ANTI-MONEY LAUNDERING:

GOOD PRACTICE GUIDELINES FOR THE ONLINE GAMBLING INDUSTRY

The Remote Gambling Association Ltd, 6th Floor, High Holborn House, 52-54 High Holborn, London WC1V 6RL

Tel: + 44 (0) 20 7831 2195 e-mail: info@rga.eu.com Web: www.rga.eu.com

ANTI-MONEY LAUNDERING: GOOD PRACTICE GUIDELINES

The Remote Gambling Association Ltd, 6th Floor, High Holborn House, 52-54 High Holborn, London WC1V 6RL

Tel: + 44 (0) 20 7831 2195 e-mail: info@rga.eu.com Web: www.rga.eu.com

Introduction

1. The RGA is committed to keeping the online gambling industry crime-free and to the encouragement of high standards of probity and integrity, both for the benefit of its members and the public generally. Combating money laundering effectively is a major objective in this area and the purpose of these guidelines is to help RGA members achieve that in a consistent manner.

2. Although many of these guidelines are specific to countries in the European Union (EU) and the regulatory and legislative structures within EU member states, the principles and many of the suggestions for good practice will have a wider geographical application.

3. There is a hierarchy of regulation where money laundering is concerned. This includes international legislation, such as the EU Money Laundering Directives, United Nations resolutions, and international policy initiatives, such as the recommendations published by the Financial Action Task Force. These are distilled into national frameworks, which can be a combination of regulatory requirements, such as gambling licence conditions and/or broader laws which may apply to a range of commercial activities. These guidelines are intended to highlight the importance of operators being in compliance with these national requirements, having regard to the wider international context. Some operators may need to comply with the national requirements of a number of countries, in which case it is usually sensible to the operator to work to the highest applicable standard across the group. The guidance is also intended to suggest practical ways to conduct AML/CTF.

4. There is continued speculation about the level of money laundering involving online gambling and the risk it presents as the industry evolves. In an attempt to bring some objectivity to these issues the RGA commissioned in 2009 a report from MHA Consulting (copies available at www.rga.eu.com). It concluded that a combination of statutory and self regulation had effectively reduced the risk of money laundering through online gambling and that there were almost no examples of money laundering in licensed jurisdictions.

5. Some of the report's key findings were that:

- 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 was a strong commitment within 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;

- 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; and

- 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.

6. The report also underlined the need for the industry to remain vigilant; to work with regulators, law enforcement agencies and others to disseminate best practice; and to ensure that all related rules and guidelines keep pace with technological developments and the inventiveness of money launderers.

Purpose

7. The production of these guidelines flows from the MHA's recommendation that such guidelines could provide a useful tool for the industry and seeks to address some specific practices that MHA suggested could be improved upon or undertaken more consistently.

8. The guidelines are meant to complement legal and regulatory requirements, irrespective of the jurisdictions where operators are licensed. They do not seek to set out the rules and regulations applicable in every jurisdiction, but rather to help those in the industry establish and implement procedures that they can be confident are broadly in line with industry best practice.

9. The aim for all companies and regulators in this sector should be to build a proportionate and risk-based AML & CTF regime. Any model adopted should be continually reviewed to ensure that it continues to cover all elements of possible risk. This methodology in turn ensures the best use of resources, value for money, and highlights the factors that represent the greater risk.

Regulatory context

10. The Financial Action Task Force has produced both high level strategic international guidance on the risk based approach to AML & CTF for casinos. This guidance suggests that individual remote operators and regulators undertake risk assessments at a country level to help inform their approach. Consequently, while the AML & CFT objectives are the same for all EU Member States and for members of the FATF the approach taken may vary from jurisdiction to jurisdiction. Even within the EU, different Member States have interpreted and enforced the requirements of the 3rd European Money Laundering Directive in different ways.

11. It should be noted that for the purposes of the Directive the regulated sector includes both on and offline casinos but operators will also need to take care to ensure that they are aware of any local regulatory requirements which apply some other form of AML/CFT regime to other gambling products. This might, for instance, be where a country decides to go further than the Directive and extend the provisions to cover betting or where separate legislation introduces different requirements for betting. An example of this would be the Proceeds of Crime Act 2002(POCA) in the UK or the Crime, Money Laundering & Proceeds Act 2007 (CMLP) in Gibraltar.

Definitions

12. This guidance is designed for those already familiar with the concept of money laundering and the methods most commonly used by money launderers, but for the sake of clarity money laundering can be described as the process(s) by which criminals conceal or attempt to conceal the origin of the proceeds of their or others' criminal activities. The process of layering money may take place over several stages with gaming being just one part of that process. The aim, once money has been laundered, is that it can then appear to be legitimate. However RGA members should check whether their country's definition of money laundering also includes illegal activities that are far more subtle and difficult to detect, e.g. in the UK simple possessing the proceeds of crime or spending the proceeds of crime (without any return) is money laundering. Similarly in the UK savings earned from crimes like tax evasion are defined as money laundering. Operators should check how their countries have enacted the issue of predicate offences.

13. A more recent development and a sub-category has been money laundering to support terrorist financing. The fight against that particular strand of money laundering is commonly known as Counter Terrorism

Financing (CTF). This is another crucial area to consider because terrorists and their supporters may commit crimes in order to finance acts of terrorism. However terrorist financing can also occur when money earned legitimately is provided to terrorist groups for an illegitimate purpose.

Industry responsibility

14. Money laundering and terrorist financing are serious international issues and it is important that such criminal activities are identified and prevented by all available means. The FATF has identified casinos as one of many industries that may be attractive to those who wish to commit crime, conceal the profits of their crime or fund terrorist activity. By extension the online gambling industry therefore has a duty to detect and prevent money laundering and the funding of terrorism wherever possible.

Customer interaction

15. It may be helpful to explain to all customers that discharging this responsibility may mean that they must complete detailed registration process before they can begin to use the services of the remote gaming provider, and subsequently provide further information about themselves, for example the 3rd EU Money Laundering Directive indicates that when a threshold of 2000 euros has been reached if the operator takes the threshold approach to customer due diligence.

16. Customer due diligence checks should already be familiar to customers from their experience of dealing with the wider banking and financial services sector. Whenever customer due diligence is performed it is important to remain vigilant throughout the relationship. It is not acceptable to turn a blind eye and hope for the best. The nature of the remote gaming sector is such that weaknesses, if exploited, could pose great risks by virtue of the sums of money involved, the speed of transactions, and the levels of turnover.

Role of the MLRO

17. Remote gaming operators should appoint a Money Laundering Reporting Officer (MLRO) with sufficient seniority and command as the reporting officer, to whom a report is to be made of any information or other matter which gives rise to a knowledge or suspicion or reasonable grounds for suspicion that a person is or may have engaged in money laundering or the funding of terrorism or that a transaction may be related to money laundering or the funding of terrorism.

18. Remote gaming operators need to consider the level of staffing and other resources they require in the fight against money laundering and the funding of terrorism. All relevant staff working for the operator in a customer facing role needs to be aware of the risks posed by money laundering and the funding of terrorism. There will be few employees whose roles are not touched by this area. Those dealing with customer registration, customer funds and customer services will need specific training highlighting the importance for them to be vigilant in order to identify higher risk situations and all staff will also need to know how to report any concerns or suspicions to their MLRO.

19. It is therefore important that a remote operator's employees know the identity of their MLRO and the deputy MLRO and how they can be contacted as well as the procedure for reporting. If staff are based in different countries from their MLRO then this needs to be dealt with in the policy.

Policy development and application

20. Senior management within remote gaming must be fully engaged in the decision making process. They must take ownership of the risk-based approach because along with the MLRO, they may be held accountable if the approach is inadequate. This means engaging and participating in the decision making process which generates the risk-based policies adopted by the remote gaming operator. This approach should be supported by regulators and, for example, in its guidance the British Gambling Commission states 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".*

21. It is common practice for jurisdictions to make it an offence if the relevant national laws and procedures are not followed properly. The risk of this happening can be minimised by proper and considered risk assessments and the implementation of proportionate AML/CTF policies which are properly documented eg a policy including, how to report, training, record keeping.

22. In relation to suspicions about specific individuals, MLROs should keep separate records of steps taken and questions asked and responses received. This should then enable the operators to demonstrate to the regulators and courts the process by which it assesses threats, and decides on the appropriate systems and procedures (including due diligence requirements) in the light of the risk assessment that has been made and how procedures work if money laundering is suspected.

23. The consequences of failure could be high. Failure to implement sufficient systems and controls could lead to the operator being criminally liable or subject to regulatory sanctions, such as fines or licence revocation. Remote gaming operators and those who work for them can reduce their personal risks by the implementation and adherence to such a program. If there is a proper consideration of the risks, together with a consideration of the way in which they can be mitigated, with discussions and decisions being properly recorded and established procedures actually being followed then there is little for those involved to fear.

Working with supervisory authorities

24. It is self evidently important to liaise with all relevant supervisory authorities in every jurisdiction where a gambling licence is held. Operators need to ensure that they know who all of these bodies are and it is reasonable to expect the local gambling regulator to respond to approaches made by operators Likewise operators need to know what regulations apply. These will normally go beyond those contained solely in a gambling licence and may not even be labelled 'money laundering'. This would, for example, be the case with the UK Proceeds of Crime Act which applies not just to the 'regulated' sector of gaming but to all commercial activities.

25. Operators will need to identify the appropriate Financial Intelligence Unit (FIU) which receive money laundering reports. International operators need to consider which FIU they will report to and in which circumstances reports need to be made to more than one FIU and of course comply with any consent or reporting requirements that might be in place.

Risk based approach

26. The fight against crime and terrorism imposes costs on government, business and taxpayers. It is essential, therefore, that the benefits of any AML/CTF program should outweigh its burdens; that action is targeted wherever possible on specific areas of risk and vulnerability and the right balance is struck between the need to prevent the industry being misused for money laundering or terrorist financing and privacy of the individual. *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* (MHA report 2009).

27. As money laundering and terrorist financing threats change constantly and vary greatly across customers, jurisdictions, products, delivery

channels and over time, it is recognised that the response for money laundering and/or terrorist financing needs to be as supple as the criminals and terrorists themselves. In this context, a prescriptive and arbitrary 'tick box' approach would miss its target and fail to deliver benefits that outweigh the costs of intervention. Risk management is a continual process and an operator's risk model should be reviewed and if necessary updated regularly to reflect any change in circumstances.

28. In order to meet the requirements of the Directive, these guidelines aim to give a high level overview of the operation of a model (the AML Scorecard or Risk Matrix as examples) that builds on the risk based approach advocated by the FATF and the Directive. This model matches the degree of risk presented by every customer with an appropriate and variable level of continuous monitoring, investigation and prioritisation.

29. The Risk Assessment documents the exposure of the business of a remote gaming licensee to money laundering and terrorist financing risks and vulnerabilities, including those which may arise from new or developing technologies that might favour anonymity taking into account its (a) size, nature and complexity; and (b) customers and services and the ways in which it provides those services.

30. Having conducted a risk assessment the remote operator is able to take discrete steps to assess the most cost effective, proportionate way to manage and mitigate those risks identified. It is recognised that each individual business is different and while regulators can offer advice and guidance, the final responsibility to assess its own risks according to its business model rests with each operator. A 'one size fits all' approach is not suitable to a risk-based environment.

31. Conducting a risk assessment for AML/CFT, is not a one-off exercise, it is an ongoing process. There are three steps in applying a risk based approach;

- *Risk Mitigation* – Identifying and applying measures effectively to mitigate risks
- *Risk Monitoring* – Putting in place management information systems and keeping up to date with changes to the risk profile through changes to the business or threats
- *Documentation* – Having policies and procedures to cover the above and deliver accountability from the Board and Senior Management down.

32. However carried out, a risk-based approach needs to be part of the operators philosophy, and as such reflected in its procedures and

controls. There needs to be a clear communication of policies and procedures along with robust mechanisms to ensure that they are carried out effectively, weaknesses are identified, and improvements are made wherever necessary. In short, an operator needs to have a compliance culture which feeds down from the Directors to frontline staff.

33. This risk assessment aggregates the risk posed by customer from registration and throughout the life of the business relationship. This methodology provides for best uses of resources and proportionate response. It means that the customers representing the greatest risk of money laundering or terrorist financing are faced with the most stringent CDD requirements at the earliest opportunity.

34. Risk scoring or a customer risk profile can be used to help analyse information in order that more objective and consistent decisions can be made more fairly and more quickly. The scoring system allocates points to a particular customer based on their behaviour throughout the business relationship and can be weighted according to the perceived risk Indeed, a risk based methodology seeks to check the identity of customers at the point that an account 'trips' a risk-based trigger. A web of triggers can be made to cover all elements of risk-related activity based upon customer attributes, funding and behaviour activity and is continually reviewed and amended to ensure that it continues to cover all elements of possible risk. It is acknowledged that operators will use a variety of system's including other methods where triggers are set to indicate that a particular account requires reviewing at a certain stage.

35. The Financial Action Task Force advises that the following range of variables will impact the level of AML/CFT risks that internet 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.

36. These risks can broadly be categorised and addressed under the following headings (following paragraphs expand on these points):

- Customer Risk
- Product/Services Risk
- Transaction/Payment Risk
- Geographical Risk
- Behavioural Risk (monitoring)

Customer Risk

37. This includes types of customers and style of business relationship. The risk assessment should consider what information the operator holds about the customer and that the information is consistent, i.e. do the details match? In addition operators should have a risk based policy on how and when to ascertain whether any customers are considered to be Politically Exposed Persons (PEPs) or named on international sanctions lists.

Products /Services Risk

38. Some products should be considered as higher risk for passing/movement of funds than others. For example, poker could be

seen to be a higher risk game due to the higher risks of collusion and chip dumping by customers whilst slots and bingo may be seen to be lower risk games, requiring minimal, if any, AML risk mitigation beyond those applied at the customer level. Any irrational funds movement should attract greater attention e.g between different products without any apparent reason.

39. Some operators may offer facilities for their customers to transfer funds to another customer - commonly known as player-to-player transfers. This presents significantly increased risk which may necessitate the implementation of additional customer due diligence procedures in relation to those involved.

40. It is not uncommon for customers to have multiple accounts and payment methods, and for them to gamble across different platforms (online sports book, casinos, poker etc). It is important therefore to have systems in place that provide an overall picture of customer behaviour as part of the business relationship.

Transaction/Payment Risk

41. Deposit and withdrawal methods are now offered from a wide variety of sources including credit/debit cards, bank transfers, wire transfers, pre-paid cards, and other methods of making deposits into and withdrawals from a customer's gaming account. These methods involve differing checks on the provenance of the funds which will have undergone due diligence to a greater or lesser degree by the payment provider. It is rare in the online gambling industry for cash deposits to be made, but, where that facility is provided, the operator must have policies and procedures in place to safeguard against the additional risk presented. Operators should try and avoid simply acting as banks, i.e customers accounts should be used to facilitate gambling, not as a substitute for conventional bank accounts.

Geographical Risk

42. Some countries are deemed to present greater risks than others for money laundering and funding terrorism. These countries typically do not have legislation which meets FATF or EU standards. Remote operators should therefore focus on money being received from and remitted to such jurisdictions. Corruption and risk indexes can be found through such organisations as Transparency International and can prove valuable in assisting in helping to assess such risks. In addition, operators should keep up to date with FATF reports, media reports, and country specific reports in order to keep their country risk assessments up to date.

Behavioural Risk/Monitoring

43. As a relationship progresses with a customer the more the operator will or should know about that customer. Monitoring of behaviour provides a good barometer for continual assessment of the risk posed by the customer and any deviations from what has become the norm for that individual should be identified and risk assessed. For example, a customer who may make a number of small deposits then starts making large deposits or a customer who deposits large quantities of funds but has little or disproportionate betting activity will increase the risk posed by that customer.

Weighting according to behaviours

44. One way of analyzing and applying the attributes listed above can be by sub-dividing them into behaviors, which are weighted and scored. The weighting remains flexible and can be adjusted dependent on how much each behavior is considered to be a risk. Meeting a pre-defined 'points' threshold triggers basic customer due diligence, or enhanced due diligence in appropriate circumstances.

45. The risk based approach can also trigger an investigation regardless of whether the person has completed customer due diligence. This continuous monitoring of customer behavior to minimize the risk of money laundering through dormant accounts, compromised accounts, accounts set up with stolen identities and accounts that have been set up specifically for money laundering after initial Customer Due Diligence (CDD) process has been completed.

46. This risk based approach requires information to be collated from a variety of sources throughout the business relationship making avoidance of due diligence measure exceptionally difficult. This methodology monitors how customers conduct their business relationship, directs resources towards the potential money launderer/terrorist financier and prevents those valuable resources being overwhelmed and ineffective.

Customer Due Diligence

Customer Due Diligence – Standard/Basic Due Diligence

47. Customer due diligence is achieved by identification which involves the customer providing their personal information and verification of that identification. Standard/Basic due diligence could take place at the outset or very soon after the commencement of the business relationship, or within the EU when the 2000 euro threshold is reached, but it does not happen as a matter of course. Such due diligence verification can be achieved by one or more of the following processes:

- Independent third party verification. eg the use of a software system and or:

- Checking personal documents e.g.
  - government issued ID proving identity & age
  - proof of address (utility bill)
  - bank statement.

- Other processes that evolve over time.

Customer Due Diligence - Enhanced Due Diligence

48. To provide the highest level of confidence, again following the principles of a risk based system for customer due diligence, this level will capture those customers and/or funds which can present a higher risk of money laundering or the funding of terrorism and is achieved by using one or more of the following processes:

- 3rd Party verification – e.g use of software, or using approved third parties to conduct face to face verification of customer documents; for example in some countries Post Offices provide this service.
- Validation of customer documents - Certified copies of documents to validate name, address, date of birth and source of funds of the customer.
- Address Validation Check - Using a secure code delivered to the customer's address to validate that the customer is actually resident at the address stated.
- Reputable funding - Ensure that the first (next) payment or transaction into the customer's account is carried out through an account held by the customer in his name with an authorised credit institution or recognised under the Payments Services Directive, or otherwise so authorised in another '[1]reputable jurisdiction'.

---

[1] **'reputable jurisdiction' means any country having appropriate legislative measures for the prevention of money laundering and the funding of terrorism, taking into account that country's membership of, or any declaration or accreditation by, any international organization recognized as laying down internationally accepted standards for the prevention of money laundering and for combating the funding of terrorism, and which supervises natural and legal persons subject to such legislative measures for compliance therewith.**
These third countries are currently considered as having equivalent AML/CFT systems to the EU. The list may be reviewed, in particular in the light of public evaluation reports adopted by the FATF, FSRBs, the IMF or the World Bank according to the revised 2003 FATF Recommendations and Methodology.
• Argentina
• Australia
• Brazil
• Canada
• Hong Kong
• Japan

- Source of funds - Confirm the immediate source from which the funds have derived.
- Internal corroboration of user identity – this could emanate from a variety of sources from customer monitoring, other databases and face to face verification.
- Other processes that evolve over time.

Customer Due Diligence - Business Accounts

49. Where operators allow business accounts for gaming products in the wider remote gambling environment, then in addition to the personal identification from at least two directors the following might usefully be sought in writing from a solicitor/account who is qualified in the relevant jurisdiction to confirm that:

    - The company is properly registered,
    - Registered name,
    - Registered address,
    - Office-holders, shareholders and/or beneficial owners.

Politically Exposed Persons

50. Politically Exposed Person ("PEP") are typically defined by the EU as natural persons who are or have been entrusted with prominent public functions and shall include their immediate family members or persons known to be close associates of such persons, but shall not include middle ranking or more junior officials.

51. The fact that a person is a PEP does not automatically mean that they are involved in money laundering. It is however something that could result in an alteration to their risk profile and justify enhanced customer due diligence measures being applied.

• Mexico
• New Zealand
• The Russian Federation
• Singapore
• Switzerland
• South Africa
• The United States

The list does not apply to Member States of the EU/EEA which benefit de jure from mutual recognition through the implementation of the 3rd AML Directive. The list also includes the French overseas territories (Mayotte, New Caledonia, French Polynesia, Saint Pierre and Miquelon and Wallis and Futuna) and the Dutch overseas territories (Netherlands Antilles and Aruba). Those overseas territories are not member of the EU/EEA but are part of the membership of France and the Kingdom of the Netherlands of the FATF. The UK Crown Dependencies (Jersey, Guernsey, Isle of Man) may also be considered as equivalent by Member States.

52. Establishing whether a person is a PEP is not straightforward and may require a number of different processes to be involved. Whatever processes are employed to screen for and identify PEPs, new customers should be screened on registration as well as regular screening of existing customers. This could include the use of internet search engines or subscriptions to suitable databases. The databases used for customer due diligence may be able to assist in this regard.

53. Remote operators will need to put into place processes for:

- identifying PEPs,
- obtaining senior management approval in accepting PEPs as customers,
- ensuring that there is proportionate monitoring of such customer accounts and,
- measures to establish the source of wealth and funds that are involved in the business relationship /transactions.

54. However, as there is no single source of information identifying PEPs and as there is a large degree of subjectivity in deciding whether someone falls into that category, this is an area where a proportionate risk assessment will represent best endeavors.

Sanctions

55. Sanctions are normally used by the international community for one or more of the following reasons:

- To encourage a change in the behaviour of a target country or regime.
- To apply pressure on a target country or regime to comply with set objectives.
- As an enforcement tool when international peace and security has been threatened and diplomatic efforts have failed.
- To prevent and suppress the financing of terrorists and terrorist acts.

56. Financial sanctions are normally one element of a package of measures used to achieve one or more of the above. Financial sanctions measures can vary from the comprehensive – prohibiting the transfer of funds to a sanctioned country and freezing the assets of a government, the corporate entities and residents of the target country – to targeted asset freezes on individuals/entities

57. Operators should examine carefully any requirements that their regulators may place on them in relation to Sanctions.

Suspicious Transaction reporting

58. Jurisdiction specific guidance can be sought from the FIU, but in almost all circumstances it will be a legal obligation for those who work for a remote gaming operator to know that they are under a duty to report suspicious transactions. These would include instances:

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

59. This includes where money laundering or funding of terrorism has been, is being, or may be committed or attempted.

60. Remote gaming operators should have a documented process in place for all employees to report when they have suspicions that a customer may be engaged in money laundering or terrorist financing to the money laundering reporting officer (MLRO) or in his absence their Deputy MLRO.

61. Operators should be aware that their obligations in this respect extend beyond their customer base, but should also encompass contractors, business contacts and the like.

62. The MLRO, must consider each report made to determine whether it gives rise to grounds for knowledge or suspicion. Where such suspicion is determined, a suspicious transaction report must be sent in compliance with any locally applicable process (normally to FIUs, but when required also to any gambling licence issuing authority). Attention will need to be given to any applicable reporting timetables. It should be remembered that in some countries, such as the UK, failure to report is in itself is a criminal offence carrying with it a possible prison sentence.

63. Operators should, or may be compelled, to document how staff shall report their suspicions promptly and without prejudice, to the MLRO or nominated officer. The MLRO or nominated officer should take into account all relevant information prior to making a report as above OR must fully document why a suspicious transaction report **is not** forwarded.

64. If there is no feedback from the relevant authorities then future transactions could continue. The MLRO should consider whether it is necessary to submit further reports or whether to allow the account to remain active.

Record keeping

65. Unlike the terrestrial gambling sector, a remote gaming operator will always enter into a business relationship with a customer. Therefore there can be no occasional or one off transactions. Remote gaming operators are required to keep the following records:-

- transaction documents
- due diligence information
- information relating to suspicious transactions
- MLRO reports
- training in relation to AML matters, and
- policies and procedures

66. This information could be required on a timely basis by regulatory authorities. The documents as outlined should be kept for 5 years from the date of the transaction or the date of completion of any related transaction. Customer due diligence information, or copies thereof, must also be kept for a minimum of 5 years from the date the person concerned ceases to be a registered customer or from the date of the customers most recent activity. These records can be kept in documentary or electronic format.

Employee training and screening

Training

67. It is imperative that staff receive appropriate and regular training as to their responsibilities with regard to:

- customer due diligence measures
- record-keeping procedures
- internal reporting procedures
- policies and procedures on internal control, risk assessment, risk management, compliance management and communications that are adequate and appropriate to prevent the carrying out of operations that may be related to money laundering or the funding of terrorism,
- relevant regulation in each jurisdiction where a licence is held; and
- the recognition and handling of transactions carried out by, or on behalf of, any person who may have been, is, or appears to be engaged in money laundering or the funding of terrorism.

68. Records should be kept of all training given to staff together with confirmation that they have reached the necessary level of understanding and competence. Staff should be made aware that they have personal responsibilities in the area of reporting.

Screening

69. Staff who are dishonest present a fraud and business risk to remote gambling operators. Operators must ensure that they have in place appropriate procedures for due diligence when hiring employees.

70. This could include reference checks, credit record checks and other vetting measures including verification of information given during the recruitment phase, and confirmation of identity.

71. To summarise, employees should:

- be identified and verified
- be screened to ensure their probity
- receive appropriate training.

Conclusion

72. The remote gambling industry is fully committed to proportionate and risk-based anti-money laundering regulations and this is underlined, for instance, by its involvement with the various initiatives set out in Annex A.

73. The regulated industry has developed an appropriate and effective set of measures to counter money laundering and terrorist financing. These guidelines reflect current best practice and shared experience within the industry, but it is recognised that they will develop further over time especially as and when new challenges arise and have to be addressed.

Annex A

Industry involvement in initiatives to combat money laundering and associated crime

RGA members have been and are actively involved in the following:

Institute of Money Laundering Prevention Officers (IMLPO)

IMLPO was established in 2001. It is a unique, cross-representative forum of anti-money laundering (AML) professionals who share views, experiences and concerns – in a safe environment – of the day-to-day business of combating money laundering.

The aims and objectives of IMLPO are to:

- establish a recognised industry forum to address specific issues of concern identified and raised by its members
- facilitate the further education and professional development of its members
- provide a broad representation for issues concerning money laundering prevention

Financial Action Task Force (FATF) Casino Working Group

The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing. The Task Force is a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

At the end of 2008 the FATF published a new guidance paper for both on and offline casinos. It focused on applying a risk-based approach to combating money laundering and terrorist financing. It resulted from a joint FATF-private sector initiative and the RGA was represented on the relevant working group and took part in the consultations that led to the production of this guidance.

The aim of the guidance is to assist both public authorities and the industry by:

- Supporting development of a common understanding of what the risk-based approach involves;

- outlining the high-level principles involved in applying the risk-based approach; and

- indicating good practice in the design and implementation of an effective risk-based approach.

RGA Crime Issues Group

The RGA also has its own dedicated sub-committee for considering and addressing issues such as fraud and money laundering. This provides a forum for the sharing of best practice and the development of industry policies.

Anti-Money Laundering Europe (AME)

AME is a Brussels-based interactive public/private sector forum on EU financial crime issues. Established in June 2004, its high level private and public sector membership engages directly with EU and international institutions to exchange view, debate and input to policy-making on EU financial crime – money laundering, fraud, terrorist financing.

Liaison

In addition to all of the above the RGA collectively, and its members individually, liaise closely with regulators, policy makers, the law enforcement agencies in multiple jurisdictions and have been heavily involved in consultations in those jurisdictions where the relevant regulations are applicable to the online gambling industry.

Conferences

In addition to being involved with conferences that deal with broader, non sector specific, AML issues, the industry holds a number of events that focus solely on its particular situation. The RGA and its members frequently support these conferences and provide speakers. Recent examples of this would be:

- Combating Cybercrime in Betting and Gaming, (which looked at fraud, security, payments, compliance, IS and the role of technology managers within i-gaming companies).

- Provide-ID Gaming Forum (addressing know your customer issues).

- Institute of Money Laundering Prevention Officers.

Related initiatives

At the end of 2008 in the lead up to Christmas the Online Gambling sector was part of the Be Smart Online Campaign in the UK.

Annex B

Glossary of abbreviations

- **"**AML" means anti-money laundering;
- "CDD" means customer due diligence;
- 'EDD' means enhanced due diligence;
- "CTF" means counter terrorism financing;
- "Directive" means Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing;
- "employees" mean all persons actively employed or engaged with a remote gaming operation;
- "FATF" means Financial Action Task Force;
- "MLRO" means money laundering reporting officer;
- "PEP" means politically exposed person;
- "Recommendations" refer to the 40+9 Recommendations on the prevention of money laundering and terrorist financing published by the Financial Action Task Force;
- "Remote gaming" means any form of gaming by means of distance communications;
- SAR means Suspicious Activity Report;