ANTI-MONEY LAUNDERING GOOD PRACTICE GUIDELINES FOR LICENSED BETTING OFFICES AND REMOTE GAMBLING

Version I
General Distribution
May 2018

GAMLG

GAMBLING ANTI-MONEY LAUNDERING GROUP

CONTENT

GAMLG
GAMBLING ANTI-MONEY LAUNDERING GROUP

PART 1

AML Good Practice in the LBO and Remote Gambling Industries

1. Introduction to GAMLG and the Associations it Represents

1.1. GAMLG is committed to keeping the gambling industry crime-free and to encourage high standards of integrity, both for the benefit of its members and the public generally. Combating money laundering effectively is a major objective for the industry as a whole and the purpose of these guidelines is to help gambling operators achieve that in a consistent and effective manner.

1.2. It is intended that these guidelines will be regularly updated to reflect alterations in Anti-Money Laundering/Counter Terrorism Funding (AML/CTF) operator practices.

1.3. 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 (FATF). These are distilled into national frameworks, which can be a combination of sector-specific regulatory requirements, such as gambling licence conditions or guidance and/or broader laws or regulations, which may apply to a range of commercial activities.

1.4. Higher level changes introduced by the EU 4th Money Laundering Directive, resulted in amendments in the following key areas:

a. The Directive covers the entire gambling sector as opposed to just casinos. However, it allows Member States to exempt sectors on the basis of proven low risk posed by the nature and scale of their services. On this basis, for example, the UK has chosen not to extend the regime beyond online and land-based casinos;
b. the introduction of beneficial ownership registers;
c. the inclusion of tax crimes as a predicate crime;
d. the expansion of the Politically Exposed Persons (PEPs) definition to include domestic PEPs; and
e. an increased emphasis on the risk-based approach.

1.5. There has been speculation about the level of money laundering involving licensed gambling and the risk it presents. Whilst it is worth noting that in 2015 the British Government classified gambling as 'low risk' in its money laundering National Risk Assessment; and subsequently in its 2017 iteration, this does not provide any grounds for complacency, but it does indicate clearly where gambling fits within the wider picture. Should risk levels in the non-remote sector increase in time, there is scope for the sector to be included within the Money Laundering Regulations.

1.6. The Gambling Commission LCCP includes the requirement that all operators undertake a risk assessment in order to identify the potential areas of risk. These will differ by operator due to the size and nature of customer base, products offered and business profile.

1.7. GAMLG's own AML Risk Assessment published in 2017, defined and evaluated 20 LBO sector and 24 Remote sector areas of risk, including controls put in place to mitigate that risk. Following that assessment, there were areas that scored an 'amber alert' status for the 'residual risk assessment after controls' in both the LBO and Remote Gambling Industries. For LBOs, the 'amber alert' areas were identified as:

1. Customer using multiple premises – same operator
2. Customer using multiple premises – different operators
3. Payment following minimal or no play (SSBTs)
4. Low risk wagering/covering all outcomes/cash out (SSBTs)

For Remote Gambling the 'amber alert' areas were identified as:

1. Multiple accounts – different operator

1.8. In the cases where customers are using multiple premises/ multiple accounts, GAMLG is working with the Gambling Commission and the Information Commissioners Office to find a way of sharing information within the Data Protection framework. If the principles of sharing information can be established and where their activity has flagged a suspicion of money laundering; the industry can then share information, to reduce the risk of individuals using multiple accounts and premises, to avoid further detection. Regardless, as highlighted in public statements issued by the Gambling Commission in relation to Anti-Money Laundering failures, operators must utilise all the information they hold on customers (whether relating to remote or non-remote activity) and be aware that customer risk profiles may increase or decrease over time.

1.9. Following a GAMLG member's project, the ABB Council has agreed additional controls for ABB members across the LBO sector, to reduce the 'amber alert' risks further, in the Customer ID and SSBT areas. This will be effective as of 1st January 2018. They should not be used in place of, but should be used to compliment the risk-based approach to combatting money laundering.

1.10. These additional AML controls are not included in this public document, to prevent the circumvention of the trigger points for proof of identity.

1.11. A minimum standard to require photo ID prior to bet placement acknowledges feedback from the Gambling Commission as part of the Operation Dace investigation. A transient customer may place a large bet which loses and not return to a shop, therefore preventing any ability to capture information or otherwise conduct meaningful checks.

1.12. A generic industry leaflet for ABB member's customers provides guidance for the request of customer ID and source of funds and/or wealth. It is proposed that operators provide customers with the leaflet at the point of a further information request, to raise awareness of checks at an industry level and increase the likelihood of customer compliance to avoid unnecessary displacement.

1.13. In 2018 GAMLG's agenda will extend to AML training good practice and technology improvements within the retail and online environments that would improve the AML provision.

2. Purpose

2.1. These guidelines are intended to highlight the importance of operators being compliant with national requirements while having regard to the wider international context. Some operators may additionally need to comply with the national requirements of a number of countries, in which case it is usually sensible for the operator to work to the most stringent standard across the group.

2.2. The guidelines are meant to complement legal and regulatory requirements, irrespective of the jurisdictions where operators are licensed and to provide practical guidance for operators to conduct AML/CTF measures where applicable. 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.

2.3. The aim for all companies and regulators in this sector should be to build a proportionate AML and CTF regime which is reactive to changes. FATF identify the requirement for a risk-based approach which is based on the concept that resources are allocated proportionately to the risks identified.

2.4. As set out in 1.6, a risk-based approach requires a risk assessment to be conducted in order to identify the potential areas of risk; these will differ by operator due to the size of customer base, products offered and business profile.

3. Regulatory Context

3.1. 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. However, all parts of the gambling industry should be alert to the risk and take measures to manage it.

3.2. The FATF has produced both high level and strategic international guidance on the risk-based approach to AML and CTF for casinos[1]. This guidance suggests that individual operators and regulators undertake risk assessments at a country level to help inform their approach. Consequently, while the AML and 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 various European Money Laundering Directives in different ways.

3.3. It should be noted that for the purposes of the Directive, the regulated sector for the UK includes both online 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.

1 http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20for%20Casinos.pdf

3.4. In the UK, for example, there is a relatively clear hierarchy of regulatory requirements which can basically be described as:

a. Global – (i.e. via FATF)
b. EU – primarily via the 4th Anti-Money Laundering Directive
c. Governmental level – (i.e. UK Money Laundering Regulations, Proceeds of Crime Act etc.)
d. Regulator level – (i.e. licence conditions set out in the Gambling Commission's LCCP including licence codes and social responsibility codes which are based on primary legislation, and ordinary code guidance issued by the Gambling Commission).

4. Definitions of Money Laundering and Terrorist Financing

4.1. 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(es) by which criminals conceal, or attempt to conceal the origin of the proceeds of their or others' criminal activities. The process of money laundering 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.

4.2. Some jurisdictions have an expanded concept of the definition of money laundering. It is therefore important for operators to check to see whether their country's definition of money laundering, includes illegal activities that are far more subtle and difficult to detect, e.g. in the UK simple possession of the proceeds of crime, or spending the proceeds of crime (without any return), constitutes money laundering.

4.3. This has a practical implication for operators as not only will it be necessary to ensure that 'classic' money laundering behaviour, detailed above, is detected i.e. the passing of criminal funds through the system with the aim of getting them back as apparently legitimate funds, but also that the AML/CTF measures include detection of criminal lifestyle spend.

"Some jurisdictions have an expanded concept of the definition of money laundering. It is therefore important for operators to check to see whether their country's definition of money laundering, includes illegal activities that are far more subtle and difficult to detect, e.g. in the UK simple possession of the proceeds of crime, or spending the proceeds of crime (without any return), constitutes money laundering."

4.4. There are also implications for operators to consider where the crimes included in the definition of a predicate offence differ across jurisdictions, for example tax evasion. This is a particularly poignant example, as in the UK, money resulting from tax evasion constitutes a predicate crime, unlike in Jersey. where tax evasion does not fall within the definition of a standalone predicate offence. Money laundering is relatively unique, in so far as court proceedings can be brought without predicate offences that result in subsequent money laundering activity. Operators should check how the countries in which they operate have enacted the issue of predicate offences and make themselves aware of any potential conflicts.

4.5. CTF is a further area to consider because terrorists and their supporters may commit crimes in order to finance acts of terrorism. Although the intended destination and usage of funds is different from money laundering, the behaviours and methods in which the funds are moved through the system are very similar. Operators should therefore be aware that the practical implementation of risk mitigation measures for terrorism financing and money laundering activity, will involve the monitoring of very similar activities and behaviours. For example, the 2017 National Risk Assessment highlighted that pre-paid cards were used as a means to fund the travel and purchase of materials by terrorists in recent UK attacks. This will in turn have a knock-on effect for internal policies and staff training.

5. Senior Management Responsibility

5.1. Senior management must be fully engaged in the decision-making process involved in the identification and assessment of risk. They must take ownership of the risk-based approach because along with the Money Laundering Reporting Officer (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: "A risk-based approach focuses effort where it is most needed and will have most impact. It requires the full commitment and support of senior management and the active cooperation of all employees"

5.2. It is common practice for jurisdictions to make it an offence where the applicable laws and procedures are not correctly followed. 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 e.g. a policy including, how to report, training and record keeping. The documenting of the policies and processes should be a reflection of their practical application and reviewed regularly to ensure that they remain up to date.

6. Working with Supervisory Authorities

6.1. 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's primary legislation (the Proceeds of Crime Act) and secondary legislation which applies to all AML-regulated sectors (Money Laundering Regulations 2017).

6.2. Operators will need to identify the appropriate Financial Intelligence Unit (FIU) which receives 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.

"It is common practice for jurisdictions to make it an offence where the applicable laws and procedures are not correctly followed. 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 e.g. a policy including, how to report, training and record keeping."

PART II

LBO Anti-Money Laundering Good Practice

Guidance issued by the ABB to its members engaged in retail & telephone betting. Adherence to the guidance is not a Gambling Commission Licensing Condition, but is an Ordinary Code Provision which means a court of tribunal can make reference to this guidance during the conduct of either criminal or civil proceedings.

1. Introduction to the LBO Sector

1.1. Betting shops are highly regulated, licensed, responsible businesses working together with the Gambling Commission, police, local authorities, and other businesses to tackle crime and protect the vulnerable in local communities across Great Britain.

1.2. In 2017, the UK Government provided the licenced betting office (LBO) sector with an exemption from the Fourth Anti-Money Laundering Directive (4AMLD) on the basis of proven low risk comparative to the wider financial sector. However, the sector must continue to demonstrate that it is fully complying and effectively enforcing risk mitigation practices to address the low-level risk that does exist within the sector.

1.3. An integral licensing requirement as set out by the Gambling Commission, is the need to keep crime, including financial crime, out of gambling. In 2016, the Gambling Commission updated its Licencing Codes and Conditions of Practice (LCCP) including the requirement under Section 12.1.1.

1.4. This version of the ABB's Guidance on Anti-Money Laundering and the Proceeds of Crime, includes guidance for operators on complying with updated licensing requirements (see above); as well as with industry codes resulting from work undertaken by the ABB and industry members since 2015, to identify and mitigate AML risks and to create a consistent application of controls across the sector.

1.5. These include controls to mitigate risks identified by the Gambling Anti-Money Laundering Group (GAMLG)'s AML Risk Assessment; Source of Wealth Guidance; consistent Retail ID Standards to be applied across the retail sector and the Gambling Commission's risk assessment of money laundering and terrorist financing risk within the British gambling industry. The GAMLG documents are not appended in this external Good Practice Guidelines for security reasons, but are available to operators via the ABB.

Licence condition 12.1.1
Anti-money laundering
Prevention of money laundering and terrorist financing
All operating licences except gaming machine technical and gambling software licences

1. Licensees must conduct an assessment of the risks of their business being used for money laundering and terrorist financing. Such risk assessment must be appropriate and must be reviewed as necessary in the light of any changes of circumstances, including the introduction of new products or technology, new methods of payment by customers, changes in the customer demographic or any other material changes, and in any event reviewed at least annually.

2. Following completion of and having regard to the risk assessment, and any review of the assessment, licensees must ensure they have appropriate policies, procedures and controls to prevent money laundering and terrorist financing.

3. Licensees must ensure that such policies, procedures and controls are implemented effectively, kept under review, revised appropriately to ensure that they remain effective, and take into account any applicable learning or guidelines published by the Gambling Commission from time to time.

a. Purpose

1.6. This guidance is periodically updated to reflect changes in the licencing and regulatory regime.

1.7. The purpose of this document is to provide guidance to those operating in the retail betting sphere, in relation to the responsibilities of betting operators and staff under the Proceeds of Crime Act 2002, Gambling Act 2005, and Terrorism Act 2000. It will also facilitate continued compliance with Anti-Money Laundering and Counter Terrorist Financing licencing and legislative requirements.

1.8. Adherence to this guidance is a requirement of membership of the Association of British Bookmakers as set out in the Responsible Gambling Code of Practice.

Definition of Money Laundering & Proceeds of Crime

1.9. Money laundering is traditionally understood to be the placement, layering and integration of money from criminal activity to disguise its original source, so that it appeared legitimate. This is distinguishable from the spending of the 'proceeds of crime', although both are regarded as money laundering activities. The law makes no distinction between the two activities and the action that any betting operator should take, and the penalties for non-action, are the same for both.

Definition of Terrorist Financing

1.10. Terrorist financing is either if a person intentionally uses, possesses or receives funds which they know, or suspect will be used for the purposes of terrorism.

1.11. Terrorist financing is in principle different from money laundering, even though once funds are in the financial system they may seek to be laundered in the same way. The Treasury, in its National Risk Assessment 2017, highlighted that methods used to raise funds for terrorism include legitimate means. While it is highly unlikely that betting shops will be in a position to detect whether terrorist funding is the purpose of any illicit activity, identified or suspected, any knowledge or suspicion is reported in the same way as money laundering. The UK Government have found no evidence of Terrorist Financing occurring via betting or gambling activity, however all operators should remain vigilant as to the risks that may arise.

b. Proceeds of Crime Act 2002 (POCA)

1.12. The Gambling Commission publishes guidance for operators on their Duties and responsibilities under the Proceeds of Crime Act 2002.

1.13. Broadly, the proceeds of crime are property from which a person benefits directly or indirectly, by being party to criminal activity. This criminal property could be stolen money, money from drug dealing or property stolen in a burglary or robbery. It could also include property which the criminal gains by spending the proceeds of criminal activity. For example, this could be where a criminal uses the money he earns from drug dealing to buy a car or a house, or the criminal spends the money he gained in a bank robbery to gamble in a casino or betting shop or the criminal spends funds that he has stolen from his employer.

1.14. There are 3 key offences that are applicable to everyone who knows or suspects that the property relates to the proceeds of crime.

Section 327 of POCA - Concealing

1. A person commits an offence if they
a. conceal criminal property:
b. disguise criminal property;
c. convert criminal property;
d. transfer criminal property;
e. remove criminal property from the UK.

How this might occur in a betting shop - the type of behaviour which may indicate an offence includes someone placing a bet and cashing in the winnings (converting), or someone placing cash into their betting account and not using it (concealing), or placing money in a betting account in Newcastle and someone else withdraws the funds in London (concealing, disguising, transferring).

1.15. **Section 328** of POCA provides that a person commits an offence if he or she enters into or becomes concerned in an arrangement which he or she knows, or suspects facilitates, by whatever means, the acquisition, retention, use or control of criminal property by or on behalf of another person.
How this might occur in abetting shop – a betting operator knowingly accepts stakes which are known to be the proceeds of crime.

1.16. **Section 329** of POCA provides that a person commits an offence if he or she:
a. acquires criminal property;
b. uses criminal property; or
c. has possession of criminal property.

How this might occur in a betting shop - this could be as simple as an individual using the proceeds of crime, for instance spending money obtained in a burglary in a High Street Betting Office.
These offences can be committed by any person, including betting operators and their employees, who have knowledge or suspicion that a customer is using the proceeds of crime.

There is a defence to the offences detailed above for a person to show that they made a protected or authorised disclosure under section 338 or 339 of the POCA, either for an employee reporting internally to their 'nominated officer' (i.e. Money Laundering Reporting Officer (MLRO)) and the MLRO reporting the knowledge or suspicion to the National Crime Agency (NCA).

The penalty upon conviction of sections 327, 328 or 329 of the POCA is a maximum term of 14 years imprisonment.

1.17. **Section 342** POCA – Prejudicing an investigation.

It is an offence for operators and their staff to disclose the knowledge of the existence of an investigation which could prejudice it. The offence can be committed before or after a report has been made.

This could include staff informing the individual who is the subject of the investigation, though staff are not prevented from making reasonable enquiries of a customer in respect of the background of their activity. It is also an offence to falsify, destroy or dispose of documents relevant to the investigation or cause this to happen.

There are several defences, one of which is that the person did not know or suspect that the disclosure is likely to prejudice the investigation.

The penalty upon conviction of section 342 is a maximum of 5 years imprisonment.

1.18. **Sections 337 to 339** Disclosures

All betting shops have legal obligations to ensure they have processes in place to ensure that employees report suspicious activity to their MLRO and that the MLRO assess and reports knowledge or suspicion to the NCA using a Suspicious Activity Report (SAR). These SAR reports must be made by the nominated officer i.e. MLRO or in the case of small operators, a person of reasonable standing in the business who can act as the nominated officer.

c. Gambling Act 2005

1.19. The gambling Act 2005, requires operators to keep crime out of gambling. This requirement is upheld and enforced by the Gambling Commission.

1.20. Before it grants a betting operating licence the Commission would have satisfied itself of the suitability of the business to hold an operating licence. This process would have included checks to ensure there was no association with the business or its key personnel with crime and/or money laundering. However, this does not prevent legitimate betting operators from being used by criminals to disguise the source of criminal property, or as an outlet for criminal spend. The key measure employed to help law enforcement agencies to detect criminal activity is to make it an obligation of any business (including betting operators) to report suspicious transactions.

1.21. As stated above, breaches of the POCA are reported to the NCA and fall to Police to investigate. However, the Gambling Commission is concerned that operators meet their duties and responsibilities under the POCA.
In October 2016, a new licence condition was included that requires:

1. *"Licensees to conduct an assessment of the risks of their business being used for money laundering and terrorist financing. Such risk assessment must be appropriate and must be reviewed as necessary in the light of any changes of circumstances, including the introduction of new products or technology, new methods of payment by customers, changes in the customer demographic or any other material changes, and in any event reviewed at least annually."*

2. *"Following completion of and having regard to the risk assessment, and any review of the assessment, licensees must ensure they have appropriate policies, procedures and controls to prevent money laundering and terrorist financing."*

3. *"Licensees must ensure that such policies, procedures and controls are implemented effectively, kept under review, revised appropriately to ensure that they remain effective, and take into account any applicable learning or guidelines published by the Gambling Commission from time to time."*

1.22. As outlined above (see b) the Gambling Commission also publishes advice on operator Duties and Responsibilities under the Proceeds of Crime Act 2002, with the latest edition published in October 2017.

1.23. Any court or tribunal, when coming to a decision about whether or not an operator had complied with its obligations under the POCA, would be entitled to consider whether or not an operator had followed the guidance, or any other formal guidance issued by the Commission.

1.24. It will also be necessary, for operators to be able to demonstrate to the Gambling Commission that staff training has taken place in this area. It is anticipated that further work will take place in 2017/18 as part of the GAMLG workstream programme.

1.25. Effective compliance with the Licence Condition 12.1.1. and adherence to the POCA Guidance, including the establishment and at least annual review of a Money Laundering Risk Assessment, should ensure compliance with operator requirements, under both POCA and licensing requirements. Risk assessments must be refreshed before the end of the 12-month period in the case of emerging business threat, product innovation, changes in legislation etc.

d. Terrorism Act 2000

1.26. The key sections of the Terrorism Act of which betting operators are required to comply with are detailed below. Terrorist financing is in principle different from money laundering, even though once such funds are in the financial system, they may seek to be laundered in the same way. While it is highly unlikely the betting shops will be in a position to detect whether terrorist funding is the purpose of any illicit activity identified or suspected, any knowledge or suspicion is reported in the same way to NCA in accordance with the obligations under the POCA.

1.27. **Section 15 - Fund Raising**

1. A person commits an offence if he:
   a. invites another to provide money or other property, and
   b. intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism.

2. A person commits an offence if he:
   a. receives money or other property, and
   b. intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism.

3. A person commits an offence if he:
   a. provides money or other property, and
   b. knows or has reasonable cause to suspect that it will or may be used for the purposes of terrorism.

1.28. **Section 16 - Use and Possession**

1. A person commits an offence if he uses money or other property for the purposes of terrorism.

2. A person commits an offence if he:
   a. possesses money or other property, and
   b. intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism.

1.29. **Section 17 - Funding Arrangements**

1. A person commits an offence if:
   a. he enters into or becomes concerned in an arrangement as a result of which money or other property is made available or is to be made available to another, and
   b. he knows or has reasonable cause to suspect that it will or may be used for the purposes of terrorism.

1.30. **Section 18 - Money Laundering**

1. A person commits an offence if he enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property:
   a. by concealment
   b. by removal from the jurisdiction
   c. by transfer to nominees, or
   d. in any other way.

2. It is a defence for a person charged with an offence under subsection (1) to prove that he did not know and had no reasonable cause to suspect that the arrangement related to terrorist activity.

1.31. **Section 19 - Disclosure of information: duty**

This section applies where a person:

a. believes or suspects that another person has committed an offence under any of the sections 15 to 18 of the Terrorism Act 2000, and
b. bases his belief or suspicion on information which comes to his attention in the course of a trade, profession, business or employment.

The person commits an offence if he does not disclose to a constable as soon as is reasonably practicable:

i. his belief or suspicion, and
ii. the information on which it is based.

1.32. **Section 20 Disclosure of information - Permission**

A person may disclose to a constable:

a. a suspicion or belief that any money or other property is terrorist property or is derived from terrorist property:
b. any matter on which the suspicion or belief is based.

The penalty upon conviction of any offence under sections 15 to 18 of the Terrorism Act 2000 is a maximum term of 14 years imprisonment, a fine, or both.

2. Internal Controls (processes and procedures)

2.1. All operators have a responsibility to ensure the proper and effective implementation of AML controls. Larger operators will have appointed Money-Laundering Reporting Officers (MLRO). In smaller operators, the licensee has overall responsibility for AML controls and procedures.

2.2. As of 1 January 2018, it has been agreed, on a cross-industry basis, that minimum standards will be implemented in relation to customer due diligence. The trigger factors included in these minimum standards should be viewed in addition to the existing risk-based approach, and not in place of it. Operators should be continually curious as to potential risks. The ambition of this move is to ensure a consistent approach to AML and to ensure that at whichever operator a customer gambles, the communication that they receive at particular trigger points, is the same.

2.3. All staff should be aware of key indicators and types of activity that could trigger the need for further information to be obtained from a customer about their identity and/or source of the money they are gambling with. The questions that should be considered at the appropriate levels in relation to individuals who spend significant sums of money in their shop include:

a. Are further KYC checks, such as asking for ID appropriate?

b. Does the customer have an account and what does the data tell us? Does the customer use a wallet across platforms, but deposit or withdraw in a non-remote environment? Additionally, is the person withdrawing or depositing in the account, the same person as the name on the account?

c. Does the customer attempt to break the payment loop, i.e. paying in cash and requesting winnings via a debit card, or switching the debit card used when placing and collecting winnings?

d. Are the staking and loss/win levels a cause for concern in terms of anti-money laundering and responsible gambling?

e. Is the customer spending out of area notes, e.g. Scottish or Northern Irish notes in England or Wales?

f. If a customer is spending increased amounts of money on machines, does this give reason to be concerned? Is there evidence of dyed note use in gaming machines? Are they trying to exchange TITO slips from other retail outlets?

g. Is the customer employed and can this be verified?

h. Does the customer appear to have a lavish lifestyle with no visible means of support?

i Is there any family wealth that accounts for the customer spend and do they have access to the funds?

j. Have they had a big win and are they using that money to fund their gambling?

k. Is there local knowledge to suggest they have had any criminal convictions, or suspicion of links to crime?

l. Is the customer placing bets on behalf of someone else? If yes, what is known about the person to whom the bets belong?

m. Are there any local newspaper articles that give any cause for concern? Is the customer averse to the use of loyalty cards or participation in hospitality events?

2.4. If when answering these questions, there are any concerns in relation to the individual, it must be reported to the MLRO, head office monitoring function or senior management of the relevant betting operator as appropriate.

3. Risk Based Approach and GAMLG's Risk Assessment Document

a. Gambling Commission approach to enforcement

3.1. The Gambling Commission adopts a risk-based regulatory approach to enforcement, including in relation to Anti-Money Laundering and POCA requirements. This means that the Commission concentrates its efforts on those operators and issues, where the impact of failure to deliver the licensing objectives would be highest. Their activities include, but are not limited to:

a. *"Promoting operators' requirements to discharging their responsibilities under POCA..., through engagement with operators on a one-to-one basis and through meetings and multi-agency forums to identify and promote best or good practice."*

b. *"Publishing formal anti-money laundering advice" (a money laundering risk assessment is also published – see latest version)*

c. *"Monitoring the submission of suspicious activity reports (SARs), and law enforcement activity."*

d. *"Undertaking compliance assessments of operators' understanding and application of money laundering risk management controls."*

e *"Producing risk assessments to assist the planning of compliance assessments."*

f *"Ensuring that Commission staff are equipped to take appropriate decisions on the suitability of anti-money laundering systems and controls".*

b. Risk Assessment

3.2. LCCP article 12.1.1. sets out the requirement for all operators regulated by the Gambling Commission, to complete a risk assessment of money laundering risks and controls on an annual basis as a minimum.

3.3. The Gambling Commission, in its guidance on Duties and Responsibilities under POCA, details that risks should be assessed on a number of questions, including:

a. What risk is posed by the business profile and the profile of customers using the gambling facilities?
b. Is the business high volume, consisting of many low spending customers?
c. Is the business low volume, with high spending customers?
d. Is the business a mixed portfolio, that is customers are a mix of high spenders and lower spenders and/or a mix of regular and occasional customers?
e. Are procedures in place to monitor customer transactions across outlets, products and platforms and mitigate any money laundering potential?
f. Is the business local with regular and generally well-known customers?
g. Are there a large proportion of overseas customers using foreign currency, or overseas based bank cheques or debit cards?
h. Are customers likely to be engaged in a business which involves significant amounts of cash?
i. Are there likely to be situations where the source of funds cannot easily be established or explained by the customer?
j. Is the majority of business conducted through customer accounts, or some other contractual arrangement?
k. Is there a local clustering of gambling outlets, which makes it easier for a person to launder criminal proceeds over multiple venues and products?
l. Does the customer have multiple, or continually changing sources of funds (for example, multiple bank accounts and cash, particularly where the funds are in different currencies or uncommon bank notes)?
m. Are patterns of play, or a high spend profile, linked to specific sporting events?

3.4. Any risk assessment should be continually reviewed, at least annually, to ensure that it continues to cover all elements of possible risk and can be updated where necessary.

3.5. A risk-based approach should be integral to operator management, with all staff aware of their responsibilities in mitigating money-laundering risk and trained appropriately. ABB-member independent operators receive online training commissioned by the ABB.

3.6. Any risk assessment should align with the following key objectives:

a. **Risk identification -** Analysis of risks particular to you as an operator

b. **Risk mitigation -** The application of measures which effectively mitigate the identified risks

c. **Risk monitoring -** Ensuring there are sufficient review systems in place to ensure that risks are identified and updates made to company policies to reflect any change in operator risk profile

d. **Documentation -** Having internal controls in the form of policies and procedures to ensure that staff are able to carry out their AML obligations

e. **Risk-review -** Evaluating the application of controls and procedures to ensure that policies are fit for purpose.

3.7. The risk assessment should accurately document the exposure of the business to money laundering and the spending of the proceeds of crime and terrorist funding risks. Final accountability sits with the licence holder and the Gambling Commission may move to suspend a licence, should it find a risk assessment is unfit for purpose.

3.8. The Gambling Commission has been clear that it will not accept a 'tick box' approach to compliance with Anti-Money Laundering requirements and that it will be looking closely at the effectiveness of controls in place.

c. Risk based approach of POCA

3.9. POCA uses a risk-based approach for implementation, including a number of discrete steps to assess the most proportionate way to manage and mitigate the money laundering risks faced by an operator. These steps require an operator to:

a. Identify the money laundering risks that are relevant to the operator

b. Design and implement policies, procedures and controls to manage and mitigate these assessed risks

c. Monitor and improve the effective operation of these controls

d. Record what has been done, and why.

Operators should be cognisant of emerging threats and risks as well as the latest information released by the Gambling Commission. Where innovation within the business takes place, consideration should be given as to any resulting money laundering risks that may arise.

3.10. Guidance on POCA 2002 published by the Gambling Commission (Oct 2017) notes that the risk-based approach means that operators focus their resources on the areas which represent the greatest risk. The Gambling Commission expects that operators have AML systems and procedures in place and in line with the LCCP and notes that a breach of these conditions can constitute a criminal offence.

3.11. Where a customer is assessed as presenting a higher risk, additional information in respect of that customer should be collected. Such information should include an understanding of where the customers' funds and wealth have come from. The need to 'know your customer' is particularly relevant here. Operators should make use of 'open source' information, including press reports, to carry out these checks. Consideration around the validation of income/wealth should also be given.

3.12. A risk-based approach requires the full commitment and support of senior management, and the active co-operation of all employees. It should be part of the operator's philosophy and reflected in policies, procedures and controls.

d. GAMLG Risk Assessment

3.13. In April 2017, the Gambling Anti-Money Laundering Group (GAMLG), conducted its own risk assessment of money-laundering and terrorist financing risk across the retail betting and remote operator sectors. This document has been independently verified by anti-money laundering experts and sets out best practice. The GAMLG Risk Assessment informs the guidance presented here.

3.14. The GAMLG produced Risk Assessment follows the suggested outline as set out by the Gambling Commission, including an assessment of risks linked to:

- Country or geographic risk;
- Customer risk;
- Transaction risk (including means of payment);
- Product risk;
- Employee risk.

3.15. **Country risk**

Some countries pose an inherently higher money laundering risk than others. The UK is not considered high risk and country-risk is not regarded as a significant risk factor in LBOs. However, operators should be vigilant for customers from high-risk jurisdictions.

3.16. **Customer risk**

A requirement to assess the potential ML risks posed by a customer, or category of customers, is critical to the development and implementation of a risk-based AML framework. Operators should use their own criteria to determine whether a particular customer poses a higher risk.

3.17. Based on these criteria, operators should seek to determine whether a particular customer poses a higher risk and the potential impact of any mitigating factors on that assessment. Categories of customers whose activities may indicate a higher risk include:

a. unknown or anonymous customers;

b. customer appearance inconsistent with spend;

c. requests for receipts of winning bets;

d. the use of 'runners' – individuals suspected of acting on behalf of a third party, but does not disclose that information;

e. requests to pay out winnings via a different payment method than was originally used to place the bet or gamble with;

f. customers using multiple premises (same operator) with a view to legitimising large quantities of cash derived from criminal activities;

g. customers using multiple premises (different operators) with a view to those wishing to legitimise funds, thus minimising the risk of being detected;

h. drastic changes or significant increases in gambling behaviour;

i. high-value staking customers via either a single transaction or cumulative stakes;

j. use of LBO to withdraw online funds (where account play is in place); and

k. unusual activity, i.e. a customer in possession of a 'carrier bag' full of high-denomination notes.

3.18. **Transaction/payment risk**

Operators should consider aspects such as products, service, game, and activities that could be used to facilitate money laundering. Operators should also consider the means by which customers stake their bets or gamble on gaming machines when undertaking the risk assessment, for example:

a. use of cash;
b. depositing of dye-stained bank notes in gaming machines;
c. unusual activity, including use of out-of-area banknotes e.g. significant sums of Scottish banknotes in England or Wales; the use of pre-paid cards; attempting to cash TITO slips from other premises.

3.19. **Product risk**

Risk will vary according to product use within the LBO environment. The GAMLG considers these variations, including specific vulnerabilities relating to gaming machines and self-service betting terminals.

3.20. **Employee risk**

Employees for example, in-shop, at headquarters, in trading or compliance teams, or higher up the management scale; may attempt to carry out acts of collusion, or manipulate records, in order to facilitate money laundering activity. It is possible that employees who live and work in the same community, would be at risk of helping friends or associates to launder criminal funds and accepting cash bribes or incentives for doing so. Employee risk includes, but is not limited to:

a. employee collusion;

b. non-compliance with AML/CTF controls due to commercial considerations;
c. staff knowledge including addressing issues around adequate training of staff; and
d. unusual activity e.g. employee active involvement or blatantly turning a blind eye to the presence of red-flag indicators in customer activity.

4. Customer Verification and Due Diligence

4.1. The Gambling Commission makes clear that whilst some operators may find their AML requirements challenging, particularly in relation to the management of customer relationships… it is incumbent on operators to have policies and procedures in place to ensure that they comply with all relevant provisions of POCA (and the Act and the relevant licence conditions and codes of practice)[2].

4.2. Operators' policies and procedures should be clear as to when additional information is required from the customer, to both verify their identity and validate their wealth income in line with the customer risk posed. The policies and procedures should also be clear as to how customer information is reviewed and appropriate decisions taken.

4.3. In the first instance, open source tools can be used to conduct research into the customer, for example via:

a. Company checks
b. Professional checks
c. Salary checks
d. Property ownership
e. Property value & profile checks
f. Insolvency and bankruptcy checks
g. Court case/crime searches
h. Background 'credit' checks
i. Internet searches
j. Social media checks
k. Inheritance checks

4.4. Where the need for Source of Wealth or Funds evidence has been established, and open source checks are unavailable or insufficient, customers may be approached to provide documentary evidence. This can also take place in instances where there is concern, but not necessarily suspicion. This information can also help to inform any report to the MLRO or senior management.

4.5. The following best practice methods might be adopted by operators where the need to establish customer identity:

a. **Loyalty cards/accounts -** encouraging or incentivising account registration (where possible) has been used as a means of capturing and verifying customer identity.

b. **Debit card and supporting evidence -** where a customer uses a debit card, staff might be encouraged to view that card to obtain the customer's name. This method is only suitable when the card has been used by the customer over a prolonged period to ensure that over reliance isn't placed on fraudulent or stolen card.

c. **Debit card verification -** physical ID may be requested at the point of debit card use on the premise of validating ownership of the card.

d. **Hospitality -** operators may consider requiring customers to provide proof of identify as part of hospitality processes. This information can then be referenced as part of a customer review.

e. **Direct ID request -** in the event that a customer identity remains unconfirmed, the customer should be asked to provide physical proof of ID. This might be requested on security grounds, or as part of hospitality as appropriate.

4.6. It is ultimately a matter for individual operators to consider the route that best reflects the individual customer in the context of the risks perceived.

4.7. Once obtained, the evidence gathered pertaining to a customer's source of funds, needs to be evaluated to ensure the operator is confident that any level of concern or suspicion is mitigated by the information gathered during the SOW check.

4.8. Strong evidence may include:

a. **Sufficient cash/assets** in declared company accounts where the customer is a beneficiary, or established company/company portfolios with physical or virtual premises which appears capable of supporting customer patterns

b. **Latest payslips**

c. **P60/Tax returns**

d. **Proof and details** of any award of payment (i.e. inheritance, lump sum)

e. **Bank statements** where there is an identifiable source of funds into the account (i.e. not transfers from other personal accounts)

f. **Gambling account statements** (or equivalent) showing winnings obtained from other operators. This should only be regarded as strong evidence where a full account history is provided showing a clear benefit from gambling activity. The responsibility for KYC remains with each individual operator

g. **Evidence of a property rental portfolio**

h. **Shareholding information**

2 Duties and responsibilities under the Proceeds of Crime Act 2002 / Advice to Operators (excluding casino operators), Third Edition, Gambling Commission, November 2016

4.9. Weaker evidence may include:

a. **One off payslips**

b. **Screen shots of bank balances** including transfers from unidentifiable sources

c. **Winnings obtained from other gambling operators** where the full customer history is not available to establish the full extent of the customer benefit

d. **Property ownership/prices**

e. **Confirmation that a customer runs a business, but no business financials reported,** and/or which does not appear capable of supporting the customer's spending patterns.

4.10. Weaker evidence should not be used in isolation and should only be considered sufficient when reviewed in conjunction with 'stronger' evidence.

4.11. The majority of cases are likely to be assessed on merit, to determine the worth of the documentation provided or information located and its validity. All information held about the customer, including that gained from open source checks, must be considered in any assessment.

4.12. Operators should ensure that clear processes are in place to periodically re-review customers, subject to SOW checks. This should include a re-assessment of customer risk and evaluation of whether the evidence held continues to match the customer profile.

5. Suspicious Activity, Reporting and Data Protection

a. Reporting obligation

5.1. Betting operators and their employees have an obligation to report when they have **knowledge** or a **suspicion** that another person is engaged in money laundering, utilising the proceeds of crime or terrorist funding.

b. What is knowledge?

5.2. Knowledge means **actually knowing** something to be true. In court, it must be shown that the individual in fact knew that a person was involved in money laundering. Knowledge can be taken from other circumstances - for example a failure to ask obvious questions may constitute 'knowledge'.

c. What is suspicion?

5.3. Suspicion has been defined as being **beyond speculation** and based on **some foundation.**

5.4. The person must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice. The suspicion does not need to be based on actual facts, but there needs to be a satisfaction beyond speculation.

5.5. To have a suspicion it is not necessary to have evidence that the customer is using the proceeds of crime, or know what the originating criminal offence is. A suspicion might be based on picking up on something unusual or establishing that facts do not tally up. However, it must be remembered that not all unusual behaviour will constitute money laundering or terrorist funding – the MLRO would need to assess the whole picture to determine whether an external report is required.

5.6. In addition, it is important that the major betting operators have internal processes in place at head office, which monitor any significant shop business fluctuations, facilitate liaison between trading and compliance teams liaise on any suspicious increase in turnover and gross win and ensure such developments are investigated properly on grounds of anti-money laundering and responsible gambling.

5.7. Examples of these types of scenarios that could happen in betting shops are detailed in the Operators version of this document. Each scenario indicates the type of activity that should be raised with the MLRO:

d. Suspicious Activity Reports (SARs)

5.8. In all cases where knowledge or suspicion is held, they must be reported internally by employees to the MLRO, who records and documents the reports, either manually or electronically.

5.9. The records should include full details of the customer, including postal address and postcode, transaction history and the reasons for suspicion or knowledge.

5.10. The MLRO is then responsible for investigating and determining whether there is knowledge or if it can be reasonably suspected that the funds are the proceeds of crime, linked to money laundering or terrorist financing.

5.11. The MLRO is required to determine whether the matter should be relayed to National Crime Agency (NCA). If it is determined that a report should be made, this will need to be made via the prescribed SAR process.

5.12. When there is knowledge or suspicion of an acquisitive crime, a decision may be required to determine whether the matter should be reported to the local police force. Regardless of whether or not a report is made, the obligations under the POCA and Terrorism Act must be considered. If there is knowledge or suspicion related to the proceeds of crime, money laundering, or terrorist financing, the MLRO must submit a SAR to the NCA. Where the matter has been reported as a crime, it is encouraged to include the Crime Reference Number in the top line of the 'Reason for Suspicion' field of the SAR.

5.13. As stated before, showing that an employee has reported internally to the MLRO and that the MLRO reports the knowledge or suspicion to the NCA, provides both the employee and MLRO a defence under the statutory provisions.

e. Timing of SARs

5.14. All SAR disclosures to the NCA, need to be made as soon as it is reasonably practicable, after the knowledge, suspicion or reasonable grounds have been determined. Failure to do so, where the MLRO either knows the identity of the suspected criminal, knows the whereabouts of the criminal property, or believes that the information on which the suspicion was based, may assist in locating the suspect, or laundered funds; could lead to MLRO liability and a prison sentence of up to five years and/or a fine.

5.15. Operators are reminded that reporting suspicious activity before, or after the event, are not equal options which can be chosen between.

5.16. Where a report is made after the offence has taken place, operators will only have a defence if there is a reasonable excuse, as to why the report was not made beforehand.

5.17. To these ends, the NCA operates a 'consent' regime (called Defence under POCA), where an operator can seek 'consent' before proceeding with a transaction, which may otherwise be a prohibited act under the POCA.

5.18. Therefore, if a customer is requesting to place a bet, and knowledge or suspicion exists, then reports should be made to the MLRO, who in turn should request consent from the NCA to proceed with the transaction. As set out in the Gambling Commission's October 2017 Duties and responsibilities under the Proceeds of Crime Act 2002, "it is an offence for a nominated officer to agree to a transaction or activity going ahead within the seven-day notice period calculated from the working day following the date of disclosure, unless the NCA provides a defence (gives consent)".

5.19. However, UK Gambling Commission guidance recognises that gambling transactions are very immediate, and in these circumstances, it may be incredibly difficult to form knowledge or suspicion or obtain consent prior to or during a transaction. Therefore, it may be reasonable to report after the transaction has taken place via an ordinary SAR. It should be noted that consent cannot be obtained after the event.

f. Consent Requests (Defence Under POCA)

5.20. Considering the above, in the betting industry, it is more probable for a transaction (i.e. bet) to be made, leading to the formulation of a knowledge or suspicion thereafter, leading to a report to the MLRO and possible report to the NCA.

5.21. If the individual still has 'winnings' to collect and knowledge or suspicion is held in these circumstances the employee should refer the matter to the MLRO, who should consider disclosing a SAR to the NCA and requesting consent for payment. In these circumstances, the operator must not allow payment to be made until a response from the NCA has been received, or otherwise if consent has not been given within seven working days.

5.22. If in doubt the Consent Team at the NCA who manage the resolution of consent SARs may be contacted

g. SAR reporting process

5.23. Operators can submit SARs via the online facility provided by NCA. The NCA website can be accessed at http://www.nationalcrimeagency.gov.uk/ for guidance on completing and submitting a disclosure. The website directs operators to SAR Online, which is designed for use by those required by the POCA and Terrorism Act 2000 to submit SARs. The online system is designed to allow SARs to be constructed and submitted in a secure and efficient manner.

5.24. In order to register, new users require an active email account, as this is used as the SAR Online user identification. No two users can use the same email address. It is recommended the registering user be an official, responsible for Anti-Money Laundering (AML) compliance within the organisation, such as the MLRO, or otherwise the individual who has responsibility for the detection and reporting of suspicious activity.

5.25. Whilst 97% of SARs are made to the NCA are completed via the online facility, the NCA do allow for SARs to be posted or faxed. Post or fax is strongly discouraged for consent SARs as this is likely to delay the process.

5.26. There is also a dedicated support team available during office hours to deal with any SAR Online enquiries. The support team can be contacted by telephone on 020 7238 8282 and selecting option '3'.

5.27. Leaflets are also available from the NCA that provide advice and relay best practice when making a SAR.

5.28. Following guidance published in the Gambling Commission's second edition of the advice document 'Duties and Responsibilities under the Proceeds of Crime Act 2002' (October 2017), operators are required to provide the Commission with copies of SARs URNS. This can be done via the Gambling Commission Key Event Portal.

h. SARs that are not disclosed

5.29. All SARs which are considered and not disclosed under the legislation will be recorded and retained, in order that any future continuing activity can be monitored and may be used as intelligence for any subsequent disclosure. It is advisable that the reasons for not submitting a SAR should be noted on the record.

i. Termination of a customer relationship

5.30. Operators need to address how to approach a suspected customer and whether future transactions should be allowed (for example after consent is received to allow a transaction to proceed or after a general SAR has been raised).

5.31. It must be remembered that although a SAR may be relevant to one transaction, there may be less concern about future transactions. However, each transaction should be considered on a case by case basis and reports made accordingly.

5.32. Equally, suspicion may increase and become actual knowledge of laundering (or consent may be refused for a particular transaction), in which case consideration needs to be given on whether operators want to sustain the risk of allowing further transactions (raising SARs where appropriate). However, the reporting defence is not intended to be used repeatedly in relation to the same customer, so termination of the business relationship needs to be considered to protect operators from any criminality and reputational damage.

5.33. Business relationships can be terminated as determined by the operator, and provided that this is done sensitively, should not prejudice an investigation. Operators should liaise with the NCA to establish the best way to turn customers away. In some cases, law enforcement may request that a relationship with a customer continue whilst investigation is underway and consent is in place.

j. Data protection

5.34. At all times, operators should be cognisant of the need for safe storage of customer data in line with the Data Protection principles. Information should only be sought for the declared purpose and should not be retained for longer than necessary.

6. Employee

a. Training

6.1. All operators must take necessary steps to ensure that employees are aware of the money laundering risks and obligations. This should include knowledge of what to do to ensure that customer details who are subject to a know your customer (KYC), source of wealth (SOW) or source of funds (SOF) check are forwarded to the nominated office, manager or other employee responsible for AML activity and communication with the National Crime Agency (NCA).

6.2. Operators should consider the frequency of the training that is required as well as assessing individuals' competency. Training records for employees are recommended. Larger operators should consider more bespoke training for individuals whose role primarily entails Compliance and/or AML activities.

6.3. For ABB-member independent members, an online training module is available for use by all staff. Additional advice is also available on the NCA website. Ensuring all employees are regularly reminded of their responsibilities with regards mitigating money-laundering risks, will help ensure the overall success of the operator's AML strategy.

b. Screening

6.4. Reflecting Gambling Commission requirements, screening of employees should take place at the senior level. Employees suitable for screening include those responsible for:

a. Overall strategy and delivery of gambling operations;

b. Financial planning, control and budgeting;

c. Marketing and commercial development;

d. Regulatory compliance;

e. Gambling related IT provision and security; and

f. Where there is a regional structure or area manager structure in place, those where responsibility for gambling operations is delegated.

6.5. Pre-employment screening can take the form of employment references, identity and address checks, which must all be successful prior to an individual starting employment with the company. It is recommended that senior employees be subject to enhanced checks on an ongoing basis.

6.6. An additional ongoing review, can include a shop activity review to ensure that suspicious activity is not linked with a particular employee or employees.

c. Awareness

6.7. Employee training is fundamental to ensuring that staff remain aware of ML risks. Independent ABB members have access to online training modules which will facilitate employee awareness. Steps should be taken to ensure that staff repeat the module on a periodic basis to ensure continued awareness, including updated policies.

d. Alertness

6.8. Training should include information to assist employees in understanding the key 'red flag indicators', across both gaming machines and over-the-counter play, which help to identify signs of potential money laundering activity.

6.9. All employees need to be aware of these triggers and encouraged to escalate concerns within the business to the Money-Laundering Reporting Officer or senior management, depending on the structure in place within the company.

6.10. Should a suspicion be formed by the MLRO, or senior manager following a review of the activity, it is then their responsibility to submit a SAR to the National Crime Agency.

7. Record Keeping

7.1. Good record keeping is integral to ensuring that suspicious activity and staff/customer interactions are logged for potential use in any SAR submission and potential subsequent liaison with law enforcement agencies.

7.2. Effective record keeping is required in order to comply with Gambling Commission guidance including customer behaviour across different parts of the business, e.g. electronic gaming machines, over-the-counter, and, where relevant, remote betting operations.

8. Electronic Gaming Machines (EGMs) and Self-Service Betting Terminals (SSBTs)

8.1. Electronic gaming machines in betting shops are programmed with AML software to detect suspicious activity. As stated above, effective monitoring and record keeping, across various products and payment points, is key to ensuring the effective mitigation of money-laundering risk.

8.2. As of 1st January 2018, all operators are required to request to see customer photo ID from previously unidentified customers, for circumstances set out in the internal version of this document.

8.3. Where these circumstances exist, photo ID will be required:

1. Prior to payment where tickets are yet to be paid; or otherwise
2. On the customer's next shop visit.

8.4. It is recognised that any request for ID prior to a payment, may be deferred where there is a perceived threat to the safety of shop colleagues.

8.5. To assist operators and shop colleagues in explaining to customers the reason for ID request, a cross-industry leaflet has been agreed and designed. The intended purpose of the leaflet is to increase customer compliance and allow for operators to manage customer risk and avoid moving customers elsewhere. The leaflets will be provided by the ABB to independent operators. Major operators are responsible for their own supply of these leaflets.

9. Conclusion

9.1. The retail betting industry was categorised as 'low risk' for money laundering in the 2015 UK Government National Risk Assessment, and subsequently in the updated version of that document published in October 2017 comparative to the financial services sector. The Gambling Commission's Risk Assessment concluded that the retail betting sector is 'high' when comparing sectors within the gambling industry.

9.2. There is cross-industry acknowledgement of the need for the effective implementation of controls, regular risk assessments to be carried out, and continual monitoring to ensure that controls remain fit for purpose, including regarding new innovations within the industry.

9.3. The retail betting industry is committed to the proper and effective implementation of anti-money laundering controls to ensure that risk within the sector remains categorised as 'low'.

PART III

Remote Gambling - Anti-Money Laundering Good Practice

GAMLG
GAMBLING ANTI-MONEY LAUNDERING GROUP

1. Introduction

1.1. 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. Application of Internal Controls (processes & procedures)

2.1. Internal Controls are the key link between the risks identified in the AML/CTF risk assessment and the practical implementation of mitigation measures. They will usually take the form of internal processes and procedures.

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

2.3. Internal controls in the form of written processes and procedures are only effective when consistently followed in practice. It is therefore advisable that operators put in place measures to monitor compliance with internal controls to ensure that the practical implementation of mitigation measures remain effective and appropriate. This may be in the form of sample checks, exception reporting or other auditing measures. Again, the risk-based approach should guide operators in determining which checks to put in place and in what format, based on where the highest risks are.

3. Risk Based Approach and GAMLG's Risk Assessment Document

3.1. A risk-based approach takes a number of discrete steps in assessing the most cost effective and proportionate ways to manage and mitigate the money laundering and terrorist financing risks faced by the operator. This is done by way of a documented risk assessment, which then forms the core of the measures put in place by the operator to mitigate the money laundering and terrorist financing risks they face. Conducting a risk assessment for AML/CTF, is not a one-off exercise, it is an ongoing process.

3.2. 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 the securing of the commercial viability of the operator. In short, any measures that are applied must be proportionate to the risk presented and effective in addressing that risk.

3.3. A risk-based approach is outlined by FATF and the 4th Anti-Money Laundering Directive and assists to ensure that the procedures, systems and controls designed to mitigate the assessed Money Laundering/Terrorist Financing (ML/TF) risks, are appropriate and proportionate to these risks, whilst providing an effective level of mitigation.

3.4. Any risk-based model adopted should be continually reviewed to ensure that it continues to cover all elements of possible risk and is updated where necessary. This methodology in turn ensures the best use of resources, value for money, and highlights the factors that represent the greatest risks. It is important to use a variety of sources to evaluate risk, such as collating information on current process and procedures and measuring effectiveness to ensure that valuable resources are being correctly directed and applied and have not become overwhelmed and ineffective.

3.5. How a risk-based approach is actually implemented is dependent upon the operator, its size and business structure. In order to meet the requirements of the Directive, these guidelines aim to give a high-level overview of the operation of a model that builds on the risk-based approach, advocated by the FATF and the Directive.

3.6. However carried out, a risk-based approach needs to be part of the operator's philosophies, and as such reflected in its procedures and controls. There needs to be a clear communication of policies and procedures to staff, along with robust mechanisms to ensure that they are carried out effectively. Any weaknesses should be identified, and improvements made wherever necessary. In short, an operator needs to have a compliance culture which feeds down from the Directors to frontline staff.

3.7. The following steps should be followed when undertaking a risk assessment:

1. **Risk Identification -** Analysing the operator's business structure and practices in order to identify areas of potential ML/TF risk

2. **Risk Mitigation -** Applying measures effectively to mitigate the identified risks

3. **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

4. **Documentation -** Having internal controls in the form of policies and procedures to cover the identified risks and deliver accountability from the Board and Senior Management down

5. **Risk Review -** Monitoring and evaluating the risks identified to ensure the effective operation of internal controls is in place to mitigate the risk.

3.8. The risk assessment should accurately document the exposure of the business of a remote gaming operator 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.

3.9. Having conducted a risk assessment, the remote operator is then in a position 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.

3.10. As money laundering and terrorist financing threats change constantly, 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. Operators should ensure that their risk model is reviewed and if necessary updated regularly to reflect any appropriate changes in risk levels, policies or internal controls. It is important to have systems in place that provide an overall picture of customer behaviour as part of the business relationship.

3.11. It should be noted that financial sanctions (i.e. the requirement to freeze assets of individuals identified as subject to financial sanctions) fall outside the risk-based approach. Similarly, there are no risk-based provisions around the reporting of suspicious activity, once identified. Both must therefore be managed independently of the operator's risk assessment.

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

1. **Customer Risk (see a & b)**

2. **Product/Services Risk (see c & d)**

3. **Transaction/Payment Risk (see e & f)**

4. **Geographical Risk (see g & h)**

5. **Behavioural Risk (monitoring) (see i)**

a. Assessing Customer Risk

3.13. This risk category includes types of customers and the style of business relationship. Customer types may include individual accounts or trade accounts. Each customer classification has distinct risks and therefore requires tailored mitigation strategies. The risk assessment should consider what information the operator holds about the customer and that the information is consistent and up to date.

b. Mitigating Customer Risk

3.14. To assist in the mitigation of the risk posed by Politically Exposed Persons (PEPs), operators should have a risk-based policy on how and when to ascertain whether any customers are considered to be PEPs.

3.15. It is important that the process for the ongoing monitoring of customer risk is continual through the lifetime of the customer relationship. This helps to ensure that any changes which may affect the risk posed by the customer are acted upon to ensure that there is limited exposure to ML/TF risk arising from out of date customer information.

3.16. Operators can look to mitigate the risk posed by customers, by conducting a review of their customer base to identify groups of customers. Once these groups have been identified, the potential risks posed by each distinct customer group can be assessed and mitigated. For example, due diligence requirements for trade accounts will differ to those of individual customers, due to the requirement to identify the beneficial owner.

c. Assessing Products/Services Risk

3.17. When assessing product/service risk, 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 potential for collusion and chip dumping by customers, whilst slots and bingo may be seen to be lower risk games, requiring minimal, if any, ML risk mitigation beyond those applied at the customer level. Any apparently irrational funds movement should attract greater attention e.g. between different products without any apparent reason.

3.18. 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 as the money may be passed from one customer to another and therefore necessitate the implementation of additional customer due diligence procedures in relation to those involved.

3.19. It is not uncommon for customers to have multiple payment methods, and for them to gamble across different platforms and interact with customers registered with another operator. This introduces a risk of the product used by the customer, allowing for the transfer of funds between customers on different networks, making it difficult to track customer funds.

d. Mitigating Products/Services Risk

3.20. The monitoring of identified high risk behaviours is a key factor in preventing ML/TF activity.

3.21. One of the key ways to mitigate the risk posed by products which involve a platform, or allow player to player transfers, is to have channels of communication between the operator and the platform operators; this may be via agreed reporting suites or by referral of customers where there is a concern.

e. Assessing Transaction/Payment Risk

3.22. Deposit and withdrawal methods into and from a customer's gaming account are now offered from a wide variety of sources, including credit/debit cards, bank transfers, wire transfers and prepaid cards. These are key factors to consider when identifying transaction/payment risk.

3.23. Different payment methods will involve the completion of differing checks on the provenance of the funds, which in turn will also have undergone due diligence to a greater or lesser degree by the payment provider.

f. Mitigating Transaction/Payment Risk

3.24. An evaluation of the features of the different payment methods offered, should constitute part of the assessment of money laundering risk to identify any particular features which may be of higher risk, for example, whether the payment method allows cash deposits.

3.25. It is less common in the online gambling industry for direct 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.

3.26. Operators should try and avoid simply acting as banks, i.e. customer accounts should be used to facilitate gambling, not as a substitute for conventional bank accounts. A review of the payment methods offered to see whether cash deposits are permitted by the payment provider, will also assist in addressing the potential risk.

g. Assessing Geographical Risk

3.27. When looking to assess geographical risk, 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.

h. Mitigating Geographical Risk

3.28. 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 invaluable in assisting 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.

i. Monitoring of Customer Behaviour

3.29. The further that a relationship progresses with a customer, the more the operator will, or should know about that customer and information regarding customer behaviour and transactions should be used over time to assist in the creation of a customer risk profile. 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 potential risk posed by that customer.

3.30. Risk scoring, or the creation of a customer risk profile may also 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.

3.31. A 'web' of triggers can be created 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 systems, including other methods where triggers are set to indicate that a particular account requires reviewing at a certain stage.

3.32. One way of analysing and applying the attributes listed above, can be by sub-dividing them into specific behaviours, which are weighted and scored. The weighting remains flexible and can be adjusted dependent on how much of a risk each identified behaviour is considered to be. Meeting a pre-defined 'points' threshold triggers basic customer due diligence, or enhanced due diligence in appropriate circumstances. The risk thresholds and triggers should be reviewed and monitored to ensure they remain a true reflection of the risk.

4. Customer Verification and Due Diligence

4.1. Customer verification is key in ensuring that operators can be satisfied, that customers are who they say they are, that they are not acting on behalf of anyone else and to ensure that enhanced due diligence measures are applied to PEPs.

Customer co-operation is vital to ensure that the right information is provided and verified and one way in which this is achieved, is by making the customer verification process as easy and user friendly as possible.

4.2. It may be helpful to highlight to customers that they must undergo a standard verification process before they can begin to use the services of the remote gaming provider; and subsequently may also be required to provide further information about themselves. The point at which customer due diligence is triggered will be dependent upon the operator's approach, for example, where the threshold approach is taken, the operator will commence customer verification when a threshold has been reached. Alternatively, operators may choose to verify customers on establishing the business relationship.

4.3. 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.

4.4. 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:

1. Independent 3rd party verification e.g. the use of a software system and/or:

2. Checking personal documents, e.g.

   i. government issued ID proving identity and age (such as passport, identity card, driving licence or birth certificate)

   ii. proof of address (such as utility bill, mobile phone bill, insurance certificate, mortgage statement, bank statement, council tax bill, electoral register documentation).

a. Customer Due Diligence - Business Accounts

4.5. Where operators allow business accounts for gaming products in the wider remote gambling environment, then in addition to the personal identification from directors, the following may also be sought in order to satisfy the applicable beneficial ownership requirements:

1. The company is properly registered
2. Registered company name
3. Registered company address
4. Office-holders, shareholders and/or beneficial owners
5. Evidence of ownership of the account funding method.

4.6. Once information has been provided by the customer in relation to the above list it can also be verified using 3rd party reliable sources, such as the applicable company register or via 3rd party verification providers. Where this is not possible, confirmation in writing may be sought from a solicitor accountant who is qualified in the relevant jurisdiction.

4.7. In addition to the company and director information, it may also to be prudent to verify the method of funding of the gaming activity to ensure that this reflects the details registered on the business account.

b. Ongoing and Enhanced Due Diligence (EDD)

4.8. Customers should be continually monitored for any update in their risk profile. Where behaviours or transactions are identified which may increase the customer's potential risk, further investigations and due diligence should be undertaken. Factors which may increase a customer's risk, may include the triggering of an internal activity or monetary threshold, a match against a PEP list/category or a sudden change in behaviour, such as increase in depositing frequency and/or amount. Operators should have transactional monitoring programs to support the ongoing/enhanced due diligence in place to identify behaviour/transactions which may be indicative of suspicious behaviour.

4.9. Enhanced Due Diligence should follow the risk-based principle, in that where the customer's ML risk increases so should the level of due diligence performed on the customer. The aim of Enhanced Due Diligence is to obtain a level of confidence that the account is not funded by the proceeds of crime or used to finance terrorism.

4.10. There are a number of processes detailed belo,w which when used may increase the confidence that there is no ML or TF concern associated with the customer;

1. **3rd party verification -** e.g. use of software, or using approved 3rd parties to conduct face-to-face verification of customer documents; for example, in some countries Post Offices provide this service.

2. **Validation of customer documents -** Certified copies of documents to validate name, address, date of birth and source of funds of the customer.

3. **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.

4. **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 'reputable jurisdiction[3].

5. **Background and lifestyle checks -** Using open source research to obtain further information about the customer's source of wealth, occupation, property ownership status and lifestyle.

6. **Source of funds -** Confirm the immediate source from which the funds have derived.

7. **Source of wealth -** corroborate sustainable wealth that matches the customer's gambling profile. This may also overlap with responsible gambling considerations. Accurately identifying a customer's source of funds and source of wealth can be a complex process and one in which approaching an online customer directly for relevant evidence may be a last resort.

8. **Internal corroboration of user identity -** this could emanate from a variety of sources from customer monitoring, other databases and face to face verification where possible.

3 '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. There are countries that 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. 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 overseas territories who 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, and Isle of Man) may also be considered as equivalent by Member States.

4.11. The information above will assist in the building and updating of a customer profile over time, which can then be used as a reference for any changes in customer behaviour or transactions.

c. Politically Exposed Persons (PEPs)

4.12. Politically Exposed Persons 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. They would normally remain in this category until one year after leaving office.

4.13. PEPs are considered to be potentially higher risk due to their position and access to wealth and resources. PEPs can provide the appearance of respectability which may assist to deflect suspicion about their transactions. As PEPs usually operate within a sphere of influence, they are uniquely placed to be involved in potential corruption and may be able to circumvent AML/CTF regulation. Corruption includes the misuse of public office for private gain as well as money laundering carried out with reduced risk of detection when public officials are incorporated into the process. The professional status of the PEP often assists and enhances the legitimacy of transactions, making them an attractive prospect to run or be involved in ML/TF activity.

4.14. The fact that a person is a PEP does not automatically mean that they are involved in money laundering. However, where there is a confirmed PEPs match the customer will automatically pose a higher risk and a relationship review and senior management sign off should be conducted. This may then result in an alteration to their risk profile and justify enhanced customer due diligence and customer monitoring measures being applied.

4.15. 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 along with the 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.

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

1. identifying PEPs,
2. obtaining senior management approval in accepting PEPs as customers,
3. ensuring that there is proportionate monitoring of such customer accounts and,
4. measures to establish the source of wealth and funds that are involved in the business relationship/transactions
5. providing evidence of decisions made as part of the PEP identification and monitoring process including records of management approval and decisions relating to the risk monitoring measures implemented to confirmed PEP matches.

4.17. However, as there is no single source of information for identifying PEPs and 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 endeavours. The employment of an automated screening provider will usually ensure that all standard lists and categories are used. Regular reviews of these lists should be carried out to ensure that they remain up to date.

d. Sanctions

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

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

4.19. 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.

4.20. Operators should examine carefully any requirements that their regulators may place on them in relation to sanctions. Organisations that might typically be involved with sanctions are the US Office of Foreign Assets Control (OFAC) or its equivalent in other countries, and the European External Action Service (EEAS).

4.21. Where an operator identifies that a customer is a designated individual subject to financial sanctions, it is not permitted to carry out any financial transactions or to remit funds back to the customer. Operators must ensure that they have appropriate systems and controls in place in order to identify such individuals within the customer-base and apply the necessary restrictions in accordance with the requirements of the relevant sanctions regimes.

4.22. Operators should additionally ensure that they meet all reporting obligations in relations to financial sanctions. For example, the UK Office of Financial Sanctions Implementation (OFSI) clarifies that reporting to the regulator or submitting a SAR to the FIU does not mean operators meet their reporting obligations for financial sanctions which must be reported to OFSI as a minimum[4].

5. Role of the MLRO

5.1. Remote gaming operators should appoint an MLRO with sufficient seniority and command within the business to fulfil this key role effectively. It is also good practice for MLROs to:

1. ensure that the company's directors and board members are aware of their responsibilities with regard to money laundering; and

2. report to the board and/or senior management regularly (exactly how and when will be dependent on each company's internal structure).

5.2. It is important to remember that the term MLRO will not always be referred to within jurisdictions outside of the UK, but the scope of the role will be very similar. For those operators who are licensed by the British Gambling Commission, it is also worth noting that an increasing number of people in these kinds of roles are expected to hold Personal Management Licences.

5.3. The role of the MLRO is wide ranging however some key responsibilities include:

1. overall responsibility for the establishment and maintenance of the AML systems,

2. monitoring of the day to day operation of the AML policies,

3. responsibility for the oversight of compliance with the regulatory requirements for the implementation of systems and controls against money laundering,

4. receive and consider internal disclosures of suspected money laundering or terrorist financing,

5. filing a Suspicious Activity/Transaction Report with the relevant authorities where the grounds for suspicion are sufficient,

6. designing and setting-up of internal anti-money laundering procedures and policies including customer due diligence measures, reporting, record-keeping, risk assessment, management and control systems,

7. organising and arranging anti-money laundering training of the firm's staff.

5.4. The MLRO will receive reports of any information or other matters which give 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. The MLRO should have direct access to the Board of Directors in order to obtain approval and backing on AML/CTF issues across the business.

4 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/636472/financial_sanctions_guidance_august_2017.pdf

5.5. Remote gambling operators need to consider the level of support provided to the MLRO by way of staffing and other resources that they may 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. All staff will also need to know how to report any concerns or suspicions to their MLRO. It is advisable to ensure that there is a clear route for the internal escalation of suspicions or concerns and that staff are aware of the process.

5.6. A remote operator's employees should know the identity of their MLRO and the deputy MLRO and how they can be contacted. If staff are based in different countries from their MLRO then this needs to be reflected in relevant policies.

6. Suspicious Activity and Transaction Reporting (also: see Gambling Commissions advice)

6.1. Jurisdiction-specific guidance can be sought from the relevant FIU, but in almost all circumstances it will be a legal obligation to report suspicious transactions. These would include instances:

1. where they know or
2. where they suspect or
3. have reasonable grounds to suspect, that a person is engaged in money laundering or funding of terrorism.

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

6.3. Remote gaming operators should have a documented process in place for all employees to escalate when they have suspicions that a customer may be engaged in money laundering, or terrorist financing. These escalations should be sent to the MLRO or in his/her absence his Deputy MLRO/ nominated officer.

6.4. 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.

6.5. The MLRO must consider each report made to determine whether it gives rise to knowledge or reasonable grounds for 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 a criminal offence, carrying with it a possible prison sentence. All decisions made in relation to the submission or non-submission of a suspicions transaction report should be recorded and documented.

6.6. 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. Where a suspicious transaction report is not submitted, the reasons for non-submission must be fully documented.

6.7. Operators should be fully aware of the relevant FIU processes in relation to consent/non-consent reporting and that the decision to continue to transact with a customer or continue the business relationship with the customer is the responsibility of the operator alone.

"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."

7. Employee

a. Employee Training

7.1. It is imperative that staff receive appropriate and regular training which is proportionate to the potential risk of exposure to ML/TF as part of their role and responsibilities. The training content may include:

1. customer due diligence measures
2. record-keeping procedures
3. internal reporting procedures
4. policies and procedures on internal control, risk assessment, risk management, compliance management
5. 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
6. relevant regulation in each jurisdiction where a licence is held; and
7. 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.

7.2. Where possible, the level of training and the means by which staff are trained should be risk-based. It may therefore be appropriate to deliver computer-based training content to Customer Support staff, whilst higher-risk departments may be more appropriately trained in a classroom environment on a wider range of subjects.

7.3. 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.

7.4. In order to ensure that training remains relevant and up to date operators should have an annual (or more frequent) review of all training material for all forms of AML/CTF training implemented.

"Where possible, the level of training and the means by which staff are trained should be risk-based. It may therefore be appropriate to deliver computer-based training content to Customer Support staff, whilst higher-risk departments may be more appropriately trained in a classroom environment on a wider range of subjects."

b. Employee Screening

7.5. 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.

7.6. 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.

7.7. To summarise, employees should:

1. be identified and verified;
2. be screened to ensure their integrity; and
3. receive appropriate training.

7.8. Operators should take into account the differences in risk posed by the different roles across their business – some roles will pose a higher risk than others, such as a member of senior management. Screening levels and frequency should be adjusted to reflect this risk.

8. Record Keeping

8.1. Unlike the land-based 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:

1. transaction documents
2. due diligence information
3. information relating to suspicious transactions
4. MLRO reports
5. training in relation to AML matters, and
6. policies and procedures.

8.2. 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 (UK regulation). 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 customer's most recent activity. These records can be kept in documentary or electronic format.

8.3. Operators need to be aware that when they operate in more than one jurisdiction, that the requirements for the length of time and the scope of the record keeping may vary and processes need to take account of this.

8.4. Consideration should also be given to the storage location and the permissions applied to the records to ensure that they are easily accessible.

8.5. In order to ensure that document retention requirements are fulfilled, all AML/CTF policy or procedural documents should be version controlled where possible and all updates recorded for ease of auditing.

8.6. The destruction of personal data is a specific requirement under the Directive. Operators should check how this is implemented through national legislation as well as regulatory guidance and put in place appropriate measures to ensure compliance in this area.

9. Conclusion

9.1. Failure to implement sufficient systems and controls may lead to the operator being criminally liable or subject to regulatory sanctions, such as fines or licence revocation. Remote gambling operators and those who work for them can reduce their personal risks by the implementation and adherence to regulatory requirements. If there is a proper evaluation of the risks, together with a consideration of the way in which they can be mitigated, there is little for those involved to fear.

9.2. 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.

9.3. 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.

10. Annex A - Industry involvement in initiatives to combat money laundering and associated crime

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

1. Institute of Money Laundering Prevention Officers (IMLPO)

a. 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.

b. The aims and objectives of IMLPO are to:

i. establish a recognised industry forum to address specific issues of concern identified and raised by its members

ii. facilitate the further education and professional development of its members

iii. provide a broad representation for issues concerning money laundering prevention

2. Financial Action Task Force Casino Working Group

a. The Financial Action Task Force 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 Slegislative and regulatory reforms in these areas.

b. 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 RGA has continued to be involved with this Group since then.

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

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

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

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

3. Gambling Anti-Money Laundering Group (GAMLG)
GAMLG was established in January 2016. Its aim is to improve the gambling industry's ability to combat money laundering. Its initial membership is comprised of the Remote Gambling Association (RGA) and the Association of British Bookmakers (ABB).

4. RGA Crime Issues Committee
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.

5. 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.

6. Liaison
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.

7. 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.

11. Annex B - Glossary of abbreviations

11.1. "AML" - Anti-Money Laundering
11.2. "CDD" - Customer Due Diligence
11.3. "EDD" - Enhanced Due Diligence
11.4. "CTF" - Counter Terrorism Financing
11.5. "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. This is unless the reference is specifically to the 4th Anti-Money Laundering Directive which EU Member States have until 2017 to implement.
11.6. "employees" mean all persons actively employed or engaged with a remote gaming operation;
11.7. "FATF" - Financial Action Task Force
11.8. "FIU" - Financial Intelligence Unit
11.9. "IMPLO" - The Institute of Money Laundering Prevention Officers
11.10. "KYC" - Know Your Customer
11.11. "LBO" - Licenced Betting Office
11.12. "LCCP" - Licensing Conditions and Codes of Conduct
11.13. "ML" - Money Laundering
11.14. "MLRO" - Money Laundering Reporting Officer
11.15. "NCA" - National Crime Agency
11.16. "OFSI" - Office of Financial Sanctions Implementation
11.17. "OTC" - Over the Counter
11.18. "PEP" - Politically Exposed Person
11.19. "POCA" - Proceeds of Crime Act 2002
11.20. "Recommendations" refer to the 40+9 Recommendations on the prevention of money laundering and terrorist financing published by the Financial Action Task Force.
11.21. "Remote gaming" means any form of gaming by means of distance communications
11.22. "SAR" - Suspicious Activity Report
11.23. "SSBT" - Self-Service Betting Terminal
11.24. "SOF" - Source of Funds
11.25. "TF" - Terrorism Financing

GAMLG

GAMBLING ANTI-MONEY LAUNDERING GROUP

GAMLG.ORG