirement of the international standards, although it is not specifically referred to in the FATF Guidance for Casinos. Neither is it covered in the UK Regulations. However, many jurisdictions do include such a requirement and the Alderney Gambling Commission Guidance covers it in the following terms:

"Employees, including relevant staff of third party providers, with access to the eGambling system and/or customer data and funds present a considerable risk. Accordingly licenses should endeavour to identify staff positions that present a high risk and introduce screening processes during the recruitment of employees filling these positions".

It is vital for the success of any AML/CFT controls that employees within the financial and non-financial businesses covered by the relevant regulations are fully aware of their obligations and responsibilities, and those of their employer, and that they are trained in how to recognise and report suspected money laundering and terrorist financing activity. As stated by the UK Gambling Commission guidance. *"The effective application of even the best designed control systems can be quickly compromised if the staff applying the systems are not adequately trained. The effectiveness of the training will therefore be important to the success of the operator's strategy."*

In the UK a failure on the part of an operator to provide adequate training that is tailored to the day to day activities of the employee will provide a defence if they should fail to recognise and report their suspicions. If such a defence were to succeed, the employer could be prosecuted for a breach of the relevant regulations.

The FATF guidance advises in paragraph 132 that "for Internet casinos, such training should be addressed to internet technology staff".

The Third European Directive covers the requirements of the international standards in the following terms:

"Member States shall require that the institutions and persons covered by this Directive take appropriate measures so that relevant employees are aware of the provisions in force on the basis of this Directive.

These measures shall include participation of their relevant employees in special ongoing training programmes to help them recognise operations which may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases".

"Member States shall ensure that the institutions and persons covered by this Directive have access to up-to-date information on the practices of money launderers and terrorist financers and on indications leading to the recognition of suspicious transactions.

The UK Gambling Commission advises that:

"*The content of any training, the regularity of training and the assessment of competence following training are matters for each operator to assess and decide in the light of the money laundering risks they identify. The Commission will expect such issues to be covered in each operator's policies and procedures*

Operators should also take reasonable steps to ensure that relevant employees are aware of:

- *their responsibilities under the operator's policies and procedures for the prevention of money laundering and terrorist financing,*
- *the money laundering and terrorist financing risks faced by an operator and each of its casino premises,*
- *the operator's procedures for managing those risks;*
- *the identity and responsibilities of the nominated officer; and*
- *the potential effect of a breach upon the operator and upon its employees".*

5.1.7 Record keeping

Record keeping is an important requirement as it provides an audit trail for law enforcement in the event that a financial investigation is necessary. Because it is not possible to detect all instances of suspected money laundering or terrorist activity, provision of historical records is often the biggest part that an operator can play within an AML/CFT regime.

The Third European directive sets out the generic basic record keeping requirements in the following terms:

Member States shall require the institutions and persons covered by this Directive to keep the following documents and information for use in any investigation into, or analysis of, possible money laundering or terrorist financing by the FIU or other competent authorities in accordance with national law:

(a) in the case of the customer due diligence, a copy or the references of the evidence required, for a period of at least five years after the business relationship with the customer has ended,

(b) in the case of business relationships and transactions, the supporting evidence and records, consisting of the original documents or copies admissible in court proceedings under the applicable national legislation for a period of at least five years following the carrying-out of the transactions or the end of the business relationship.

The record keeping requirements within most jurisdictions have now progressed beyond the basic standards. The UK Gambling Commission guidance provides the following example of what is currently required:

"*The operator's record keeping policy and procedures should cover records in the following areas:*

- *Details of how compliance has been monitored by the nominated officer.*
- *Delegation of AML/CFT tasks by the nominated officer.*

- *Nominated officer reports to senior management.*
- *Information not acted upon by the nominated officer, with reasoning why no further action was taken.*
- *Customer identification and verification information.*
- *Supporting records in respect of business relationships or occasional transactions.*
- *Staff training records.*
- *Internal and external suspicious activity reports*
- *Contact between the nominated officer and law enforcement or SOCA, including records connected to appropriate consent.*

5.2 Industry practice to manage and mitigate the perceived AML/CFT risks vulnerabilities

5.2.1 Vulnerability levels

Whilst the absence of cases and examples of money laundering and terrorist financing within the remote gambling industry appear to indicate that the risks are low, there are three possible vulnerability levels that need to be managed and mitigated:

1. When payment for the gambling activity is drawn from a bank account or credit card in the customer's name and winnings/funds can only be returned back to that account, the risks are at their lowest. Under such circumstances, the money laundering loop has been closed. Indeed were in not for the fact that customers are being dealt with non-face to face, the activity would qualify for simplified due diligence under the various money laundering regulations.
2. When deposits are being accepted and payments returned via an unregulated payment service provider or from an account that cannot be confirmed as being in the name of the customer there is a standard level of risk and controls should reflect this level of risk. These will generally be the controls that guard against fraud including the fraudulent use of credit cards and ID theft.
3. The highest level of risk is present only in a relatively small number of cases when cash is being accepted in payment or when the funds are being accepted through an e-payment service provider that accepts cash. In recognition of the additional risks posed by cash, Malta's Remote Gambling Regulations prohibit the acceptance of cash.

5.2.2 Measures in place to address the risks and vulnerabilities

In order to manage and mitigate money laundering and terrorist financing risks and the vulnerabilities set out in 5.2.1, the remote gambling industry has put in place the following procedures, systems and controls.

5.2.2.1 The acceptance of cash

Only a minority of operators are part of groups that have land-based establishments where cash can be accepted as payment for online gambling.

Where this is the case, all shop-based transactions involving the funding of online accounts are recorded and will show the type of payment made by the customer e.g. cash, bankers' draft, cheque, card transfer. Cash converted from electronic form or to electronic form is therefore well defined in the gambling accounting process and is therefore traceable and attributable. Consequently the records create an audit trail against which to monitor the source, destination and nature of all funds. This audit trail will also be supported and strengthened in most cases by the use of digital CCTV imagery to record the person making the transaction. Identification evidence is required for shop based withdrawals.

5.2.2.2 Payment mechanisms

All approved pre-paid card transactions are carried out by the money services providers who are required to be regulated and licensed. Some online payment systems e.g. Paypal and MoneyBookers add an extra layer of customer due diligence and integrity to the transaction.

Some or all of the following domestic and international payment mechanisms are used by operators within the survey.

- E-wallets e.g. MoneyBookers, PayPal, WebMoney, neteller, click2pay, click&buy
- Quick cash vouchers (enable customers to deposit and withdraw cash in an operator's land-based betting shops, in exchange for a voucher they can use on their online account)
- Pre-paid gift debit cards and virtual card schemes e.g. Entropay
- Cheques and bankers drafts
- BPay and PoliPayment (Asian)
- Wire transfers (cash (via ADI and bank and account transfer)
- Western Union
- BACS
- Debit and credit cards.

Significant fraud prevention measures have been put in place by Operators to guard against fraudulent payment mechanisms. The close linking of fraud prevention and AML/CFT measures across the industry enables the fraudulent use of stolen credit cards and ID theft to be quickly detected. For example, historic measurement of the use of fraudulently obtained cards within the remote gambling sector is lower than other online businesses with the loss, if measured by charge-backs, being less than 1% of the total funds deposited.

5.2.2.3 AML/CFT procedural strengths

MHA evidenced a strong commitment to prevent and detect money laundering and terrorist financing, to comply with the various legislative and regulatory requirements and to co-operate with the authorities.

As was the case with the majority of retail banks in the early 1990s, money laundering prevention has become an additional focus of the remote gambling operators' Security Departments and this has resulted in a highly practical approach rather than a principal focus of mere compliance with the Regulations.

The Security Departments are primarily manned by ex-police officers and the MLRO is generally a member of the security team. Because security and fraud prevention are vital aspects of remote gambling operations, the MLRO or Head of Security has direct access to senior management.

As would be expected from the different organisations within the RBA, not all have taken the same measures to reach compliance with their AML/CFT obligations. However the following examples were generally evidenced.

5.2.2.4 Policies and procedures

As required by various regulations, codes and guidance, operators use industry guidance as the basis for their own tailored and documented policies and procedures. The guidance is then adapted to reflect the operator's risk-based strategy and approach, the nature of the operator's business and its customer base.

Whilst all aspects of the UK Money Laundering Regulations and Gambling Commission Guidance are generally covered within the policies and procedures of the operators, as is the case with other parts of the AML regulated sector, the depth and tailoring of the content varies. Also in line with other parts of the regulated sector the extent, nature and quality of staff training varies.

5.2.2.5 Customer identification

The requirement across the industry to register all customers, regardless of whether the gambling facility is used only once a year (e.g. to bet on the Grand National) or more regularly, provides an automatic start point for customer identification. This is combined with the requirement for over-18 age verification to guard against underage gambling. Whilst age verification is not an AML requirement, date of birth is an important aspect of identity and vital for law enforcement in an investigation.

The need to guard against fraudulent activity generally causes operators to undertake diligent procedures to verify identity. The primary use of electronic identification facilities where they are available strengthens the process through the depth and breadth of the checks undertaken.

Proprietary software is generally used to undertake sanctions checks.

5.2.2.6 Activity monitoring

As a result of the objective to promote responsible gambling and the to guard against the risk of fraud, all customer activity is recorded and monitored, often on-line real time using a range of sophisticated security systems and resources, These enable suspicious transactions, gambling abuse, irregular play and disproportionate gaming to be identified and for play to be suspended where necessary through intervention by security and audit teams.

A range of internet search engines is used to examine betting patterns and behaviours and to provide lifestyle intelligence checks on high spenders. Disproportionate gambling when measured against the level of funds deposited and withdrawn by customers through their accounts is closely monitored.

All accounts which have a single common feature are linked permitting customers with multiple accounts to be identified.

5.2.2.7 Transfers between customers

All inter-account funds transfers are recorded and accounted for to maintain an audit trail. However, the beneficial owner of bets and wagers is not determined and therefore any bet or wager may have singular or plural beneficiaries which may require the transfer of funds to be made legitimately between customers in order to share the profit or loss.

Transfers between players can be identified, authorised and controlled. The same process can identify unusual and suspicious transaction that might indicate money laundering or related criminal activities. In addition, there are extensive procedures in place to detect chip dumping i.e. the fraudulent extraction of funds from a bank account followed by deliberate loss of funds to an accomplice across the poker table whose "winnings" are then paid out by the credit card company.

Some operators require documentary evidence to confirm that funds are being paid from an account in the customer's name and the application of enhanced due diligence when funds cannot be returned to where they originated from. Transfers between customers are often only possible through the operator.

5.2.2.8 Compliance monitoring

A variety of measures are used to monitor compliance with the AML/CFT and fraud prevention requirements. This can range from the presence of a nominated officer and/or MLRO in each separate jurisdiction to implementing a programme of compliance review visits by the MLRO. Monitoring the receipt of court orders and equivalent requests highlights where there are gaps in policies and procedures or whether additional training is necessary.

In some cases there is an acknowledgment in documented policies and procedures that the Board of Directors is ultimately responsible for compliance with the AML/CFT requirements of an operator

5.2.3 Recommendations for the industry

It is generally acknowledged that international standards and regulations drawn up for application by the financial sector cannot easily be applied to non-financial sector businesses. However, there are a number of areas where the industry could work together to provide a practical basis for compliance that works specifically for the remote gambling industry.

5.2.3.1 Identification and verification requirements

There is a general absence of knowledge that because remote gambling customers are non-face to face, additional due diligence measures are required by the international standards and regulations. Standard verification procedures using EID measures could be drawn up that remove any competitive advantage or disadvantage across the industry. Discussions could usefully be held with the EID providers to tailor the facilities to the specific needs of the industry where necessary. Where EID is not available, standardisation of practice would also be an advantage.

In particular, operators need advice on the type of enhanced due diligence that is necessary to manage the additional non-face to face risks and the extent of information that should be sought for players who present a higher level of risk. For example, the extent of additional information that can be reasonably sought

in respect of source of funds/occupation within the confines of a recreational activity needs to be explored and, if necessary, discussed with regulators and law enforcement agencies. Without such information on the economic background of a customer, it is difficult to determine when that customer is either gambling with funds that might not have been legitimately earned or with funds supplied by a third party.

It is essential requirement of the Directive and Regulations that operators know whose funds they are handling and verify the identity of that person when CDD measures are required. However, this provides significant problems for the industry. Discussions again need to be held with regulators and law enforcement to examine the extent to which this is necessary in all cases and to identify the measures that can be taken in higher risk circumstances.

5.2.3.2 Monitoring for suspicious activity

The application of strong fraud prevention and detection mechanisms across the industry provides both strengths and weaknesses. There is a tendency to over-investigate suspicious activity when it has occurred, but an absence of general consensus as to the prevention mechanisms that might be put in place to guard against money laundering and terrorist financing. Whilst it is necessary to examine all information that is available within the operator that might confirm or set aside an internal suspicion report, it is not the responsibility of the regulated sector to investigate suspicions and prove or disprove them. Fraud and MLRO teams cannot have access to the investigations being conducted by the law enforcement agencies and timely disclosure is vital as the information will often result in providing important additional intelligence.

Because of the close links with law enforcement, there is often a tendency to breach customer confidentiality and to provide information to investigating agencies merely on request, or to respond without question to the extensive use by law enforcement of Data Protection Act requests in place of POCA production orders. The misuse of DPA requests will render the information inadmissible and productions orders provide protection for the operator as it is this evidence that is used in court in support of a prosecution case.

5.2.3.3 Procedures for reporting suspicious activity

Some operators advise within policies and procedures that the identification of suspicious activity is primarily the responsibility of fraud and security teams. However, the legislation places the responsibility for identifying suspicious transactions and activity on individual members of staff. In the UK there is an offence of failing to report which can be committed by individual employees where there are reasonable grounds to suspect. If employees believe it is not their role to identify suspicions, they will be unlikely to exercise sufficient vigilance.

Internal SARs are not always documented by operators. It should be recognised that the general requirement to document internal SARs provides protection for an employee if a SAR that is set aside by a nominated officer is later found to have been a be a valid disclosure for the investigating agencies. Many money laundering and terrorist financing investigations are undertaken several years after the act that may have originally been considered by an employee to be suspicious. The existence of an objective test means that employees can be called to account at a later stage on the grounds that there were reasonable grounds to suspect money laundering based on the information that was

available to them at the time. The absence of any evidence that they reported their suspicions removes their defence.

6 Conclusions

6.1 Susceptibility of remote gambling to money laundering and terrorist financing

Whilst no service sector can be immune from the attention of criminals, there appears to be little evidence to support the view that remote gambling has, to date being particularly susceptible to money laundering and terrorist financing. The United States has published the results of official government studies concluding that online gambling is not a likely accessible avenue for money laundering because:

- the identities of the gamblers are known;
- the financial transactions between the bettors and operators are all in electronic format; and
- all of the wagering is recorded.

Whilst there is regular evidence of cash-based laundering through land-based gambling operations[8], many of which are US-based, which has led to Casinos being included within the AML/CFT regulated sector, there does not appear to be similar evidence relating to remote gambling. The only case is that of Tsouli/Al-Daour in July 2007 which was credit card, not cash, related[9]. The case involved cards issued by a number of regulated payment service providers and related to a major money laundering operation using a variety of different products and services. Unfortunately, because this was related to terrorism, significant publicity was given to the case which was hailed as the world's first cyber-terrorism trial. The fact that a number of attempts to launder through a remote gambling site were unsuccessful in that they were identified, SARs submitted and the accounts were closed, was not reported in the media.

6.2 Gaining reputation through regulation and co-operation

There is evidence that some regulators are significantly stronger than others and a view amongst some operators that the regulators within the different jurisdictions do not communicate with each other. Whilst the key factors in choosing a licensing jurisdiction primarily relate to financial viability and tax burdens, as the regulations in some jurisdictions start to bite there is a danger that some operators may use 'regulatory arbitrage' to determine the location of their operation, thereby driving international standards downwards.

[8] www.casinowatch.org/crime/moneylaundering

[9] Al-Daour allegedly laundered money through online gambling sites, using accounts set up with stolen credit card number and victims' identities. He and other members of the group conducted 350 transactions at 43 different online gambling sites, using more than 130 compromised credit card accounts. Winnings were withdrawn and transferred to online bank accounts the men controlled

Nevertheless, as with the banking and trust sectors, some operators will undoubtedly seek to locate their operations in the strongest regulated jurisdictions to guard against reputational risk.

The Chief Executive of the Alderney Gambling Control Commission is clearly of the view that regulators, operators and trade bodies within the industry can and must play a valuable role in establishing common standards. In an article published in a 2008 edition of eGaming Review[10], Andre Wilsenach made the following observations on the challenges facing remote gambling regulators following the advent of community games.

"Players owned by operators in one jurisdiction are now exported to other jurisdictions where the poker/bingo room is based. In today's open systems, operators offer players a broad range of products often based in multiple jurisdictions, implying that the player is being exported/imported across borders all the time. This raises a number of regulatory questions:

- If the game no longer takes place in my jurisdiction, what is it that I am regulating?
- Should I allow the players of my licensee to be 'exported' without having any knowledge of the background and operating practices of the entity that offers the game?
- How do I ensure that the game offered elsewhere is fair, secure and auditable?
- What benefits does it have to require that the gambling and related server be in my jurisdiction and is it in view of the developments in the industry still logical to require operators to base their servers in my jurisdiction.

The above scenario requires a network of cross border relationships between operators, platform providers and content providers. Conversely, if I am expected to deal with the public's concern in respect of fairness and player protection, I need to have a certain level of comfort about what is on offer to the player registered with an Alderney licensee and how it is being offered. This raises the clear and urgent need for international cooperation at regulatory level and the adoption of common standards internationally."

The article goes on to advise that the International Association of Gaming Regulators has been working on the development of common standards and guidelines to deal with the some if not all of the questions that Andre Wilsenach has highlighted. How the remote gambling industry reacts to the draft standards when they are released will provide an indication of whether operators and regulators are truly ready for the same level of international cooperation that exists amongst the financial sector regulators.

6.3 Industry practice

The application of money laundering and terrorist financing requirements is relatively new to the remote gambling industry. For the period 1990 to 2003, AML/CFT obligations were imposed only on the financial sector. Being covered by such obligations and recommendations from the outset enabled the financial sector to influence the evolution of best practice and permitted financial sector businesses to adapt their own operations and procedures over a number of years to meet the evolving requirements. Significant experience was gained

[10] From an article in EGaming Review "Across the Border" by Andre Wilsenach, Chief Executive of the Alderney Gambling Control Commission, published by Pageant Media © 2008

along the way and the regulators, law enforcement and businesses themselves were able to learn from their mistakes.

Whilst the non-financial sector businesses and professions that are now covered by the requirements are able to benefit from the experience gained by the financial sector, they have entered the arena at an advanced stage in the evolution of AML/CFT requirements. It has also resulted in measures that were designed for the heavily regulated and significantly vulnerable financial services sector being imposed on a wide range of non-financial sector businesses. Consequently there has been the need across the remote gambling industry for a significant learning curve within a relatively short space of time. In many cases there has also been the need for a significant cultural change to deal with regulatory "pinch points".

The remote gambling industry appears to have risen to the challenge presented by the new requirements and demonstrated a commitment to making them work that was not always evident within the financial sector. The passage has perhaps been helped by the commitment the gambling industry has displayed in promoting responsible gambling. Whilst there are some gaps in the initial customer due diligence programmes, these are generally countered by the extensive monitoring procedures that are put in place to guard against fraud, including fraudulent use of stolen credit cards, and criminal misuse of operators' systems and facilities.

However, as was the case with the financial sector, there is some way to go before the industry can demonstrate the clear commitment of senior management within all operators.

The Remote Gambling Industry has a distinct advantage in that it is truly multi-jurisdictional and operators can have the advantage of drawing from best practice requirements from all relevant jurisdictions. However, it is important that operators share good practice within their peer group and work with the Regulators to ensure that Regulations and Guidance is set at a consistently high standard. This is particularly important in respect of risk assessment strategies, CDD, monitoring, awareness and training. The RGA might consider following in the footsteps of the financial sector trade associations which publish the JMLSG Guidance for the Financial Sector[11] and publish AML/CFT guidance specifically for online gambling, drawing on international best practice for the industry.

6.3.1 The anticipated success of the risk-based approach

A reasonable designed and effectively implemented risk-based approach will provide an appropriate and effective control structure to manage identifiable money laundering and terrorist financing risks. However, it is recognised that regardless of controls, it is not possible to eliminate money through any sector or business and that the controls, policies and procedures in place will not identity and detect all instances of money laundering or terrorist financing.

The FATF Guidance acknowledges that regardless of the strength and effectiveness of AML/CFT controls, criminals will continue to attempt move illicit funds undetected and will, from time to time, succeed. They are more likely to target non-financial sector businesses, including casinos, if other routes become

[11] www.jmlsg.org.uk

more difficult. For this reason casinos may be more or less vulnerable, depending on the effectiveness of the AML/CFT procedures applied in other sectors. A risk-based approach allows casinos to more efficiently and effectively adjust and adapt as new money laundering and terrorist financing methods are identified.

Whilst no amount of legislation, regulation, and private sector practices will deter the most determined criminals with unlimited resources at their disposal, putting barriers in their way is a significant step in the armoury of prevention and detection. Sound regulation and international cooperation within the public sector and effective corporate governance and prevention mechanisms in the private sector have proved to be a sound deterrent in the past. Similar measures for remote gambling will assist in guarding against reputational and operational risks for both regulators and operators. They will also help in the battle to deter, detect and deprive criminals of their ill-gotten gains.

6.4 Legislation v prohibition – promoting responsible practices that guard against money laundering

Whilst the campaign against prohibition and protectionist practices in respect of online gambling is not part of our brief, we believe that our report would not be complete without some comment in respect of this matter.

In August 2007, Professor Peter Collins, Executive Director of the South African National Responsible Gambling Programme (NRGP) presented his submission on remote gambling to the Parliamentary Portfolio Committee responsible for gambling legislation. The question being addressed was whether remote gambling should be prohibited, regulated or left to develop a free market as was the case at the time of the report. The report advised that:

"At present such gambling is illegal in South Africa – although most South Africans appear to be unaware of this. It is not a prohibition which South Africa's law enforcement agencies could reasonably be expected to enforce e.g. by raiding people's homes confiscating their hard drives and ascertaining whether they have been playing poker online. Public opinion would not stand for such an extravagant use of law enforcement resources nor for such draconian infringements of individual liberties.

Thus the main challenge for South African legislators is how to subject this industry to appropriate regulation so as to protect actual and potential African consumers, especially the young and those in danger of doing themselves and those close to them significant harm by gambling too much. It would also be desirable to regulate in such a way that some economic benefits accrue to the general public through various kinds of taxation, investment and employment.

In this respect the challenge now facing the SA government in respect of remote gambling is very similar to that which faced the government in the early nineties with respect to authorising and regulating casinos in circumstances where illegal casinos proliferated in huge numbers in every large city and most medium-sized towns."

The NRGP concluded that they favoured the legalisation of remote gambling for the reasons that it is possible "to use technology to tame technology" and operators can be required to conform to strict codes, regulations and responsible practices.

In respect of the arguments in favour of regulation, an analogy can be drawn with Trust and Corporate Service Providers. Once the regulated traditional financial sector had taken steps to protect itself against significant amounts of

money laundering, the criminals turned their attention to unregulated financial services. Laundering through unregulated trusts and offshore companies became commonplace. As the regulators in Jersey, Guernsey, Isle of Man and Gibraltar tightened their grip, the criminals moved their business to the less-well regulated offshore jurisdictions. Many are still there.

Sue Thornhill and Michael Hyland

Directors, MHA Consulting

June 2009

APPENDIX

1 AML/CFT legislation, regulations and international standards affecting the remote gambling industry

1.1 The Financial Action Task Force Recommendations

The principal international standards relating to the prevention and detection of money laundering and terrorist financing emanate from the Financial Action Task Force (FATF). The FATF recommendations single out the business sectors where there are believed to be the highest risks of money laundering and terrorist financing.

The FATF is an inter-governmental body, bringing together the policy-making power of legal, financial and law enforcement experts of 33 countries. It was founded at the 1989 OECD Economic Summit, as a response by the heads of state of the G-7 nations to the growing problem of money laundering and in recognition that, initially, money laundering and subsequently also terrorist financing, are global problems that require global solutions.

The FATF states its purpose in the following terms[12]:

- To establish and refine global standards for combating money laundering and terrorist financing.
- To foster and monitor countries' implementation of standards.
- To expand the geographical reach and implementation of the FATF standards through a limited increase in membership and by enhanced relationships with FATF-style regional bodies (FSRBs) and non-member countries.
- To identify money laundering and terrorist financing threats.
- To conduct outreach to relevant stakeholders.

FATF first issued its Forty AML Recommendations in 1990 aimed at governments and financial institutions. Together, these Recommendations form a comprehensive regime against money laundering and have been accepted world-wide as one of the more comprehensive bases for tackling money laundering. Following revisions in 1996 and an additional 9 Special Recommendations on Terrorist Financing in 2001, a significantly revised set of 40 recommendations were published in June 2003 which recognised the need for a risk-based approach to the prevention and detection of money laundering and terrorist financing.

These 40+9 recommendations now provide the global standards against which the AML/CFT legislation and strategies of all jurisdictions are assessed, by the FATF itself (for its members) and by the IMF and the World Bank for non-FATF

[12] An overview of the FATF, its work and copies of its recommendations and guidance can be found on the FATF website www.fatf-gafi.org

members. The AML/CFT regimes of all the countries in which the RGA members operate have been assessed against the FATF recommendations and those assessments published.

The FATF recommendations single out the business sectors where there are believed to be the highest risks of money laundering and terrorist financing. This includes remote and non-remote casinos.

1.1.1 FATF RBA Guidance for Casinos

In June 2007 the FATF adopted guidance for public authorities and the financial sector on applying a risk based approach to money laundering and terrorist financing.[13] Following the establishment of a special advisory group drawn from the public and private sectors, the FATF published specific guidance for Casinos in October 2008[14]. The UK Money Laundering Reporting Officer of William Hill in the UK, a member of the RGA, was a member of the FATF Casino Advisory Group and played an active role in drawing up the RBA Guidance for Casinos.

The FATF guidance states that

"Casinos must be subject to a comprehensive regulatory and supervisory regime that ensures they have effectively implemented the necessary AML/CFT measures. An important aspect of such regulation is to ensure the honesty and integrity of casino staff. Special care should be taken to ensure that all staff members are aware of their casino's policy and procedures relating to assisting or facilitating customers to launder money.

As a minimum:

- Casinos should be licensed.
- Competent authorities should take the necessary legal or regulatory measures to prevent criminal or their associates from holding to being the beneficial owner of a significant or controlling interest, holding a management function in, or being an operator of a casino.
- Competent authorities should ensure that casinos are effectively supervised for compliance with requirements to combat money laundering and terrorist financing".

The FATF's specific recommendations for Casinos relating to assessing customer risk and undertaking risk-based customer due diligence (CDD) are set out in Section 6 of this Report.

1.2 European legislation

There are no measures as yet directed towards harmonising and regulating games of chance and gambling in particular. However, arrangements to prevent and detect money laundering and counter terrorist financing (AML/CFT) are prescribed by the European Commission by way of Directives transposed into domestic legislation. The Third European Council Directive on Money

[13] FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing

[14] FATF RBA Guidance for Casinos

Laundering[15] consolidates the First and Second Directives and accommodates the FATF 40 plus 9 recommendations.

Article 2 of the Third Directive includes 'casino activities' as a 'financial business' subject to AML/CFT due diligence procedures. It goes on to refer in Articles 10 to Identification and Verification of the Identity of Casino Customers; in Article 36 to the requirement to licence casinos and in Article 37 to the powers for on-site inspections. Separate references to casinos and the internet are made in the Preamble to the Directive (paragraphs 14 and 39). In Article 13 the Directive describes all non-face to face transactions as presenting a 'higher risk' thereby triggering specific additional measures to verify identity and guard against identity fraud.

All European Member States, including Gibraltar, are obliged to implement Council Directives into their domestic legislation. Whilst The Isle of Man Guernsey (including Alderney) and Jersey are not required to do so, all three Crown Dependencies have brought forward legislation to implement the Money Laundering Directives in order that their finance and professional sectors can operate effectively when undertaking European business.

An overview of the AML/CFT Law and Regulation within the EU Member States, the Isle of Man, Guernsey, Jersey and Antigua is contained in Appendix 1.

Most member states of the EEA have shaped their regulation of both 'bricks and mortar' and remote gambling with explicit reference to the need to prevent crime and money laundering. They have done so in order to justify (in part) erecting barriers to the free movement of gambling services, yet to this extent almost all regulation of the sector purports to be in respect of "anti-money laundering". When the purpose of legislation is primarily economic rather than anti-money laundering, it has been included in this report only where necessary or explanatory. A further tranche of legislation deals with gaming equipment and technical requirements; although this legislation is also intended to prevent crime and by definition money laundering, it lies outside the scope of this report and has therefore been omitted.

In accordance with the international standards and directives, the Gambling industry is subject to regulation and supervision in all of the countries in which the RGA members operate. The principal countries within the EEA and the Crown Dependencies which they are licensed are the United Kingdom, Gibraltar, Malta, Alderney and Italy.

1.3 Regulation of the Remote Gambling Industry within the UK

Following the Gambling Act 2005[16] the British government has put in place stringent regulation of the gambling sector, including operators of remote gambling offering casino, bingo and machine-style gaming. Regulation is overseen by the Gambling Commission. Organisations and individuals that provide facilities for betting or gaming remotely require a licence to operate. The objective is to ensure that the public have the choice of gambling on sites that meet the high standards required by the Commission. Customers are able to

[15] Directive 2005/60/EC on the Prevention of Money Laundering and Terrorist Financing

[16] http://www.opsi.gov.uk/acts/acts2005/en/ukpgaen_20050019_en_1

ensure that operators are licensed by a statement on their website which includes their Commission operating licence number and a link to the Commission's website.

There are two types of licence required by remote operators:

i) Operating licences are required by those that provide facilities for gambling in Britain

ii) Personal licences are required by individuals in certain management positions, except for those organisations categorised as small-scale operators.

Licensees are required to comply with the Commission's remote gambling software technical standards and to have their products tested in line with the Commission's requirements for testing.

The Commission's Licence Conditions and Codes of Practice (LCCP) set out the rules which operators must observe to meet the following licensing objectives:

- Keeping crime out of gambling;
- Ensuring that gambling is fair and open; and
- Protecting children and other vulnerable people from being harmed or exploited by gambling.

Following extensive consultation, new licence conditions and codes of practice came into effect on 1 January 2009. A provision within the LCCP requires casino operators to act in accordance with the guidance that the Commission has issued on the Money Laundering Regulations 2007.

1.3.1 The UK Money Laundering Legislation, Regulations 2007 and the Gambling Commission Guidance

The current legislation framework for meeting the UK's anti-money laundering strategy is formed by:

- The Proceeds of Crime Act 2002 (POCA), as amended by the Serious Organised Crime and Police Act 2005. POCA sets out the principal money laundering offences and defences that apply to all UK persons and businesses. In addition POCA places additional requirements on financial and professional sector firms, and other businesses such as casinos to report their suspicions of money laundering and terrorist financing to the Serious Organised Crime Agency through a specifically appointed Nominated Officer.
- The Terrorism Act 2000, as amended by the Anti-Terrorism Crime and Security Act 2001 and the Counter-Terrorism Act 2008, creates a number of criminal offences, some of which are specific to firms covered by the Money laundering Regulations, which includes Casinos.
- The Money Laundering Regulations 2007 which implements the Third European Directive and sets out the scope of the 'regulated sector' and the preventative measures they must take. It also contains the supervisory powers and registration requirements for the non-financial sector.

1.3.2 The requirements of the Regulations

The Money Laundering Regulations 2007 came into effect on 15th December 2007, replacing the Money Laundering Regulations 2003. Both remote and land-based casinos fall within their scope. Regulation 20 requires that regulated financial and non-financial businesses falling within its scope, including Casino operators must establish and maintain appropriate documented risk-sensitive policies and procedures relating to:

- Customer due diligence measures and ongoing monitoring, including procedures to determine whether a customer is a politically exposed person.
- Reporting to a nominated officer where there is knowledge, suspicion, or reasonable grounds to suspect that a person is engaged in money laundering or terrorist financing
- Record keeping.
- Internal controls, including policies and procedures which take additional measures for products and transactions which might favour anonymity.
- Risk assessment and management.
- The monitoring and management of compliance with, and communication of, such policies and procedures
- Policies and procedures which provide for the identification and scrutiny of:
  - complex or unusually large transactions;
  - unusual patterns of transactions which have no apparent economic or visible lawful purpose; and
  - any other activity which may be related to money laundering or terrorist financing.
- Awareness and training of management and staff.

Failure to comply with any of the requirements of the Regulations constitutes an offence punishable by up to two years' imprisonment (for the directors or senior managers) or a fine, or both.

1.3.3 The Gambling Commission Guidance

Money laundering is a complex subject and the Money Laundering Regulations seek only to provide a statutory framework from which individual business sectors can develop their detailed approach to preventing money laundering and terrorist financing through specific industry guidance.

The Gambling Commission is the designated supervisory authority for Casinos and as such the Commission has produced guidance to assist casino operators to meet the requirements of the law and is workable in remote and non-remote casinos.

The Gambling Commission states[17] that the purpose of its guidance is to:

- Outline the full legal framework for anti-money laundering and counter terrorist financing requirements and systems across the remote and non-remote casino sector.
- Interpret the requirements of the relevant laws and regulations, and how they might be implemented in practice.
- Indicate good industry practice in AML/CFT procedures through a proportionate risk-based approach.
- Assist operators to design and implement the policies and procedures necessary to mitigate the risks of being used in connection with money laundering and the financing of terrorism.

1.3.3.1 Status of the Gambling Commission guidance

POCA requires a court to take account of industry guidance that has been approved by a Treasury Minister when considering whether a person within the regulated sector has committed a breach of the Regulations or the offence under POCA of failing to report their knowledge, suspicion, or where there were reasonable grounds to know or suspect that another person is laundering the proceeds of crime. Similarly the Terrorism Act requires a court to take account of such approved industry guidance when considering whether a person has failed to report under that Act.

The Gambling Commission advises that the guidance provides a sound basis for operators to meet their legislative and regulatory obligations when tailored by operators to their particular business risk profile. Departures from the guidance, and the rationale for doing so, must be documented and may have to be justified to the Commission or the courts.

The commission is not a 'designated prosecution authority' under the Regulations and therefore does has not have powers to take action against Casino operators that breach the regulations. However, the Commission has revised both remote and non-remote casino operating licences to state that compliance with the guidance is a licensing requirement.

1.4 Regulation of remote gambling within Gibraltar

All gaming operations in Gibraltar require licensing under the Gambling Act 2005. Remote Gambling licences, including for telephone and internet betting, are issued by the Licensing Authority.

The Gibraltar Regulatory Authority is the Gambling Commissioner under the provisions of the Gambling Act 2005. The Act grants the Gambling Commissioner powers to ensure that licensees conduct their operations in accordance with their licenses and in such a manner as to maintain the good reputation of Gibraltar.

The Licensing Authority states[18] that will only consider licensing blue chip companies with:

[17] Gambling Commission: The prevention of Money Laundering and Combating the Financing of Terrorism – Guidance for remote and non-remote casinos December 2007

- a proven track record in gaming;
- licensed in a reputable jurisdiction;
- of good standing; and
- with a realistic business plan.

As at 1 September 2008 there were twenty licensed operators.

The licences are issued on the basis that the advertising and promotion of gambling activities can only be directed to citizens of jurisdictions in which it is not illegal for such activities to be undertaken and that the licensee will not provide gambling activities to any person where the provision of such services by the licensee would be illegal under the applicable law.

Licensees must at all times be controlled and managed from Gibraltar. All relevant bank accounts, credit card merchant accounts and processing of customer funds and transactions must also be undertaken in Gibraltar.

A requirement of the licence is that the licensee must comply fully with all obligations under the Gibraltar Criminal Justice Act and any other statute relating to money laundering including the Anti Money Laundering Guidelines published by the Gambling Commissioner.

1.4.1 The Gibraltar money laundering Legislation and Code

The AML requirements of the Third Directive were transposed into Gibraltar's domestic legislation through the Crime (Money Laundering and Proceeds) Act 2007 (CMLP). The third Directive, the CMLP Act and the Gambling Act effectively identify the Gambling Commissioner as the competent authority for supervising anti-money laundering policies and procedures in the Gibraltar gambling industry.

In January 2009, the Gambling Commissioner issued a Consultative Document on a proposed Code of Practice for the Gambling Industry on Anti Money Laundering and Counter Terrorist Financing Guidance. The final code is intended to be 'interpretative guidance' to the Gibraltar gambling industry in respect of the requirements of the Third Directive, Gambling Act 2005 and the CMLP Act. A Code may only be issued with the consent (approval) of the Minister for Gambling and subsequently may be taken into account in any proceedings before a court or in any matter to be determined by the Licensing Authority.

The Consultative Document advises that it is intended the Code will apply to all financial transactions associated with relevant gambling activities undertaken under the authority of a Gibraltar gambling licence. It will build on the existing good practice of the Gibraltar gambling industry, and be consistent with the anti-money laundering guidance notes issued by the Financial Services Commission and with recommendations from the FATF and the IMF.

The Commissioner is recommending that 'relevant gambling activities' for the purposes of the Code should include all remote gambling activities as defined by

[18] www.gibraltar.gov.gi/gov_depts/internet_gaming/internet_gaming.htm

the Gambling Act, including remote betting, and all gambling in casino premises unless specifically excluded.

In line with the requirements of the Directive the key provisions of the code for all remote and non-remote licence holders will be the requirement:

- for a suitably senior nominated officer to take responsibility for implementing and overseeing all AML arrangements for a Gibraltar licence holder;
- to undertake a formal risk assessment of the business taking into account that "some games, bets, states and transaction methods have already established a reputation as being open to certain 'lower level money laundering typologies, other elements of gambling have proved unproblematic";
- to apply basic and enhanced customer due diligence and the requirement for all remote and all higher spending customers to be subject to enhanced due diligence and recording;
- not to permit anonymous accounts
- to apply ongoing due diligence and ongoing monitoring based on a customer's expected and developing gambling profile;
- to apply the due diligence requirements to existing customers giving priority to those who are less well established or whose pattern of gambling or spending profile is outside the expected parameters;
- to train all relevant staff to monitor patterns and styles of customer registration, gambling activities and personal information for indication of money laundering activities and to how to respond when they suspect or believe that money laundering may be taking place;
- to keep due diligence and transaction records for the required period;
- to report knowledge or suspicion of money laundering to the relevant authorities.

1.5 Regulation of remote gambling within Malta

Gambling in Malta is governed by the Lotteries and Other Games Act 2001. Remote gaming via foreign operators is permitted under licence and is regulated by the Lottery and Gaming Authority (the Gaming Authority). To provide remote betting/gaming services from Malta, an operator needs to obtain a licence of the class appropriate to its operations. The framework requires that licensees comply with the Gaming Authority's policies, laws and regulations, as well as anti-money laundering laws, e-commerce and other applicable legislation.

The Remote Gaming Regulations issued in early 2004 by the Gaming Authority superseded the Operation of Betting Offices Regulations 2000. They were designed to improve the existing rules and further enhance Malta's reputation as a jurisdiction to be trusted by both players and operators. The Regulations provide for four different classes of licences, namely;

Class 1 - Remote Gaming Licence for online gaming i.e. operators managing their own risk on repetitive games (casino-type games, skill games and online lotteries).

Class 2 - Remote Gaming Licence for online betting office i.e. operators managing their own risk on events based on a matchbook (fixed odds betting, pool betting and spread betting).

Class 3 – Promotion and abet gaming from Malta and operators taking a commission from promoting and/or abetting games (P2P, poker networks, betting exchange and game portals).

Class 4 – Hosting and managing online gaming operations, excluding the licensee himself i.e. software vendors developing platforms from which gaming operators can operate.

Licences are issued for a minimum period of five years and may be extended for further periods of five years each.

The aim is stated as being to provide a Cyber-Space Gaming Licence that is both technology neutral and game neutral, encompassing any type of gaming using any means of distance communication, including Internet, digital TV, mobile phone technology, telephone and fax.

Obtaining an online gaming licence in Malta is considered to be a serious matter for the protection of consumers and Malta's reputation. Being perceived by players as safe and credible provides greater credibility to online gaming sites and therefore assists in making them more competitive. The application of a gaming licence requires the following documentation:

i. Detailed profile of the promoting company.
ii. A copy of the last audited accounts of the promoting company, where applicable.
iii. A business plan indicating the economic activity – including job creation if any – which will be carried out from Malta.
iv. Personal details of all shareholders having more than 5% interest in the local operations.

Both hardware and software involved in the operations must be located in Malta; third party companies can provide this service without the need for the licensee to obtain its own premises.

The Malta Financial Services Authority which regulates the financial services sector registers all companies, including betting companies, oversees the due diligence process on prospective licences and advises the Gaming Authority on the suitability of an applicant for the issue of a betting licence.

The activities of the International Trading Company set up to operate the gaming licence are limited to those undertaken outside Malta. No Maltese resident is permitted to place bets with such a company.

1.5.1 Malta's anti-money laundering legislation

The Third European Directive was implemented by the Prevention of Money Laundering Act 2008. The Act makes reference to casinos, but the word casino bears the same meaning as under the Gaming Act 1998, which is "such premises in relation to which the Minister has granted a concession".

The Remote Gaming Regulations 2004 set out the principal anti-money laundering requirements for the remote gambling industry. Under the Regulations:

- customers may only create one account;
- the identity of customers withdrawing more that Lm 1000 must be clearly established;
- funds must be remitted back to that account from which they have been received;
- no cash may be accepted;
- the registration of players must be conducted via a valid email address.

The Regulations are currently being updated in line with the Third Directive and the 2008 Act.

1.6 Regulation of remote gambling in Alderney

Alderney is subject to Guernsey substantive law including The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law 1999.

Gambling in Alderney is governed by the Alderney eGambling Ordinance and Regulations of 2006. The Gambling Control Commission (the Commission) was appointed by the government of Alderney in 2000 to oversee gambling operations within its jurisdiction.

The following types of licenses and certificates are available:

- A full eGambling licence.
- An Associate certificate.
- A Hosting certificate
- A Restricted Use eGambling licences.
- A Key individual certificate.

Licensing is the first step in the regulatory framework the second being technical compliance and the third relating to internal controls.

The main objective of the licensing stage is to ensure that the applicant company is 'fit and proper'. The owners, managers, systems providers and sources of finance are all subjected to probity investigations. This is a rigorous process that will typically involve examination of financial records, including personal financial records and the business history of the applicant company and its associates. If the outcome is satisfactory and the Commission makes a finding of suitability, the applicant company and its key personnel are awarded licences conditional upon the approval of both their operating and gambling systems as well as their internal controls. These further approvals are required before the licensee can commence business.

The holder of an eGambling licence can lawfully effect gambling transactions of any type (betting, gaming or online lottery). Any entity not wishing to incorporate an Alderney company to hold a full licence can seek a restricted use eGambling licence. Such a licence is sometimes held as business continuity support in the event that its primary site, based elsewhere, is unavoidably unusable.

Gambling transactions can only legally be effected at "approved premises", which are controlled by the holder of a hosting certificate. "This is a new concept responding to the reality of the industry whereby an eGambling operator generally locates its gambling equipment at the premises of a "telco", over which the operator has little or no control. Consequently, the introduction of hosting certificates creates a direct regulatory relationship between the Commission and the telcos"[19].

The main objectives of the Commission are to ensure that:

- all gaming and betting is conducted honestly and fairly;
- the funding, management and operation of online gambling on Alderney remains free from criminal influence and exploitation; and
- gaming and betting activities are regulated and monitored so as to protect the interests of the public, in particular, ensuring that players understand what they being offered when they take part in gambling.

An eGambling licensee and, where appropriate, its associates are obliged to take steps to comply with applicable international measures in respect of money laundering and terrorist financing.

The Commission's stated aim is to ensure that its regulatory and supervisory approach meets the very highest of international standards. To achieve this objective, the Commission is engaged in regular dialogue with other regulatory bodies at an international level. It is a member of the Gaming Regulators European Forum (GFEF) and the International Association of Gaming Regulators (IAGR).

1.6.1 Alderney's anti-money laundering regulations

The Alderney eGambling (Money Laundering Amendments) Regulations, 2008 came into force on 1st May 2008 and amended the Alderney eGambling Regulations, 2006. The 2008 Regulations 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 the FATF recommendations.

Before they can commence operations, an eGambling licensee must prepare a document setting out its Internal Control System. Part of this document must address the procedures and processes a licensee will adopt to prevent and detect money laundering and to counter terrorist financing.

Licensees must now apply a risk-based approach when considering how they will meet their AML obligations. The Commission has determined that within remote gambling, the concept of lower risk does not exist and that all licensees are subject to the two higher levels of risk: standard risk and higher risk.

Under the Regulations licensees must:

- Compile a Business Risk Assessment (BRA) documenting the exposure of the business to money laundering and terrorist financing risks and vulnerabilities, including those which may arise from new or developing

[19] Alderney's new e-gambling legislation - Crown Advocate Richard McMahon Director of Civil Litigation, States of Guernsey (World Online Gambling Law Report)

technologies. The BRA must cover the general risks relevant to the industry and specific risks relating to customers, products and services, banking methods and geographical areas of operation and employees.

- Appoint a Money Laundering Reporting Officer and a Nominated Officer.
- Implement controls to mitigate the identified risks including activity and transaction monitoring.
- Undertake an individual risk assessment for each customer either at the time of registration or as soon as is reasonably practicable thereafter.
- Undertake standard customer due diligence in order to identify every customer and enhanced due diligence for high risk customers.
- Perform CDD measures on a player where the customer regularly makes deposits of, or exceeding, €3000, or where the value of deposits in any period of 24 hours reaches or exceeds €3000.
- Ensure that no anonymous accounts or accounts in fictitious names can be set up.
- Report transactions and activity to the MLRO or nominated officer where there is knowledge, suspicion, or reasonable grounds for knowing or suspecting money laundering or terrorist financing.
- Keep records as required by the Regulations.
- Record the actions they take to achieve compliance with Bailiwick laws.

1.7 Regulation of remote gambling within Italy

Following the lengthy reluctance of the Italian government to license foreign remote gambling operators, the blacklisting of websites of foreign gambling operators and the intervention of the European Court of Justice, on 30 June 2006 the Italian Council of Ministers enacted a Law Decree legalising remote gambling. Companies were invited to tender for licenses and subsequently 33 remote gaming licences were awarded.

The same provision also authorised the Italian gaming regulator (AAMS) to implement relevant regulations by 31 December covering, amongst other services:

- Interactive Peer-to-Peer Betting on Fixed Odds – a brand new gaming product for the Italian gaming market.
- Real-Money Remote Skill Gaming - a gaming product for the Italian gaming market
- New regulation of remote gaming services including real money skill games subject to a fee of €300,000.

The Finance Act 2007 removed the blacklisting of foreign sites and included a definition of card games as skill-based games, provided:

i they are organised in the form of a tournament; and

ii the stake is limited to the tournament entry fee only.

In December 2007, Italy notified the European Commission of the proposed new remote gaming rules and the lighter licensing requirements. The new

regulations attracted adverse comments from the European Commission particularly in relation to:

- the cost of the licence;
- the requirement for operators to connect their systems to the government central database; and
- the requirement for operators to have reached a certain level of betting turnover in the past to be eligible for a licence.

Following further meetings and discussions the new regulations were finalised at the end of 2008. In particular:

- Any gaming company licensed and operationally based in another EU jurisdiction may apply for an AAMS licence subject to proving a global gaming turnover of not less than €1.5 million over the last biennium
- A non-gaming operator will be able to apply for an AAMS remote gaming licence subject to:
  - i proving that he holds all required logistic, technical and organisational infrastructure;
  - ii releasing a €1.5 million bank guarantee in favour of AAMS;
  - iii setting up a company in an EU jurisdiction and locating there the hardware and software infrastructure that will be running the games covered by the AAMS licence.

Among the new licensing requirements, the server location rule will make it possible for a foreign-based AAMS licensee to keep his servers abroad provided (i) they are within the European Union; and (ii) a 24/7 remote linkup with the AAMS centralised system is guaranteed for bets validation, compliance monitoring and tax purposes[20].

1.7.1 Italy's anti-money laundering regulations

The Third Money Laundering Directive was implemented by Legislative Decree No 231 in November 2007. Whilst there are as yet no regulations or guidance for the remote gambling industry, the following general requirements of the Directive will apply:

- The need for policies, procedures, internal controls, compliance management and communication in order to forestall and prevent operations relating to money laundering or terrorist financing.
- The application of a risk-based approach.
- Customer due diligence (CDD) when a business relationship is being established and identification verified when the €2000 threshold is reached.
- CDD for beneficial owners and third parties.

[20] "an Outlook of the Italian gaming market at two years from its liberalisation" – Quirino Mancini, partner, Sinisi Ceschini Mancini Advocats

- Additional measures to verify identity for non-face to face transactions and activity.
- Enhanced due diligence and monitoring for politically exposed persons and other higher risk customers.
- Ongoing monitoring and scrutiny of transactions and activity.
- Paying special attention to complex or unusually large transactions or unusual patterns of transactions which have no apparent economic or visible lawful purpose.
- Arrangements for awareness raising and training of staff.
- Reporting to Italy's financial intelligence unit (the UIC)) where the remote gambling operator or an employee knows, suspects or has reasonable grounds to suspect that money laundering or terrorist financing is being committed.
- Retain CDD and transaction/activity records.