GAMBLING COMMISSION

Money laundering and terrorist financing risk within the British gambling industry

Contents

1 Executive summary

1.1 The Gambling Commission's (the Commission) money laundering and terrorist financing risk assessment 2018 highlights the core risks associated with each of the sectors within licensed land-based and remote activity in Great Britain's (British) gambling industry.

1.2 The purpose of this risk assessment is to:

- act as a resource for the industry in informing their own money laundering and terrorist financing (ML/TF) risk assessments
- meet our statutory anti-money laundering supervisor responsibilities
- advise HM Government on risks in the industry; and
- inform and prioritise our compliance activity to raise standards in the industry.

1.3 In consultation with in-house and external subject matter experts, this assessment has been developed with input from a wide range of sector and industry specialists. This includes law enforcement, such as the National Crime Agency (NCA), and considers approaches taken by other anti-money laundering (AML) supervisory authorities, such as the Financial Conduct Authority (FCA). The Commission also considers , the EU Supranational Risk Assessment on money laundering and terrorist financing (SNRA) and HM Treasury's National Risk Assessment (NRA) of money laundering and terrorist financing 2017 and Financial Action Task Force (FATF) recommendations when assessing the key threats posed by the risks identified in the British gambling industry.

1.4 The reporting period this assessment is based on is from 1 November 2017 to 31 October 2018. The methodology has changed slightly from previous iterations to reflect ongoing development of the Commission's risk-based approach. The 'very high' rating has been devised as part of the development of the progressive risk-based approach the Commission is adopting and accounts for the areas of greatest current risk in British gambling. For more detail on the methodology and terminology used, please refer to the 'methodology' section found at the end of this report.

1.5 In summary, the risk ratings for each gambling sector are shown below. Note that the overall risk ratings after assessment, has not changed in comparison to the previous risk assessment, published in March 2018, terrorist financing is being assessed separately for the first time:

Arcades (non-remote)	Family Entertainment Centres (FECs)	Betting (non-remote) Off-course	Betting (non-remote) On-course	Bingo (non-remote)	Casinos (non-remote)	Gaming Machines technical gambling software (remote and non-remote)	Lotteries (remote and non-remote)	Remote (casinos, betting and bingo)
Medium	**Low**	**High**	**Low**	**Medium**	**High**	**Medium**	**Low**	**High**

	Current overall risk rating
Terrorist financing	**Medium**

1.6 In this assessment, terrorist financing is rated on evidence and information accessible by the Commission. The risks were rated drawing on the contents of the NRA which provides further insight. The Commission has provided input to, and undertaken engagement with relevant security agencies and through this engagement has been able to share knowledge with and raised understanding in the industry. Over the last year, the Commission has strengthened stakeholder partnerships with counter terrorist teams across the UK. Through these partnerships, tri-lateral training and awareness session on the typologies and vulnerabilities associated with international terrorism and domestic extremism has been accessed by licensed operators. The Commission aims to continue educating the gambling industry in this vital area to achieve a high state of awareness.

1.7 There are many risks/ typologies or *vulnerabilities* in the gambling industry related to money laundering or terrorist financing (ML/TF). The nature of the industry is highly segmented, with a wide range of operators based both domestically and overseas, offering diverse products, in different environments, to different types of customers, with various payment methods. Criminals are increasingly looking for alternative ways to launder criminal proceeds and the gambling industry needs to be alert to this.

1.8 This assessment is a key tool in ensuring the Commission is focussing its resource and expertise on the highest risk areas of ML/TF in the British gambling market. Please read the previous publication of the risk assessment to learn more about existing risks and typologies highlighted in this report. We expect all operators to have an awareness of the vulnerabilities, controls and consequences associated with the ML/TF risks in gambling. This document is intended to act as a valuable resource for the industry in informing their own ML/TF risk assessments.

1.9 It is mandatory for gambling operators from all gambling sectors to comply with the licensing objective to keep crime and its proceeds out of gambling, as set out in the Gambling Act 2005 (the Act) and the Licence Conditions and Codes of Practice (LCCP). Furthermore, all gambling operators have legal duties under the Proceeds of Crime Act 2002 (POCA) and the Terrorism Act 2000 (TACT) to mitigate financial crime. Casinos, both land-based and remote, must also comply with the requirements set out in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Regulations) for casino gaming, gaming machines and money service business (MSB) activities offered. It is imperative for all gambling operators, regardless of gambling sector, to ensure they have effective risk assessments, policies, procedures and controls in place to prevent ML/TF and continue to raise standards in that regard.

2 Introduction

2.1 Regulation 17 of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Regulations) places an obligation on supervisory authorities to carry out a risk assessment of their supervised sector. The Commission is the supervisory authority for casinos and this obligation is met by this risk assessment. The Commission will also continue to use this risk assessment to inform HM Government of the level of risk of ML/TF within the entire gambling industry in Britain.

2.2 The Government acknowledges that a variety of factors can cause vulnerabilities and risks attributed to a particular gambling sector to become higher or lower risk over time. Consequently, where a gambling sector can no longer be deemed low risk (including where the sector fails to effectively manage the ML/TF risks), then it will likely lead to their inclusion within the provisions of the Regulations, subjecting that sector to its requirements.

2.3 A risk assessment is extensively recognised as the key requirement to understand the money laundering (ML) and terrorist financing (TF) risks that a business is exposed to. This is done through the identification, assessment, management and where possible, the mitigation to control and/ or prevent ML/TF. By knowing and understanding the risks to which the gambling industry is exposed, HM Government, law enforcement, the Commission and operators can work together to ensure that gambling in Britain is a hostile place for money launderers and terrorist financers seeking to exploit it.

2.4 In March 2018, we published our previous Money Laundering and Terrorist Financing Risk Assessment. The money laundering vulnerabilities in said assessment were gathered through analysis of a variety of information sources, which in turn provided a clear evidence-based understanding. This year's assessment of the risk assessment re-visits each of the vulnerabilities which the previous publication raised and seeks to build on key findings and potential vulnerabilities which have since been brought to the attention of the Commission. Therefore, it is recommended that this year's assessment should be used in conjunction with the previous assessment as it highlights further risk areas which are either emerging or inherent within the British gambling industry by sector.

2.5 This report is set out by firstly, reviewing existing inherent and emerging risk, which the previous risk assessment highlighted key vulnerabilities in each sector. Followed by an assessment of new inherent and existing risks.

2.6 Each of the risks have been reassessed using information sources such as enforcement case work, compliance assessment analysis, as well as external sources of information such as HM Treasury's National Risk Assessment, FATF recommendations, combined with qualified professional judgement by Commission AML/CTF experts.

3 The threat of money laundering and terrorist financing in the gambling industry

3.1 ML/TF threatens the UK's national security, the economy and international standing. Money laundering and terrorist financing are significant threats. It has detrimental impacts on society, damages communities and undermines the integrity of both public and private sector organisations. The ML/TF threats that the gambling industry face are diverse, complex and are steeply evolving.

3.2 Serious and organised crime has been estimated to cost the UK tens of billions of pounds every year. That is why we must continue to crack down on illicit crime and dirty money seeking to exploit the British gambling sector (National risk assessment of money laundering and terrorist financing 2017).

3.3 Money launderers and terrorist financers use similar methods to store, move and obtain funds, although their motives differ. Depriving terrorist groups of funds is an essential aspect of preventing these groups from recruiting and committing terrorist acts.

3.4 If left unimpeded, this may result in:

- significant potential for terrorist financing exploitation
- significant potential for criminal exploitation and detriment to society
- a major threat to business environment/ wider industry
- potential for serious breaches that can lead to significant penalties, fines or sanctions which will need heavy compliance action
- cost to implement AML/CTF controls anticipated to be a significant percentage of operator's budget
- international concern, resulting in governmental inquiry or sustained adverse national/international media

- critical failure of gambling operation/ business i.e. the survival of the operator is under imminent or severe threat, ultimately harming consumers and/ or negatively impacting the gambling industry as a whole.

4 Regulatory framework

The Gambling Act 2005 (the Act) and the National Lottery etc. Act 1993

4.1 Section 1(a) of the Act places a responsibility on all gambling operators to prevent gambling from being a source of, being associated with crime or disorder, or being used to support crime.

4.2 The Commission also regulates the National Lottery under the National Lottery Act 1993. The National Lottery Act requires that the National Lottery is (including every lottery that forms part of it) run with all due propriety, and that the interests of every participant in a lottery that forms part of the National Lottery are protected.

The Proceeds of Crime Act 2002 (POCA)

4.3 The Proceeds of Crime Act 2002 (POCA) places a further obligation on all gambling operators to be alert to attempts by customers to gamble with or launder money acquired unlawfully and to report such activity to the appropriate authorities. This applies to all forms of money laundering including, for example, 'washing' criminal money, attempting to disguise the criminal source of the funds, or simply using criminal proceeds to fund gambling. It applies to all persons, including gambling operators and their staff, and includes specific obligations to report suspected money laundering to the United Kingdom's Financial Intelligence Unit (UKFIU).

The Terrorism Act 2000 (TACT)

4.4 The Terrorism Act 2000 (TACT) establishes several offences concerned with engaging in or facilitating terrorism, as well as raising or possessing funds for terrorist purposes. It applies to all persons, including gambling operators and their staff, and includes specific obligations to report suspected terrorist financing to the UKFIU.

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Regulations)

4.5 The Regulations came into effect on 26 June 2017. These replaced the Money Laundering Regulations 2007. The Regulations require remote and non-remote casinos to, for example, and not limited to, identify the source of funds for customers and source of wealth and funds for Politically Exposed Persons, undertake ML/TF risk assessments, conduct customer and enhanced due diligence checks, establish policies, procedures and controls, and provide employee training to mitigate the risks of ML/TF. The Regulations designate the Commission as the supervisory authority for casinos in Britain. While, under the Regulations, HM Revenue and Customs (HMRC) is the supervisory authority for Money Service Businesses (MSB) activities, the Commission and HMRC have agreed, under regulation 7(2) of the Regulations, that the Commission will act as the supervisory authority for MSB activities carried out by casinos which includes: foreign exchange, third-party money transmission and third-party cheque cashing.

The Gambling Commission's Licence Conditions and Codes of Practice (LCCP)

4.6 The risk of crime, however, affects all gambling operators, including those in the non-money laundering regulations sector, and they are required to have regard to POCA and

TACT, and adopt a risk-based approach consistent with the Commission's Licence Conditions and Codes of Practice (LCCP), guidance and advice.

4.7 Licence condition 12.1.1 requires all operating licensees (except for gaming machine technical and gambling software licensees) to assess the risks of their businesses being used for ML/TF. Licensees must also ensure they have appropriate policies, procedures and controls to prevent ML/TF. They must ensure that such policies, procedures and controls are implemented effectively, kept under review, revised appropriately to ensure that they remain effective, and consider any applicable learning, publications or guidelines published by the Commission.

Financial Action Task Force (FATF)

4.8 The Commission has based its framework for this and the previous assessment on FATF's risk assessment methodology. The Financial Action Task Force (FATF) has published its Mutual Evaluation Report (MER) of the UK's AML and CTF framework, which is evaluated every ten years. Their report, which assessed technical compliance with FATF standards (the 40 Recommendations) and effectiveness of a country's AML/CTF regime (the 11 Immediate Outcomes) rated the Commission positively and singled us out as displaying *"…a very strong understanding of risks both at a sector and firm-specific level."*

4.9 For the next assessment, the Commission will continue to use FATF's framework and continue to develop and publish bespoke methodologies specific to gambling, to provide additional information on sector specific risks and threats to operators, consumers and Government.

GAMBLING COMMISSION

Arcades

5 Arcades

Arcades	Previous overall risk rating	Current overall risk rating
	Medium	Medium
Family Entertainment Centres (FECs)	Low	Low

Existing inherent risk rating

5.1 Further information on the risks, the consequences and the controls, please see the previous publication. The assessment shows no substantial change has occurred overall for the sector, noting a slight decrease in the inherent risk around businesses being acquired by organised crime for money laundering purposes.

	Vulnerability	Risk	Previous overall rating	Likelihood of event occurring	Impact of event occurring	Movement
				Current rating		
Arcades	Operator Control	Operators failing to comply with prevention of money laundering and terrorist financing legislation and guidance	M	M	M	↔
	Licensing & Integrity	Arcade businesses being acquired by organised crime to launder criminal proceeds	M	L	M	↓
	Customer	Anonymous customers laundering proceeds of crime through gaming machines	M	M	M	↔
	Product	Automated ticket redemption (ATR) machines used to facilitate the laundering of criminally derived funds (excluding FECs).	M	M	M	↔
	Product	Gaming machines, category B3 being used to launder criminally derived funds (excluding FECs).	M	M	M	↔
	Means of Payment	Cash transactions	M	M	M	↔
	Means of Payment	Ticket-in-ticket-out (TITO) facilities used to launder funds when used in conjunction with ATR machines (excluding FECs)	M	M	M	↔

Existing emerging risks

Privacy booths

5.3 There is one emerging risk; first raised in the previous assessment, concerning 'privacy booths' in the gaming sector. The assessment noted the introduction of privacy booths in premises where gaming machines are available for play. Its concept is to afford the player additional privacy by way of screens or pods, this however, may cause a reduction in supervision by employees.

5.4 The concern raised previously highlighted Licence condition 9.1, which states "*Facilities for gambling must only be offered in a manner which provides for appropriate supervision of those facilities by staff at all times".* Affording additional privacy to customers may reduce the supervision by employees in respect of preventing money laundering and criminal lifestyle spending.

5.5 The previous assessment noted privacy booths as an emerging risk which was identified in both arcades and betting shops. This risk has been considered and updated for the purposes of this assessment and has been rated as 'medium', the same as the previous assessment.

Arcades	Vulnerability	Risk	Previous overall rating	Likelihood of event occurring	Impact of event occurring	Movement
				Current rating		
	Operator Control	Privacy booths	M	M	M	↔

New inherent risks

5.6 Following in-depth analysis, this assessment has highlighted no further risk areas associated with arcades. Below we consider further vulnerabilities first identified in the previous risk assessment:

Issue / Threat	Sector	Type of Vulnerability	Likelihood of event occurring	Impact of event occurring	RAG
Vulnerability The incompetency of key personnel and licence holders exploited by criminals seeking to launder the proceeds of crime in the arcades sector. **Consequences** Poor competence and lack of suitability can result by having: • poor policies, procedures, controls, monitoring and training • lack of decisive action, high staff turnover/ lack of resources and/ or failing business model • failing to embed AML learning published by the Commission which can exacerbate existing ML vulnerabilities in this sector, such as criminal lifestyle spending and 'smurfing' • falling below the Commission's expected standards which can result in an assessment of 'inadequate' • failing to review and adjust it in the light of new and emerging threats. The Commission will take affirmative action where it identifies non-compliance, which may range from action plans through to the review and/or revocation of personal and/or operating licences. Failure to follow good practice as advised by the	Arcades	Operator Control	L	M	12

Commission, through ordinary code provision 2.1.1, will be a material factor in considering any action we take to review and/or revoke personal and/or operating licences.					

Controls / Mitigations	
• Ensuring fit and proper persons are in key positions. Operators and key personnel must comply and implement with the Act, POCA, TACT, and LCCP policies, procedures and controls to mitigate the risk of ML/TF occurring. Policies, procedures and controls implemented effectively should minimise the risk of ML/TF through effective risk assessments, monitoring, training and revision of risk assessments.	Preventive
• Controls within the sector largely rely on staff supervision and face-to-face interactions with the customer. Ensure centres are adequately staffed and employees have regular and current AML training and awareness of ML and TF vulnerabilities.	Detective
• In instances where there are concerns about staff integrity, operators will act where appropriate. If the staff are also licensed by the Commission, we may consider revocation of their personal licences.	Preventive

New emerging risks

Cashless payments

5.7 Within the arcades sector, there is very little change in terms of ML/TF vulnerabilities compared to previous years. However, there is a move in the wider gambling industry around the use of cashless payments.

5.8 This is in the form of crediting machines via smartphone applications fed via bank accounts/ debit cards. The money laundering vulnerability this presents, is the reduction in staff interaction with customers. There are anti-money laundering controls that can be put in place to mitigate this risk and one opportunity this offers is an audit trail to identify or investigate suspicious activity.

5.9 A further update regarding this risk will be provided in the next published assessment.

GAMBLING COMMISSION

Betting

6 Betting (non-remote)

Betting (non-remote)	Previous risk rating	Current risk rating
	Higher	High

Off-course	Higher	High
On-course	Lower	Medium

Existing inherent risk rating

6.1 Further information on the risk, the consequences and the controls, please see the previous publication. The assessment shows that no significant change has occurred for each risk area.

	Vulnerability	Risk	Previous overall rating	Likelihood of event occurring	Impact of event occurring	Movement
				Current rating		
Betting non-remote	Operator Control	Operators failing to comply with prevention of money laundering and terrorist financing legislation and guidance	H	H	H	↔
	Licensing & Integrity	Betting operations being acquired by organised crime to launder criminal proceeds	MH	M	H	↔
	Licensing & Integrity	Betting employees acting in collusion with organised criminals to launder criminal funds	MH	M	H	↔
	Customer	Anonymous customers laundering proceeds of crime through betting	H	H	H	↔
	Customer	Accessibility to multiple premises/operators (off-course only)	H	H	H	↔
	Customer	False or stolen identification documentation used to bypass controls in order to launder criminal funds (off-course only)	M	M	M	↔
	Product	Gaming machines, B2 (FOBTs)/SSBT/TITO to launder criminal funds (off-course only)	H	H	H	↔
	Means of Payment	Cash transactions	H	H	H	↔

Existing emerging risks

Bring Your Own Device (BYOD)

6.3 The product emerging risk of BYOD is an evolution of Self-Service Betting Terminals (SSBT), where consumers use their own device to place bets through non-account-based

play either in off-course premises or at on-course venues. The previous risk assessment recognised this and gave this product development a risk likelihood and impact rating of medium.

6.4 Anonymity is a potential vulnerability with BYOD, as a customer could place bets without needing an account or interacting with employees of the operator. The previous assessment noted the risk is increased when customers use multiple premises without this being identified by the operator, due to the lack of interaction the product offers and heightened further with lack of staff knowledge and awareness.

6.5 However, upon revisiting this risk for this assessment it has been found that whilst this technology is available to operators, the Commission is not aware of any licensed betting operator offering the facility. It is now known that customers need to buy 'bet credits' through staff and collect winnings through interaction with staff. On this basis, the money laundering threat has been reduced.

	Vulnerability	Risk	Previous overall rating	Likelihood of event occurring	Impact of event occurring	Movement
Betting non-remote				Current rating		
	Product	Bring your own device	M	VL	M	↓

New inherent risks

6.6 Following in-depth analysis, this assessment has captured further vulnerabilities which builds on further from the previous report:

Issue / Threat	Sector	Type of Vulnerability	Likelihood of event occurring	Impact of event occurring	RAG
Vulnerability Lack of adequate 'know your customer' (KYC) checks conducted resulting in criminals exploiting the non-remote betting sector by laundering the proceeds of crime. This risk has been rated as 'high' due to some relationships with customers being transient or temporary in nature. Despite this, operators still need to consider this issue in relation to all customers. In comparison to the betting and bingo remote sector, where customer accounts are present, creating an audit trail, the non-remote betting sector have an inconsistent 'nom du plume' system which is focussed on commercial viability not AML/CTF. **Consequences** Poor KYC, due diligence and source of funding checks can result by having: • poor policies, procedures, controls, monitoring and training, causing a lack of understanding of when and how to apply	Betting non-remote	Operator Control	M	H	6

checks • failing to embed AML learning published by the Commission which can exacerbate existing ML vulnerabilities in this sector, such as criminals spending the proceeds of crime • continued evidence of money laundering through criminal lifestyle spending prevails in non-remote betting, due to the anonymised business model used by the sector • decline in the use of loyalty schemes increases the anonymity of customers in the sector, which provides opportunities for criminals to spend their criminal funds. The consequences to the operators can be the following: • falling below the Commission's expected standards which can result in an assessment of 'inadequate' • systemic AML failings and breaches leading to enforcement action by the Commission, leading to reputational, legal, financial and operational damage.					

Controls / Mitigations	
Effective customer risk assessment • Operators should satisfy themselves that the sources of information employed to carry out KYC checks are suitable to mitigate the full range of risks to which they might be exposed, and these include money laundering and social responsibility risks. For example, local or open source information, such as press reports, may be particularly helpful in carrying out these checks. • Deciding that a customer presents a higher risk of money laundering does not automatically mean that the person is a criminal or is laundering money. Similarly, identifying a customer as having a low risk of money laundering does not mean that the customer is not laundering money or engaging in criminal spend. Operators, therefore, need to remain vigilant and use their experience and judgement in applying their risk-based criteria and rules. • Where a customer is assessed as presenting an increased risk, additional information in respect of that customer should be collected through KYC checks to ascertain the source of funds. This will help the operator judge whether the higher risk that the customer is perceived to present is likely to materialise and provide grounds for proportionate and recorded decisions.	Detective
Regular maintenance of operator's AML risk assessment and regular reviews of policies and procedures to ensure effectiveness • Much like the Commission regularly updates and maintains this risk assessment; operators are expected to produce and regularly review their own risk assessments. • Licence condition 12.1.1 requires all operating licensees (except for gaming machine technical and gambling software licensees) to assess the risks of their businesses being used for ML/TF. Licensees must also ensure they have appropriate policies, procedures and controls to prevent ML/TF when considering their own risk assessment. They must ensure that such policies, procedures and controls are implemented effectively, kept under review, revised appropriately to ensure that they remain effective, and consider any applicable learning or guidelines published by the Commission.	Preventive
Interaction with customers • Controls within the sector largely rely on staff supervision and face-to-face interactions with customers. Loyalty schemes have the potential to increase operators' knowledge	Preventive

of their customers and assist in the detection and prevention of money laundering. All loyalty schemes must be compliant with the LCCP and must be designed in a way that does not encourage problem gambling. CCTV and automated triggers assist in identification and reporting of suspicious behaviour by operators to law enforcement.	

Issue / Threat	Sector	Type of Vulnerability	Likelihood of event occurring	Impact of event occurring	RAG
Vulnerability Lack of effective customer interaction in betting shops resulting in a failure to prevent or detect money laundering or terrorist financing. This risk has been rated as 'high' due to the Commission holding intelligence and evidence of this vulnerability materialising. **Consequences** Poor or lack of customer interaction may occur from: • poor due diligence and KYC checks on customers (see previous risk for more detail) • low staffing levels in betting shops resulting from high turnover or cutbacks. This can cause limited employee knowledge, poor 'local knowledge' of regular customers due to the decline in interaction • criminals exploiting operators based on location and staffing levels • triggers based on monetary values set too high and/ or not effective • providing customers with additional anonymity by failing to identify 'high risk' customers • reporting of suspicious behaviour triggered by automated systems and/or observed behaviour is delayed, either due to limited employee knowledge of the customer or by employees being too intimidated to report suspicions about local criminals	Betting non-remote	Operator Control	M	H	6

Controls / Mitigations	
• Normal customer enquiries will not, in the Commission's view, amount to prejudicing an investigation under POCA, unless it is known or suspected that a SAR has already been submitted and that an investigation is current or impending and enquiries of the customer is made in a way that staff discloses those facts. However, there may be instances where customer enquiries are deemed necessary for ML duties and counter or frontline staff may not be aware that the nominated officer has submitted a SAR to the NCA. Reasonable and tactful enquiries regarding the background to a transaction or activity that is inconsistent with the customer's normal pattern of activity is good practice, forms an integral part of KYC measures (and may be driven by social responsibility concerns) and should not give rise to the prejudicing of an investigation.	Detective
• Ensuring betting shops are adequately managed and proportionately staffed by employees with working knowledge of relevant AML/CTF legislation and guidance. • Operators must comply and implement the Act, POCA, TACT, and LCCP policies,	Preventive

procedures and controls to mitigate the risk of ML/TF occurring. Policies, procedures and controls implemented effectively should minimise the risk of ML/TF through effective risk assessments, monitoring, training and revision of risk assessments. • ML Triggers must be reviewed to ensure they are fit for purpose and to include rigorous checks on individuals as to when and how those checks can be made.	
• Membership schemes have the potential to increase operators' knowledge about their customers and assist in the detection of money laundering. • CCTV and automated triggers assist in identifying and reporting suspicious behaviour by customers to law enforcement, however, this is unlikely to be in real time.	Preventive

New emerging risks

Crypto-assets in source of funds checks

6.7 Crypto-assets have been identified as a possible vehicle for money laundering, like any other monetary instrument. Guidance on Blockchain Technology and Crypto-assets can be found on the Commission website. Whilst the gambling industry has been reluctant to accept virtual currency as a means of payment, operators have encountered incidences of customers undergoing source of funds checks claiming they are investors or traders in crypto-assets. Whilst there are further checks that the operator can conduct to ascertain source of funds, operators have highlighted concerns they could fall foul of the AML regulations should those trades later be found to be part of a money laundering exercise. To mitigate this risk, the operator must adopt a culture that encourages curiosity and questions the customer to ensure credibility. A medium rating is given to this risk and further update will be sought in the next risk assessment.

Informal Value Transfer System (IVTS) in source of funds checks

6.8 Another source of funds related emerging risk in the non-remote betting sector is that of customer funds being obtained using IVTS. An informal value transfer system (IVTS) is where money is sent by individual(s) to an 'agent' who resides in the same region/ country as the intended receiver of funds. The agent delivers the money to the receiver, usually for a fee and not always in the same form. An IVTS is an age-old, alternative and unregulated method of the transmission of money and circumvents the banking system. A few examples of IVTS include:

- hawala – as known in the Middle East, Afghanistan and India
- fei ch'ien – meaning 'flying money' in China
- phoe kuan – as known in Thailand
- black market peso exchange – as known in South America

The Commission seeks to highlight this risk as operators could come across issues around confirming customers sources of funds when conducting due diligence AML/ CTF checks. Mitigation will be along the same lines as highlighted in the above crypto-asset paragraph. The Commission will be conducting a review of the impact of IVTS upon gambling and will publish its findings in due course. This vulnerability has been rated as medium.

Cashless payments

6.9 Cashless payments in the non-remote betting sector are conducted on self-service betting terminal (SSBTs). This presents a risk where money laundering could be facilitated using fraudulently obtained and stolen cards. Whilst there are controls in place through closed loop systems, this mitigation is wholly reliant on the operator and its employees' effective application. There is also an enforced limit on the number of transactions per day and a

monetary cap on each transaction. This emerging risk will be updated in the next publication of the risk assessment as there is a growing number of operators accepting contactless debit card payments and is currently rated as a medium level risk.

GAMBLING COMMISSION

Bingo (non-remote)

7 Bingo (non-remote)

Bingo (non-remote)	Previous overall risk rating	Current overall risk rating
	Medium	Medium

Existing inherent risk rating

7.1 Further information on the risk, the consequences and the controls, please see the previous assessment. This year's assessment shows no significant movement on overall risk rating for the bingo non-remote sector from 'medium', however, noting some decrease in some risk areas as outlined below.

Bingo non-remote	Vulnerability	Risk	Previous overall rating	Likelihood of event occurring	Impact of event occurring	Movement
				Current rating		
	Operator Control	Operators failing to comply with prevention of money laundering and terrorist financing legislation and guidance	M	M	M	↔
	Licensing & Integrity	Gambling operations being acquired by organised crime to launder criminal proceeds	M	L	M	↓
	Licensing & Integrity	Employees colluding with criminals	M	L	M	↓
	Customer	Anonymous customers laundering proceeds of crime through gaming machines	M	M	M	↔
	Means of Payment	Ticket-in-ticket-out (TITO) facilities used to launder funds when used in conjunction with ATR machines	M	M	M	↔

Existing emerging risks

7.3 The existing emerging risks in the bingo non-remote sector identified in the previous risk assessment have been reassessed and rated as medium. There is no significant change in the risk ratings due to no real movement in terms of the risks and issues identified in this update.

7.4 In regard to the risk relating to electronic bingo terminals (EBTs) including virtual table top gaming, with gaming machine features being used to launder criminal funds; there is now clarity that EBTs do not accept cash. Loading is usually done at the counter or by paying money to an account on the EBT or at a terminal. This involves some customer interaction with the operator/ employees and offers an audit trail. The risk of illicit funds being used in EBTs exists and must be mitigated similarly to how self-service betting terminals (SSBTs) are controlled in betting. This mitigation is wholly reliant on the operator and its employees' effective application of policies, procedures and controls. Therefore, the risk rating for this vulnerability is still rated as medium.

	Vulnerability	Risk	Previous overall rating	Likelihood of event occurring	Impact of event occurring	Movement
Bingo non-remote				Current rating		
	Operator Control	Changes to local licensing default premises conditions on times of bingo	M	M	M	↔
	Operator Control	Removal of membership schemes	M	L	M	↓
	Product	EBTs -electronic bingo terminals incl. table top gaming, either traditionally or via EBT content	M	L	M	↓
	Product	Gaming machines Cat B3 max stake £2 max price £500	M	M	M	↔

New inherent risks

7.5 Following in-depth analysis, this assessment has captured further vulnerabilities which builds on further from the previous publication:

Issue / Threat	Sector	Type of Vulnerability	Likelihood of event occurring	Impact of event occurring	RAG
Vulnerability Lack of adequate 'know your customer' (KYC) checks conducted resulting in criminals exploiting the non-remote bingo sector by laundering the proceeds of crime. This risk has been rated as 'medium' due to most bingo clubs offering membership and a higher take up on loyalty and reward cards which captures KYC details and enables monitoring, thus creating an audit trial. **Consequences** Poor KYC, due diligence and source of funding checks can result by having: • poor policies, procedures, controls, monitoring and training, causing a lack of understanding of when and how to apply checks • failing to embed AML learning published by the Commission which can exacerbate existing ML vulnerabilities in this sector, such as criminals spending the proceeds of crime. The consequences to the operators can be the following: • falling below the Commission's expected standards which can result in an assessment of 'inadequate'	Bingo non-remote	Operator Control	M	M	9

• systemic AML failings and breaches leading to enforcement action by the Commission, leading to reputational, legal, financial and operational damage.					

Controls / Mitigations	
Effective customer risk assessment • Operators should satisfy themselves that the sources of information employed to carry out KYC checks are suitable to mitigate the full range of risks to which they might be exposed, and these include money laundering and social responsibility risks. For example, local or open source information, such as press reports, may be particularly helpful in carrying out these checks. • Deciding that a customer presents an increased risk of money laundering does not automatically mean that the person is a criminal or is laundering money. Similarly, identifying a customer as having a low risk of money laundering does not mean that the customer is not laundering money or engaging in criminal spend. Operators, therefore, need to remain vigilant and use their experience and judgement in applying their risk-based criteria and rules. • Where a customer is assessed as presenting a higher risk, additional information in respect of that customer should be collected through KYC checks to ascertain the source of funds. This will help the operator judge whether the higher risk that the customer is perceived to present is likely to materialise and provide grounds for proportionate and recorded decisions.	Detective
Regular maintenance of operator AML risk assessment and regular reviews of policies and procedures to ensure effectiveness • Much like the Commission's regular updates and the process undertaken to maintain this risk assessment; operators are expected to produce and regularly review their own risk assessments. • Licence condition 12.1.1 requires all operating licensees (except for gaming machine technical and gambling software licensees) to assess the risks of their businesses being used for ML/TF. Licensees must also ensure they have appropriate policies, procedures and controls to prevent ML/TF when considering their own risk assessment. They must ensure that such policies, procedures and controls are implemented effectively, kept under review, revised appropriately to ensure that they remain effective, and consider any applicable learning or guidelines published by the Commission.	Preventive
Interaction with customers • Controls within the sector largely rely on staff supervision and face-to-face interactions with customers. Loyalty schemes have the potential to increase operators' knowledge of their customers and assist in the detection and prevention of money laundering. CCTV and automated triggers assist in identification and reporting of suspicious behaviour by operators to law enforcement.	Preventive

New emerging risks

7.6 There are no emerging risks in the bingo non-remote sector.

GAMBLING COMMISSION

Casino (non-remote)

8 Casino (non-remote)

Casino (non-remote)	Previous overall risk rating	Current overall risk rating
	Higher	High

Existing inherent risk rating

8.1 The previous risk assessment highlighted key vulnerabilities in this sector. Further consideration has been given to cover additional responsibilities which impact the non-remote casino sector regarding the regulation under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Regulations).

8.2 For further information on the risks, the consequences and the controls, please see the Commission's previous risk assessment publication. This assessment shows that some of the risk ratings have increased due to the re-assessment of the impact of the event occurring:

	Vulnerability	Risk	Previous overall rating	Likelihood of event occurring	Impact of event occurring	Movement
				Current rating		
Casinos non-remote	Operator Control	Operators failing to comply with prevention of money laundering and terrorist financing legislation and guidance	H	H	H	↔
	Licensing & Integrity	Gambling operations being acquired by organised crime to launder criminal proceeds	MH	M	H	↔
	Licensing & Integrity	Ultimate Beneficial Ownership	MH	M	H	↔
	Licensing & Integrity	Employees colluding with criminals	MH	M	H	↔
	Customer	Customer from high-risk jurisdictions using casino facilities to launder money	M	M	VH	↑
	Customer	Customers appearing on international sanctions list laundering corrupt or criminal funds	M	M	VH	↑
	Customer	Domestic Politically Exposed Person (PEP) identification & verification	M	M	M	↔
	Customer	False or stolen ID docs used to bypass controls	MH	M	H	↔
	Customer	International PEP using casinos to clean criminal funds	MH	H	VH	↑
	Customer	Customers breaking up large amounts of cash into	MH	H	H	↑

		small transactions in order to minimise suspicion and evade CDD requirements at the threshold (smurfing)				
	Customer	Use of third parties or agents to obscure the source or ownership of money gambled by customers & their identities	M	H	H	↑
	Means of Payment	Cash Transactions	H	H	H	↔
	Means of Payment	TITO enabled gaming machines used to launder funds when used with ATR machine	H	H	H	↔
	Product	Electronic roulette - when used with TITO & ATRs	H	H	H	↔
	Product	Gaming Machines (all)	H	H	H	↔
	Product	Peer to peer gaming (poker) B2C	H	H	H	↔

Existing emerging risks

8.2 There are no updates to existing emerging risks in casinos non-remote sector.

New inherent risks

8.3 Following in-depth analysis, this assessment has captured further vulnerabilities which builds on further from the previous publication:

Issue / Threat	Sector	Type of Vulnerability	Likelihood of event occurring	Impact of event occurring	RAG
Vulnerability The lack of competency of key personnel and licence holders exploited by criminals seeking to launder the proceeds of crime in the non-remote casino sector. This risk has been rated overall as 'medium' due to its detrimental impact should it materialise. **Consequences** Poor competence and lack of suitability can result by having: • Poor implementation of policies, procedures, controls, monitoring and training • Lack of decisive action regarding suspicious activity or unclear, unrecorded or uncontrolled decision making • High staff turnover/ lack of resources can result in a failure to understand risk and identify issues relating to ML/TF	Casino non-remote	Operator Control	L	H	8

• A failing business model which may focus on commercial advantages and does not factor in governance and measures around AML/CTF • Failing to embed AML learning published by the Commission which can exacerbate existing ML vulnerabilities in this sector, such as criminal lifestyle spending and 'smurfing' • Continued evidence of money laundering through collusion, cheating and criminal lifestyle spending, due to policies, procedures and controls not being effectively implemented, monitored or revised by senior licensed employees and senior management • Licensed employees colluding with customers for personal gain remains evident in the sector. Cheating is a criminal offence under the Act and any personal gain from cheating is the proceeds of crime • Failure by senior management and nominated officers to identify areas of ineffective or negligent staff training, which results in poor compliance by staff, including: not following policies, procedures and controls; and not identifying that senior licensed staff are failing to monitor the effectiveness of employees' performance and their ability to follow policies, procedures and controls. Senior management's failure to identify and rectify failures by employees in the above areas remains a concern in the sector • Nominated officers' failing or being prevented by senior management to submit SARs when knowledge or suspicion has been identified by them. Procedures are not sufficiently effective for the nominated officer to assess whether knowledge and suspicion has been identified, both remain areas of concern in this sector • Failure by licensed employees and senior management to follow their own policies, procedures and controls intended to mitigate ML/TF has resulted in criminal lifestyle spending continuing in the sector • Lack of understanding of when to submit and/ or the lack of submitting of 'Defence against money laundering' or 'Defence against terrorist financing' (DAMLs/DATFs) to prevent a principle ML offence being committed. This includes submitting DAMLs/DATFs post movement of monies to obtain a defence as opposed to pre-movement. The Commission will take affirmative action where it identifies non-compliance, which may range from action plans through to the review and/or revocation of personal and/or operating licences. Failure to follow good practice as advised by the Commission, through ordinary code provision 2.1.1, will be a material factor in considering any action we take to review and/or revoke personal and/or operating licences.					

Controls / Mitigations	
• Ensuring fit and proper persons are in key positions. Operators and key personnel must comply and implement with the Act, POCA, TACT, ML Regulations and LCCP policies, procedures and controls to mitigate the risk of ML/TF occurring. Policies, procedures and controls implemented effectively should minimise the risk of ML/TF through effective risk assessments, monitoring, training and revision of risk assessments. • Senior management or the Board must appoint a nominated officer within the firm, and they must comply with requirements in the Regulations to minimise the risk of ML/TF occurring. The role of the nominated officer includes reporting suspected or known ML/TF activity via SARs, applying for a defence against a principle money laundering offence where criminal funds are suspected, providing adequate training to employees, maintaining records of decisions made in their role as nominated officer and reporting annually on the business's AML activities to their senior management and board. • One of the requirements of the Regulations 2017 is for casino operators to appoint, where appropriate, with regard to the size and nature of their business, an individual who is either a member of the board of directors (or if there is no board, of its equivalent management body) or of its senior management, as the officer responsible for the operator's compliance with the Regulations. The pertinent regulation is 21(1)(a).	Preventive
• Policies, procedures and controls implemented effectively should minimise the risk of ML/TF through effective risk assessments, monitoring, training and revision of risk assessments.	Preventive
• In instances where there are concerns about staff integrity, operators will act where appropriate. If the staff are also licensed by the Commission, we may consider revocation of their personal licences. • Adequate supervision of table gaming and gaming machines to minimise the risk of money laundering, criminal lifestyle spend, cheating and collusion.	Detective

Issue / Threat	Sector	Type of Vulnerability	Likelihood of event occurring	Impact of event occurring	RAG
Vulnerability Lack of adequate and relevant due diligence checks conducted resulting in criminals exploiting the non-remote casino sector by laundering the proceeds of crime. This risk has been rated as 'high' due to the Regulations imposing additional requirements on the regulated sector. These include risk assessments and requirements in respect of written policies, and procedures and controls, internal controls, CDD, record keeping and training. The Commission also holds intelligence and evidence of this vulnerability materialising. **Consequences** The consequences of poor customer due diligence, enhanced due diligence (CDD/EDD) and source of funding/wealth checks:	Casino non-remote	Operator Control	M	H	6

• The carrying out of the CDD obligations, including monitoring customer transactions and activity being improper i.e. poor record keeping, not adopting a risk-based approach and failing to identify suspicious activity • Money laundering through collusion, cheating and criminal lifestyle spending, due to policies, procedures and controls not being effectively implemented, monitored or revised by senior licensed employees and senior management. Failure by licensed employees to follow policies, procedures and controls intended to mitigate ML/TF has resulted in criminal lifestyle spending continuing in the sector • Failure by senior management and nominated officers to identify areas of ineffective or negligent staff training, which results in poor compliance by staff, including: not following policies, procedures and controls; and not identifying that senior licensed staff are failing to monitor the effectiveness of employees' performance and their ability to follow policies, procedures and controls. • Decline in the use of full membership schemes and threshold or hybrid CDD schemes increases the opportunity for customers in the sector to spend criminally derived funds for a period before reaching the monetary threshold and triggering full CDD procedures • Lack of understanding in the non-remote casino sector around a business relationship and when that is triggered. Over-reliance instead by operators on enquiries of customers sources of funds once the 2000 Euro threshold is met • Real time reporting of suspicious behaviour triggered by employee intervention, automated systems and/or observed behaviour is delayed due to the use of threshold and or hybrid CDD models, limiting the level of information known about customers • Senior management decision makers with oversight of data and suspicion are not effectively identifying criminal lifestyle spending within their estate and reporting it to UKFIU • Failing to monitor the sanctions list, for either country or individual restrictions, resulting in illicit funds being used in the sector and ultimately infiltrating the UK's financial system • Failing to identify PEPs prior to gaming increases the likelihood of monies derived from corruption and bribery being laundered through the casino and ultimately infiltrating the UK's financial system.					

Controls / Mitigations	
• Conducting adequate CDD/EDD checks, including the verification of customer identities and source of funds, which should limit the risk of exposure to money laundering.	Detective

• Using Commission published guidance when conducting checks and considering the following: ○ adopting a risk-based approach ○ senior management taking responsibility for effectively managing the money laundering and terrorist financing risks faced by the casino operator's businesses; ○ the role and responsibilities of the nominated officer; ○ the proper carrying out of the CDD and EDD obligations, including monitoring customer transactions and activity; ○ record keeping; and ○ the identification and reporting of suspicious activity and requesting appropriate defences against principle money laundering offences. • This includes PEP monitoring which should minimise corruption and the risk of money laundering occurring. • Ensuring effective monitoring of sanction lists, both country and individual specific, taking note of the restrictions and acting accordingly to mitigate the risk of criminally derived cash infiltrating the UK financial and associated sectors.	
• Policies, procedures and controls implemented effectively should minimise the risk of ML/TF through effective risk assessments, monitoring, training and revision of risk assessments. • This includes adequate staff supervision, of gaming tables and gaming machines, utilising CCTV and automated triggers derived from transactional data to assist in identifying and reporting suspicious behaviour by customers to UKFIU. • Membership schemes increase the operators' ability to know their customers, confirm their details and verify their identity, ascertain their source of funds and/or if a PEP, their source of funds and wealth, and check their PEP and sanctions list status. This decreases the risk of money laundering and terrorist funding in the sector.	Preventive
• Membership schemes increase the operators' ability to know their customers, confirm their details and verify their identity, ascertain their source of funds and wealth, and check their PEP and sanctions list status. This decreases the risk of money laundering and terrorist funding in the sector.	Preventive

Issue / Threat	Sector	Type of Vulnerability	Likelihood of event occurring	Impact of event occurring	RAG
Vulnerability Casinos acting as money service businesses (MSB) Due to the cash intensive nature of this risk and known evidence of terrorists and criminals having moved funds through and out of the UK through the wider financial markets, it is identified as high-risk. Specific jurisdictions of high risk are identified by the HM Treasury's National Risk Assessment, law enforcement agencies and the Office of Financial Sanctions Implementation's (OFSI) consolidated list. **Consequences** Under the Regulations 2017 an MSB is defined as a natural or legal person which by way of business operates a currency exchange office, cashes cheques made payable to customers or transmits money (or any representation of monetary value) by any	Casino non-remote	Means of Payment	H	H	4

means. It is known by the Commission that certain casinos offer, incidentally to their main casino and machine gaming activities, MSB services (cashing cheques, money transmission or currency exchange activities) for their casino customers, including overseas individuals. Risk based consequences regarding the provision of MSBs are: • MSB activities, such as foreign currency exchange, not implemented correctly or effectively may result in overseas criminally derived funds infiltrating the UK's financial system and the potential for committing criminal offences by circumventing other jurisdictions' money laundering legislation and controls • Customer records not being maintained/ or adequately maintained to show MSB activity • Operators having a lack of understanding the ML/TF risks associated with MSB provisions • There is a threat of casino members/ customers not using the casino for the purposes of gambling but purely to utilise the MSB facilities, thus using it as a bank rather than a casino • It is known that casinos use third parties to conduct currency conversion. It is not known whether casinos have adequately vetted these parties and if they adopt the casinos policies and procedures. This includes LCCP Social responsibility code provision 1.1.2 which sets out responsibilities for third parties that all licence holders must comply with. Therefore, opening UK financial system to the risk of money laundering and terrorist financing • MSBs can be used by casino employees and it is not known if there are adequate internal controls in place. This presents a risk of money laundering and terrorist financing to happen in 'plain sight' • HM Treasury's NRA highlights that the NCA has identified criminals advertising fake jobs in newspapers and on the internet often targeting students or recently arrived migrants. Coercing them to use MSB facilities to launder criminal benefits for financial gain • Operators may risk contravening Section 81 of the Act which prohibits credit in casinos when rolling over cheques as a means of credit for customers • Operators must not accept CDD/EDD at face value and without effectively scrutinising source of funds or source of wealth; particular monitoring on money movement within accounts. This includes the lack of satisfactory checks around where funds have originated from and the CDD/EDD source of funds checks or source of wealth checks for PEPs conducted by other casinos and other casinos in foreign jurisdictions.					

Controls / Mitigations	
• Policies, procedures and controls implemented effectively should minimise the risk of ML/TF through effective risk assessments, monitoring, training and revision of risk assessments. • Legislation includes Section 81 of the Act which prohibits credit in casinos. With effectively implemented policies and procedures, this limits the risk of illegal money lending (which is also subject to an ordinary code provision in LCCP 3.8.1) Casinos also must comply with The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Regulations) in respect of Money Business Services for foreign currency exchange to minimise the risk of ML/TF.	Preventive
• Operators providing these services may gain a fuller view of the characteristics of gamblers and the detection of criminal activity done effectively and efficiently. Controls can be in the form of conducting further risk assessment for MSB activities and incorporate obligations to conduct further checks and maintain records by putting sufficient processes and procedures in place. Operators providing MSB activity may then gain a better understanding of the characteristics of gamblers by further KYC, source of funds, source of wealth (PEP), and audit trails which helps in detecting criminal activity more quickly.	Detective

Issue / Threat	Sector	Type of Vulnerability	Likelihood of event occurring	Impact of event occurring	RAG
Vulnerability Undermining of the Money Laundering Reporting Officer (MLRO) or nominated officer in the gambling operation can intentionally or unintentionally lead to exploitation by money launderers. This risk has been rated as 'high' as the Commission has come across evidence that there is a vulnerability in operators where the MLRO/ nominated officer is not a 'key position' and in some instances which the Commission recommends or the MLRO/nominated officer is in a 'key position' and is prevented from fulfilling their obligations due to senior management commercial priorities, this undermines the legal importance of the role and potentially leads to principle money laundering offences being committed and being under reported to the UKFIU. **Consequences** Risk based consequences regarding the undermining of the nominated officer/ MLRO: • employees not sighting or seeking guidance from their nominated officer as appropriate. Under POCA and the Terrorism Act, individual employees face criminal penalties if they are involved in money laundering or terrorist financing. If they do not make an internal report to their nominated officer when necessary, they may also face criminal sanctions. It is important, therefore, that employees are made aware of their legal obligations, and are given training in how to discharge them	Casino non-remote	Operator Control	H	H	4

• senior management not involving/ adequately sighting the nominated officer in operational matters and the effectiveness of the operator's systems and controls to combat money laundering and terrorist financing • senior management favouring commercial advantages over AML obligations, without considering input from the nominated officer or disregarding nominated officers' concerns • the nominated officer does not have sufficient seniority within the business with a clear path of reporting to Board or the equivalent.					

Controls / Mitigations	
• Senior management should require that the nominated officer provide an annual report covering the operation and effectiveness of the operator's systems and controls to combat money laundering and terrorist financing and take any action necessary to remedy deficiencies identified by the report in a timely manner. In practice, senior management should determine the depth and frequency of information provided by the nominated officer that they feel is necessary to discharge their responsibilities.	Preventive
• Casino operators should also ensure that relevant employees are aware of and understand: the identity, role and responsibilities of the nominated officer, and what should be done in their absence. • The nominated officer should be heavily involved in devising and managing the delivery of such training, taking particular care to ensure that systems are in place to cover all part-time or casual employees.	Detective
• The nominated officer is responsible for the oversight of all aspects of the casino operator's AML/CTF activities at all premises. They are the focal point for all activity within the operator relating to AML/CTF. The individual appointed as nominated officer must have a sufficient level of seniority. • The nominated officer should hold a personal management licence (PML) issued by the Commission. • The job description of the nominated officer should clearly set out the extent of the responsibilities given to it and its objectives. The nominated officer will need to be involved in establishing the basis on which a risk-based approach to the prevention of money laundering and terrorist financing is put into practice. • Accurate record keeping of reporting must be maintained as a matter of course. Staff must be aware of the reporting process and including how and when to report. The nominated officer is obliged to keep written records including the decisions made and particularly when a decision is made not to report.	Preventive

New emerging risks

Crypto-assets in source of funds checks

8.3 Crypto-assets have been identified as a possible vehicle for money laundering, as equivalent to other monetary instruments. Whilst the gambling industry have been reluctant to accept virtual currency as a means of payment, operators have encountered incidences of customers undergoing source of funds checks claiming they are investors or traders in

crypto-asset. Whilst there are further checks that the operator can conduct to ascertain source of funds, operators have highlighted concerns they could fall foul of the AML regulations should those trades later be found to be part of a money laundering exercise. To mitigate this risk, the operator must adopt a culture that encourages curiosity and interrogate the customer to ensure credibility. A medium rating is given to this risk and further update will be sought in the next risk assessment.

Informal Value Transfer System (IVTS) in source of funds checks

8.4 Casinos are regulated by the Commission under both the Act and the Regulations, this requires source of funds and source of wealth checks satisfy legal customer due diligence (CDD) or enhanced due diligence (EDD) requirements.

8.5 This emerging risk is regarding customer funds being obtained using IVTS being used such as 'hawala', 'fei ch'ien', 'phoe kuan' or, black market peso exchange. The Commission seeks to highlight this risk as operators could come across issues around confirming customers sources of funds when conducting due diligence AML/ CTF checks. Mitigation will be along the same lines as highlighted in the above crypto-assets paragraph. The Commission is currently reviewing intelligence and evidence in this area and it will be reviewed in the next risk assessment. This vulnerability has been rated as medium.

Individuals with known criminal records

8.6 There is an emerging risk in the non-remote casino sector of licensable and non-licensable employees being vulnerable to being exploited or groomed by criminals in order to facilitate the laundering of money or enabling criminal spending within casinos. The Commission aims to raise awareness of this vulnerability soon with casino nominated officers and suggests that operators conduct stringent, and ongoing vetting checks for all employees working within a licensed environment. Other mitigation can include review of 'Know Your Employee' (KYE) policies, procedures and controls, improving existing measures and ensure policies and procedures (such as in respect of receiving tips, see LCCP Licence condition 10.1.1 on tipping) are robust and in place. This risk has been rated with a likelihood scoring of medium and an impact rating as high.

GAMBLING COMMISSION

Gaming machine technical and gambling software

9 Gaming machine technical and gambling software

Gaming machine technical and gambling software	Previous overall risk rating	Current overall risk rating
	Low	Low

Existing inherent risk rating

9.1 Further information on the risk, the consequences and the controls, please see the previous publication. The assessment shows that no significant change has occurred for each risk area.

Gaming machine technical and gambling software	Vulnerability	Risk	Previous overall rating	Likelihood of event occurring	Impact of event occurring	Movement
				Current rating		
	Operator Control	Operators failing to comply with prevention of money laundering and terrorist financing legislation and guidance	L	L	L	↔
	Product	Gaming machines used to launder or spend the proceeds of crime	L	L	L	↔
	Product	Gaming machines Cat B2, FOBT, SSBT, TITO used to launder the proceeds of crime	L	L	L	↔
	Product	TITO enabled gaming machines used to launder funds when used with ATR machine	L	L	L	↔
	Means of payment	TITO used in conjunction with ATR machines in casinos, bingo halls and AGCs (machine operator issue, but provides an opportunity for manufacturers and retailers to cooperate to mitigate the risks)	L	L	L	↔

Existing emerging risks

9.3 There are no existing emerging risks in the gaming machine technical and gambling software sector.

New inherent risks

9.4 There are no new inherent risks in the gaming machine technical and gambling software sector.

New emerging risks

Cashless payments

9.5 The Gaming Machines (Circumstances of Use) Regulations 2007 provide prohibitions and restrictions on the use of debit and credit cards for payments to play machines. The Commission takes the view that card payments that originate from contactless mobile

payment systems such as Apple Pay, Android Pay or Samsung Pay should be regarded as the same as payments to use a gaming machine by means of a card itself. This is because the device used for such types of payment (e.g. a smartphone or watch) is essentially just a medium by which a contactless card payment is made (i.e. the debit card sat behind the payment system is charged directly and the customer's bank account is debited; the same as for any payment where the debit card itself is used). Both contactless card and mobile payment system transactions can be completed quite rapidly, and so the risks to the consumer are largely identical.

9.6 The regulations also prescribe limits as to the amounts an individual can deposit onto a gaming machine in any single action, and separately the (non-refundable) amount a player can commit to play the machine. These measures must be observed regardless of the means of payment. That is, whether the customer has inserted cash into the machine, or whether they have transferred funds from a debit card via indirect means, a TITO (ticket-in, ticket-out) method or an operator-provided app-based digital wallet.

9.7 Operators should use these new opportunities to support innovation in AML/CTF controls and the protection of customers. For example, cashless payment technology may assist operators in tracking their customers' play, allowing them to collect better data on their customers' gambling behaviour and therefore helping to inform an assessment of money laundering and terrorist financing. The Commission encourages operators to consider how they can gather data both before and after the implementation of any measure so that they can demonstrate the impact of control measures.

9.8 There are certain conditions and codes of practice that must be adhered to when providing cashless payment facilities. These include, for example, the need to implement effective policies and procedures for minimising certain risks to the licensing objectives; and provisions that limit the circumstances in which credit can be provided, or credit cards accepted (and where the Gambling Act does not otherwise prohibit or restrict any such facility). Operators should refer to the LCCP for full details of the relevant requirements below:

- Licence condition 5.1 – cash and cash equivalents, payment methods and services
- Social responsibility code provision 3.7.1 – credit cards
- Social responsibility code provision 3.7.2 – provision of credit

9.9 As discussed earlier in this report in the betting sector section, the nature of this risk exposes a vulnerability that money laundering could be facilitated through the use fraudulent and stolen cards. Whilst there are controls in place through closed loop systems, this mitigation is wholly reliant on the operator and its employees' effective application. There is evidence known to the Commission that demonstrates failures by employees' application and senior management oversight in the detection of such issues. There is also an enforced limit on the number of transactions per day and a monetary cap on each transaction. This emerging risk will be updated in the next risk assessment as there are a growing number of operators accepting contactless debit card payments.

Test houses

9.10 Gambling products are tested by a test house before they are released to the market. The Commission publishes a list of approved test houses which are fully accredited to BS/ENISO 17025 which covers the scope of the Commission's technical standards and requirements each test house can check for compliance.

9.11 The ML vulnerabilities around this risk are:

- Games not being tested correctly, either through incompetence or collusion leaving them vulnerable to exploitation

- The servers where the live game is hosted may not be as secure as the test environment, leaving it vulnerable to corruption and collusion
- Mergers and acquisitions within the industry can mean legacy technology architecture (which can be weaker) is being integrated into wider systems of large operators
- Competency, continual professional development and training, identity and integrity of the actual testers used by test houses is not monitored and this can lead to games not being tested correctly, either through incompetence or collusion.

9.12 This emerging risk will be updated in the next risk assessment.

Cyber-crime threat

9.13 There is an emerging risk related to cyber-crime concerning operator vulnerability in terms of the security of their systems, as well as their games. Some operators may hold a form of system security insurance; insuring against the threat of cyber-crime. However, operators are expected to have controls in place as well as this, to mitigate risks around security breaches.

9.14 The ML vulnerabilities are around operators being potentially open to system breaches that allow criminals to gain access to customer funds and customer databases. Consequently, criminals could deposit into existing accounts, withdraw funds, set up new accounts, delete accounts, edit accounts (including marking CDD and/or EDD as completed etc.) and steal customer information, or the entire database and extort the operator. Another ML vulnerability is around criminals setting up new accounts. Criminals with access to the database could set up accounts and deposit money as a way of storing funds for later use or create 'administrator' or 'test' accounts which are not 'live' to the operator, thus evading checks. A distributed denial of service attack (DDoS) is an example where criminals target sites or services hosted on high-profile web servers which is designed to disrupt and damage trade.

9.15 This emerging risk will be updated in the next risk assessment however in the meantime we encourage operators to be alive to these risks and plan for them accordingly.

White label partners

9.16 A white label provider partners up with companies who can market the gambling product utilising their unique brand and in return pays the marketing partner a profit share of the revenues generated. The white label provider is providing the facilities for gambling and, in order to advertise and operate in Great Britain legally, is required to be licensed by the Commission. If the marketing partner does nothing more than offer marketing via their branded website, they do not require an operating licence.

9.17 The ML vulnerabilities around this risk relate to:

- White labels being run by criminals who are laundering money through fake accounts
- White labels allowing ML to occur by not being robust enough in enforcing AML/TF counter measures and focussing more on commercial advantages
- The onus on background checks on white labels is with licensed operators. The Commission has no authority to conduct checks or keep records on white labels. This heightens the risk of criminal conduct being masked. Also, incompetent or potentially

criminal white label providers can infiltrate the industry by moving from operator to operator undetected, without any attention to historical issues/ undesirable actions.

9.18 There is evidence to show that operators have no control and a lack of due diligence checks conducted on their white label partner(s). The Commission expects operators to manage and control risks associated with embarking on a partnership with third-party white labels. This means the operator is accountable for any criminal benefit or money laundering breaches in the event it was caused by the white label partner.

9.19 In order to safeguard the operator and fully mitigate the risks surrounding money laundering and terrorist financing (ML/TF), the operator should only use white label partners to provide marketing and branding. The maintenance of duties such as 'back office' facilities which includes managing all customer interaction through frontline customer service, VIP services and AML checks conducted on customers, including the direct liaison with customers should be completed directly by operators. AML/CTF checks on customers should not be delegated to the white label partner.

9.20 This emerging risk will be updated in the next publication of the risk assessment and is currently rated as high risk.

GAMBLING COMMISSION

Lotteries (non-remote and remote), including the National Lottery

10 Lotteries

Lotteries (remote and non-remote) including National Lottery	Previous overall risk rating	Current overall risk rating
	Low	Low

Existing inherent risk rating

10.1 Further information on the risk, the consequences and the controls, please see the previous publication. The assessment shows that no significant change has occurred for each risk area.

Lotteries (remote and non-remote) including National Lottery	Vulnerability	Risk	Previous overall rating	Likelihood of event occurring	Impact of event occurring	Movement
				Current rating		
	Operator Control	Operators failing to comply with prevention of money laundering and terrorist financing legislation and guidance	L	L	L	↔
	Licensing and integrity	Lottery operator acquired by organised crime to launder criminal funds	L	L	M	↔
	Customer	Anonymous customers (non-remote), excluding the National Lottery	L	M	VL	↑
	Customer	Anonymous customers (non-remote) - National Lottery only	M	M	M	↔
	Customer	False and stolen identity documentation	L	L	L	↔
	Customer	Customer not physically present (remote), excluding the National Lottery	L	L	L	↔
	Customer	Customer not physically present (remote) – National Lottery only	L	L	L	↔
	Products	Scratch cards/interactive instant win games	L	L	VL	↔
	Means of Payment	Cash transactions	L	L	M	↔

Existing emerging risks

10.3 There are no existing emerging, no new inherent and no further new emerging risks in the lotteries (remote and non-remote) including National Lottery sector.

GAMBLING COMMISSION

Remote: Casinos

11 Casino (remote)

Casino (remote)	Previous overall risk rating	Current overall risk rating
	Higher	High

Existing inherent risk rating

11.1 Further information on the risk, the consequences and the controls, can be found in the previous assessment. This year's assessment shows that no significant change has occurred for each risk area.

	Vulnerability	Risk	Previous overall rating	Likelihood of event occurring	Impact of event occurring	Movement
				Current rating		
Casinos (remote)	Operator Control	Operators failing to comply with prevention of money laundering and terrorist financing legislation and guidance	H	H	H	↔
	Licensing and integrity	Gambling operations run by organised criminals to launder criminal funds	MH	M	H	↔
	Customer	Customer not physically present for identification purposes	H	H	H	↔
	Customer	False or stolen identity documentation used to bypass controls to facilitate the laundering of criminal funds	M	M	H	↑
	Customer	Accessibility to multiple remote casinos	H	H	H	↔
	Customer	Customers from high risk jurisdictions using casino facilities to launder criminal funds	M	L	VH	↔
	Customer	Customers who appear on sanctions lists laundering criminal funds	M	L	VH	↔
	Customer	PEPs using casinos to launder illicit or criminal funds	M	M	VH	↑
	Customer	Domestic Politically Exposed Person (PEP) identification & verification	M	M	M	↔
	Customer	International PEP using casinos to clean criminal funds	MH	M	VH	↑

Existing emerging risks

11.3 The existing emerging risks in the casino remote sector identified in the previous risk assessment have been assessed and rated as below. The risk level has increased for the poker related product risks and note the slight change (increase) in the vulnerabilities around pre-paid cards as a means of payment risk. For more detail on the vulnerabilities, consequences and controls; please see last year's published risk assessment.

Peer to peer gaming (poker) - B2B & B2C

11.4 The vulnerability of peer-to-peer gaming (poker) is associated with the ability for customers to collude and deliberately 'transfer' funds to one another, sometimes referred to as 'chip dumping'. The Commission considers the impact of peer-to-peer gaming (poker) offered by remote casinos through B2B and B2C gaming operators providing facilities as being very detrimental and a 'high' risk rating has been given. This has not changed from the 'higher' rating from last year's risk assessment.

E-Wallets

11.5 Limited examples of vulnerabilities related to e-wallets being used to place laundered funds into the gambling industry , however, FATF recognises the ML/TF risk associated with this payment type. This payment methods makes it difficult for the operator to identify the source of funds. This vulnerability creates difficulties in identifying where the funds for gambling are coming from.

Pre-paid cards

11.6 This vulnerability creates difficulties in identifying where the funds for gambling are coming from. The risk is deemed higher than a customer using a debit card due to the anonymous nature of vulnerabilities associated with the use of these cards and the demand of further AML checks. However, the monetary limits attached to the conditions of use of pre-paid cards mitigates the money laundering risks somewhat. There is no change in the risk rating from the previous assessment.

Digital/Crypto-assets

11.7 Digital and crypto-assets are recognised as an emerging means of payment vulnerability, however, use of such currencies has not widely emerged within the sector. The potential use of digital or crypto-assets to launder criminally derived funds is relevant to payment type vulnerabilities. Although limited in use at present, the ongoing use of such currencies by organised crime highlights the potential for abuse within the British gambling industry. The Commission recognises the higher risk associated with digital currencies if they were to be used within the sector. Little evidence is yet revealed that an operator can demonstrate they can effectively manage risk to do with the use of digital currencies. A medium rating is given to this risk and further update will be sought in the next risk assessment.

Casinos	Vulnerability	Risk	Previous overall rating	Likelihood of event occurring	Impact of event occurring	Movement
				Current rating		
	Product	Peer to peer gaming (poker) - B2B	H	H	H	↔

	Product	Peer to peer gaming (poker) - B2C	H	H	H	↔
	Means of Payment	E-wallets	M	M	M	↔
	Means of Payment	Pre-paid cards	M	M	M	↔
	Means of Payment	Digital/ Crypto-assets	M	M	M	↔

New inherent risks

11.8 Following in-depth analysis, this assessment has captured further vulnerabilities which builds on further from the previous assessment:

Issue / Threat	Sector	Type of Vulnerability	Likelihood of event occurring	Impact of event occurring	RAG
Vulnerability The incompetence of key personnel and licence holders exploited by criminals seeking to launder the proceeds of crime in the remote casino sector. This risk has been rated as 'high' due to its detrimental impact should it materialise. **Consequences** Poor competence and lack of suitability can result by having: • Poor policies, procedures, controls, monitoring and training • Lack of decisive action in regard to suspicious activity or unclear, unrecorded or uncontrolled decision making • high staff turnover/ lack of resources can result in a failure to understand risk and identify issues relating to ML/TF • failing business models which does focus on commercial advantages and does not factor in governance and measures around AML/CTF • Failing to embed AML/CTF learning published by the Commission which can exacerbate existing ML vulnerabilities in this sector, such as criminal lifestyle spending and 'smurfing' • Continued evidence of money laundering through collusion, cheating and criminal lifestyle spending, due to policies, procedures and controls not being effectively implemented, monitored or revised by senior licensed employees • Licensed employees colluding with customers for personal gain remains evident in the sector. Cheating is a criminal offence under the Act and any personal gain from cheating is the proceeds of crime • Failure by senior management and nominated officers to identify areas of ineffective or negligent staff training, which results in poor compliance by staff, including: not following policies, procedures and controls; and not identifying that senior licensed staff are failing to monitor the effectiveness of employees' performance and their ability to follow policies, procedures and controls. Senior management's failure to	Casino remote	Operator Control	H	H	4

identify and rectify failures by employees in the above areas remains a concern in the sector • Nominated officers' failing or being prevented by senior management to submit SARs when knowledge or suspicion has been identified by them. Procedures are not sufficiently effective for the nominated officer to assess whether knowledge and suspicion has been identified, both remain areas of concern in this sector • Failure by licensed employees and senior management to follow their own policies, procedures and controls intended to mitigate ML/TF has resulted in criminal lifestyle spending continuing in the sector • Lack of understanding of when to submit and/ or the lack of submitting of 'Defence against money laundering' or 'Defence against terrorist financing' (DAMLs/DATFs) to prevent a principle ML offence being committed. This includes submitting DAMLs/DATFs post movement of monies to obtain a defence as opposed to pre-movement. The Commission will take affirmative action where it identifies non-compliance, which may range from action plans through to the review and/or revocation of personal and/or operating licences. Failure to follow good practice as advised by the Commission, through ordinary code provision 2.1.1, will be a material factor in considering any action we take to review and/or revoke personal and/or operating licences.					

Controls / Mitigations	
• Ensuring fit and proper persons are in key positions. Operators and key personnel must comply and implement with the Act, POCA, TACT, and LCCP policies, procedures and controls to mitigate the risk of ML/TF occurring. Policies, procedures and controls implemented effectively should minimise the risk of ML/TF through effective risk assessments, monitoring, training and revision of risk assessments. • Senior management must appoint a nominated officer and must comply with requirements in the Regulations to minimise the risk of ML/TF occurring. The role of the nominated officer includes reporting suspected or known ML/TF activity via SARs, providing adequate training to employees, and reporting annually on the business's AML activities to their senior management and board.	Preventive
• Policies, procedures and controls implemented effectively should minimise the risk of ML/TF through effective risk assessments, monitoring, training and revision of risk assessments.	Preventive
• In instances where there are concerns about staff integrity, operators will act where appropriate. If the staff are also licensed by the Commission, we may consider revocation of their personal licences. • Adequate supervision of table gaming and gaming machines minimise the risk of money laundering, criminal lifestyle spend, cheating and collusion.	Detective

Issue / Threat	Sector	Type of Vulnerability	Likelihood of event occurring	Impact of event occurring	RAG
Vulnerability Lack of adequate and relevant due diligence checks conducted resulting in criminals exploiting the remote casino sector by laundering the proceeds of crime. This risk has been rated as 'high' due to the Regulations imposing additional requirements on the regulated sector. These include risk assessments and requirements in respect of written policies, and procedures and controls, internal controls, CDD, record keeping and training. The Commission also holds intelligence and evidence of this vulnerability materialising. **Consequences** The consequences of poor customer due diligence, enhanced due diligence (CCD/EDD) and source of funding/wealth checks: • The carrying out of the CDD/EDD obligations, including monitoring customer transactions and activity being improper i.e. poor record keeping, not adopting a risk-based approach and failing to identify suspicious activity • Money laundering through collusion, cheating and criminal lifestyle spending, due to policies, procedures and controls not being effectively implemented, monitored or revised by senior licensed employees. Failure by licensed employees to follow policies, procedures and controls intended to mitigate ML/TF has resulted in criminal lifestyle spending continuing in the sector • Failure by senior management and nominated officers to identify areas of ineffective or negligent staff training, which results in poor compliance by staff, including: not following policies, procedures and controls; and not identifying that senior licensed staff are failing to monitor the effectiveness of employees' performance and their ability to follow policies, procedures and controls • Use of VPN to mask identification of customer location, for example, when players from high risk jurisdiction use VPNs to mask their true location. The money laundering risk is heightened when used as part of stolen/ fraud identification as lack of identification checks by an operator into a player's location to link the log in of customer can create a vulnerability • Lack of understanding in the remote casino sector around a business relationship and when that is triggered. Real-time reporting of suspicious behaviour triggered by employee intervention, automated systems and/or observed behaviour is delayed due to the use of threshold and or hybrid CDD models, limiting the level of information known about customers • Senior management decision makers with oversight of data	Casino remote	Operator Control	M	H	6

and suspicion are not effectively identifying criminal lifestyle spending within their estate and reporting it to law enforcement • Failing to monitor the sanctions list, for either country or individual restrictions, resulting in illicit funds being used in the sector and ultimately infiltrating the UK's financial system. Failing to identify PEPs prior to gaming increases the likelihood of monies derived from corruption being laundered through the casino and ultimately infiltrating the UK's financial system • The Commission is not assured by the remote casino sector's compliance with the Act, POCA, TACT, the Regulations, LCCP and Commission guidance. The evidence gathered during the assessments demonstrated frequent and systemic failures in complying with the legal requirements. This non-compliance significantly increases the likelihood of vulnerabilities being exploited in the sector.					

Controls / Mitigations	
• Conducting adequate CDD/EDD checks, including the verification of customer identities and source of funds, which should limit the risk of exposure to money laundering. • Using Commission published guidance when conducting checks and considering the following: ○ adopting a risk-based approach ○ senior management taking responsibility for effectively managing the money laundering and terrorist financing risks faced by the casino operator's businesses; ○ the role and responsibilities of the nominated officer; ○ the proper carrying out of the CDD/EDD obligations, including, when a business relationship is formed, monitoring customer transactions and activity; ○ record keeping; and ○ the identification and reporting of suspicious activity. • This includes PEP monitoring which should minimise the risk of corruption and the risk of money laundering occurring. • Ensuring effective monitoring of sanction lists, both country and individual specific, taking note of the restrictions and acting accordingly to mitigate the risk of criminally derived cash infiltrating the UK financial and associated sectors.	Detective
• Policies, procedures and controls implemented effectively should minimise the risk of ML/TF through effective risk assessments, monitoring, training and revision of risk assessments. • This includes adequate staff supervision of customer accounts and automated triggers derived from transactional data assist in identifying and reporting suspicious behaviour by customers to law enforcement.	Preventive
• Account-based play increase the operators' ability to know their customers, confirm their details and verify their identity, ascertain their source of funds and wealth, and check their PEP and sanctions list status. This decreases the risk of money laundering and terrorist funding in the sector. • The operator should assess the threat of criminals utilising VPN to mask identification on location and implement relevant controls to mitigate this risk.	Preventive

Issue / Threat	Sector	Type of Vulnerability	Likelihood of event occurring	Impact of event occurring	RAG
Vulnerability Casinos acting as money service businesses (MSB) Due to the nature of the risk and that it is identified as a high-risk area and specific jurisdictions of high risk are identified by the HM Treasury's National Risk Assessment and law enforcement agencies. **Consequences** Under the MLR 2017 an MSB is defined as a natural or legal person which by way of business operates a currency exchange office, cashes cheques made payable to customers or transmits money (or any representation of monetary value) by any means. It is understood that certain casinos offer, incidentally to their main gaming activities, MSB services (cashing cheques or money transmission and currency exchange activities) for their casino customers. Risk based consequences regarding the provision of MSBs: • MSB activities, such as foreign currency exchange, not implemented correctly or effectively may result in overseas criminally derived funds infiltrating the UK's financial system and the potential for committing criminal offences by circumventing other jurisdictions' money laundering legislation and controls • Customer records not being maintained/ or adequately maintained • Operators having a lack of understanding the ML/TF risks associated with MSB provisions • There is a threat of casino members/ customers not using the casino for the purposes of gambling but purely to utilise the MSB facilities, thus using it as a bank rather than a casino • It is known that casinos use third parties to conduct currency conversion. It is not known whether casinos have adequately vetted these parties and if they adopt the casinos policies and procedures. Therefore, opening to the risk of money laundering and terrorist financing • MSBs can be used by casino employees and it is not known if there are adequate internal controls in place. This presents a risk of money laundering and terrorist financing to happen in 'plain sight'.	Casino remote	Means of Payment	H	H	4

Controls / Mitigations

• Policies, procedures and controls implemented effectively should minimise the risk of ML/TF through effective risk assessments, monitoring, training and revision of risk assessments. • Legislation includes Section 81 of the Act which prohibits credit in casinos. With effectively implemented policies and procedures, this limits the risk of illegal money lending (which is also subject to an ordinary code provision in LCCP 3.8.1). Casinos also must comply with The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Regulations) in respect of Money Business Services for foreign currency exchange to minimise the risk of ML/TF.	Preventive
• Operators providing these services may gain a fuller view of the characteristics of gamblers and the detection of criminal activity done effectively and efficiently. Controls can be in the form of conducting further risk assessment for MSB activities and incorporate obligations to conduct further checks and maintain records by putting enough processes and procedures in place. Operators providing MSB activity may then gain a better picture of the characteristics of gamblers by further KYC, source of funds, audit trails which helps in detecting criminal activity more quickly.	Detective

Issue / Threat	Sector	Type of Vulnerability	Likelihood of event occurring	Impact of event occurring	RAG
Vulnerability Undermining of the Money Laundering Reporting Officer (MLRO) or nominated officer in the gambling operation can intentionally or unintentionally lead to exploitation by money launderers. This risk has been rated as 'high' as the Commission has evidence that there is a vulnerability in operators where the MLRO/ nominated officer is not a 'key position' in the business and in some instances, this undermines the importance of the role. **Consequences** Risk based consequences regarding the undermining of the nominate officer/ MLRO: • Employees not sighting or seeking guidance from their nominated officer as appropriate. Under POCA and the Terrorism Act, individual employees face criminal penalties if they are involved in money laundering or terrorist financing. If they do not make an internal report to their nominated officer when necessary, they may also face criminal sanctions. It is important, therefore, that employees are made aware of their legal obligations, and are given training in how to discharge them • Senior management not involving/ adequately sighting the nominated officer in operational matters and the effectiveness of the operator's systems and controls to combat money laundering and terrorist financing • Senior management favouring commercial advantages over AML obligations, without considering input from the	Casino remote	Operator Control	H	H	4

nominated officer or disregarding the concerns of the nominated officer • The nominated officer does not have sufficient seniority within the business with a clear path of reporting to Board or the equivalent.					

Controls / Mitigations	
• Senior management should require that the nominated officer provides an annual report covering the operation and effectiveness of the operator's systems and controls to combat money laundering and terrorist financing and take any action necessary to remedy deficiencies identified by the report in a timely manner. In practice, senior management should determine the depth and frequency of information provided by the nominated officer that they feel is necessary to discharge their responsibilities.	Preventive
• Casino operators should also ensure that relevant employees are aware of and understand: the identity, role and responsibilities of the nominated officer, and what should be done in their absence. • The nominated officer should be heavily involved in devising and managing the delivery of such training, taking particular care to ensure that systems are in place to cover all part-time or casual employees.	Detective
• The nominated officer is responsible for the oversight of all aspects of the casino operator's AML/CTF activities at all premises. They are the focal point for all activity within the operator relating to AML/CTF. The individual appointed as nominated officer must have a sufficient level of seniority. • The nominated officer should hold a personal management licence (PML) issued by the Commission. • The job description of the nominated officer should clearly set out the extent of the responsibilities given to it and its objectives. The nominated officer will need to be involved in establishing the basis on which a risk-based approach to the prevention of money laundering and terrorist financing is put into practice. • Accurate record keeping of reporting must be maintained as a matter of course. Staff must be aware of the reporting process and including how and when to report. The nominated officer is obliged to keep written records including the decisions made and particularly when a decision is made not to report.	Preventive

New emerging risks

Gambling as a disguise for cash deposits into bank accounts

11.9 This typology of masking illicit funds as gambling winnings into bank accounts has been identified as a possible vehicle for money laundering. This risk closely ties in with the 'lack of adequate CDD and / or EDD' risk outlined above due to links with source of funds and source of wealth. The gambling industry must remain vigilant to criminals and if it is known or suspected that there has been money laundering or terrorist financing, operators are reminded of the obligations to make reports to the National Crime Agency's suspicious activity reporting (SAR) regime. An overall 'medium' rating is given to this risk and further update will be sought in the next risk assessment.

GAMBLING COMMISSION

Remote: Betting and bingo sectors

12 Betting and bingo sector (remote)

Betting and bingo sector (remote)	Previous overall risk rating	Current overall risk rating
	Higher	High

Existing inherent risk rating

12.1 For further information on the risk, the consequences and the controls, please see the previous assessment. This assessment shows that overall, there has been no significant change in the judgement of risk in this sector. Please note some slight variances on the inherent risks, which has been assessed as below for each risk area.

Betting and bingo sector (remote)	Vulnerability	Risk	Previous overall rating	Likelihood of event occurring	Impact of event occurring	Movement
				Current rating		
	Operator Control	Operators failing to comply with prevention of money laundering and terrorist financing legislation and guidance	H	H	H	↔
	Operator Control	Operators staking and winning directly and indirectly on their own products	M	M	M	↔
	Licensing and integrity	Gambling operations run by organised criminals as a means to launder criminally derived funds	MH	M	H	↔
	Customer	Customer not physically present for identification	H	M	H	↓
	Customer	False or stolen documentation used to bypass controls in order to launder criminally derived funds	H	M	H	↓
	Customer	Accessibility to multiple remote accounts	H	H	H	↔
	Customer	Customers from high risk or non-cooperative jurisdictions using remote facilities to launder criminally derived funds (Betting -remote sector only)	MH	M	VH	↑
	Customer	Customers who appear on international sanctions lists laundering criminally derived funds (Betting -remote sector only)	MH	VL	H	↓

Existing emerging risks

12.3 The existing emerging risks in the betting and bingo remote sector identified in the previous risk assessment have been assessed and rated as below. There is no significant change in

the risk ratings due to no real movement. For more detail on the vulnerabilities, consequences and controls; please see last year's published risk assessment.

'Bring your own device' (BYOD)

12.4 The last version noted the product risk of BYOD is identified in the non-remote betting sector. However, customers using their own mobile devices to place bets on licensed premises is being used in remote gambling. This year's review of the current threat of BYOD has shown non-emergence. The threat is reduced as the Commission is not aware are of any operator offering the facility.

Ultimate beneficial ownership (UBO) and seeding

12.5 This risk relating to means of payment arises when businesses apply to be licensed, or those already licensed, apply for a 'Change of Corporate Control' (CoCC). It has emerged that companies incorporated in overseas jurisdictions with overseas UBOs are then attracting new shareholders who are expected to place liquidity (through a seeding arrangement) into the betting exchange. In the absence of information regarding the secondary shareholders adding liquidity to the betting exchange, the Commission will not be sufficiently assured regarding the source of wealth and funds. This potentially exposes the British gambling market and consumers to the risk of ML/TF. This emerging risk has been revealed in the remote betting sector, however, sufficiently robust controls implemented by the Commission have so far prevented any applications or CoCC being granted under these circumstances and is rated the same as last year.

E-wallets

12.6 Limited vulnerabilities of e-wallets being used to place laundered funds into the gambling industry have been realised, however, FATF recognises the ML/TF risk associated with this payment type. This payment method makes it difficult for the operator to identify the source of funds. This vulnerability creates difficulties in identifying where the funds for gambling are coming from.

Pre-paid cards

12.7 This vulnerability creates difficulties in identifying where the funds for gambling are coming from. The risk is deemed higher than a customer using a debit card due to the anonymous nature of vulnerabilities associated with the use of these cards and the demand of further AML checks. However, the monetary limits attached to the conditions of use of pre-paid cards mitigates the money laundering risks somewhat. There is no change in the risk rating from the previous assessment.

Digital/Crypto-assets

12.8 Digital and crypto-assets are recognised as an emerging means of payment vulnerability, however, use of such currencies has not widely emerged within the sector. The potential use of digital or crypto-assets to launder criminally derived funds is relevant to payment type vulnerabilities. Although limited in its use at present, the ongoing use of such currencies by organised crime highlights the potential for abuse within the British gambling industry. The Commission recognises higher risk associated with digital currencies if they were to be used within the sector. Limited evidence as yet is revealed that an operator can demonstrate they can effectively manage risk to do with the use of digital or crypto-assets. A further update will be sought in the next risk assessment.

Betting and bingo	Vulnerability	Risk	Previous overall rating	Likelihood of event occurring	Impact of event occurring	Movement
				Current rating		
	Product	'Bring your own device' (BYOD) where consumers use their own device to place bets through non-account-based play.	M	VL	M	↓
	Means of Payment	Ultimate beneficial ownership (UBO) and seeding	MH	M	H	↔
	Means of Payment	E-wallets	M	M	M	↔
	Means of Payment	Pre-paid cards	M	M	M	↔
	Means of Payment	Digital/ Crypto-assets	M	M	M	↔

New inherent risks

12.9 Following in-depth analysis, this assessment has captured further vulnerabilities which builds on further from the previous publication:

Issue / Threat	Sector	Type of Vulnerability	Likelihood of event occurring	Impact of event occurring	RAG
Vulnerability The incompetence of key personnel and licence holders exploited by criminals seeking to launder the proceeds of crime in the remote betting sector (remote betting sector only as deemed as higher risk than remote bingo sector). This risk has been rated as 'high' due to its detrimental impact should it materialise. **Consequences** Poor competence and lack of suitability can result by having: • Poor policies, procedures, controls, monitoring and training • Lack of decisive action, high staff turnover/ lack of resources and/ or failing business model • Failing to embed AML learning published by the Commission which can exacerbate existing ML vulnerabilities in this sector, such as criminal lifestyle spending and 'smurfing' • Continued evidence of money laundering through collusion, cheating and criminal lifestyle spending, due to policies, procedures and controls not being effectively implemented, monitored or revised by senior licensed employees • Failure by senior management and MLROs to identify areas of ineffective or negligent staff training, which results in poor compliance by staff, including: not following policies, procedures and controls; and not identifying that senior	Betting remote	Operator Control	H	H	4

licensed staff are failing to monitor the effectiveness of employees' performance and their ability to follow policies, procedures and controls. Senior management's failure to identify and rectify failures by employees in the above areas remains a concern in the sector • MLROs failing to submit SARs when knowledge or suspicion has been identified by them, or procedures are not sufficiently effective for the MLRO to assess whether knowledge and suspicion has been identified, remains an area of concern in this sector • Failure by licensed employees to follow policies, procedures and controls intended to mitigate ML/TF has resulted in criminal lifestyle spending continuing in the sector. The Commission will take affirmative action where it identifies non-compliance, which may range from action plans through to the review and/or revocation of personal and/or operating licences. Failure to follow good practice as advised by the Commission, through ordinary code provision 2.1.1, will be a material factor in considering any action we take to review and/or revoke personal and/or operating licences.					

Controls / Mitigations	
• Ensuring fit and proper persons are in key positions. Operators and key personnel must comply and implement the Act, POCA, TACT, and LCCP policies, procedures and controls to mitigate the risk of ML/TF occurring. Policies, procedures and controls implemented effectively should minimise the risk of ML/TF through effective risk assessments, monitoring, training and revision of risk assessments. • Senior management must appoint a MLRO and must comply with requirements in POCA and TACT to minimise the risk of ML/TF occurring. The role of the MLRO includes reporting suspected or known ML/TF activity via SARs, providing adequate training to employees, and reporting annually on the business's AML activities to their senior management and board.	Preventive
• Policies, procedures and controls implemented effectively should minimise the risk of ML/TF through effective risk assessments, monitoring, training and revision of risk assessments.	Preventive
• In instances where there are concerns about staff integrity, operators will act where appropriate. If the staff are also licensed by the Commission, we may consider revocation of their personal licences.	Detective

Issue / Threat	Sector	Type of Vulnerability	Likelihood of event occurring	Impact of event occurring	RAG
Vulnerability Lack of adequate 'know your customer' (KYC) checks conducted resulting in criminals exploiting the remote betting and bingo sector by laundering the proceeds of crime. **Consequences** The consequences of poor KYC checks: • the Commission is not assured by the remote betting and bingo sector's compliance with the Act, POCA, TACT, LCCP and Commission guidance. The evidence gathered during the assessments demonstrated frequent and systemic failures in complying with the legal requirements. This non-compliance significantly increases the likelihood of vulnerabilities being exploited in the sector • money laundering through collusion, cheating and criminal lifestyle spending, due to policies, procedures and controls not being effectively implemented, monitored or revised by senior licensed employees. Failure by licensed employees to follow policies, procedures and controls intended to mitigate ML/TF has resulted in criminal lifestyle spending continuing in the sector • failure by senior management and MLRO to identify areas of ineffective or negligent staff training, which results in poor compliance by staff, including: not following policies, procedures and controls; and not identifying that senior licensed staff are failing to monitor the effectiveness of employees' performance and their ability to follow policies, procedures and control • use of VPN to mask identification of customer location, for example, when players from high risk jurisdiction use VPNs to mask their true location. The money laundering risk is heightened when used as part of stolen/ fraud identification as lack of identification checks by operator into a player's location to link the log in of customer, can create a vulnerability • senior management decision makers with oversight of data and suspicion are not effectively identifying criminal lifestyle spending within their estate and reporting it to law enforcement • failing to monitor the sanctions list, for either country or individual restrictions, resulting in illicit funds being used in the sector and ultimately infiltrating the UK's financial system. Failing to identify PEPs prior to gaming increases the likelihood of monies derived from corruption being laundered through the casino and ultimately infiltrating the UK's financial system.	Betting & bingo remote	Operator Control	M	H	6

Controls / Mitigations	
• Conducting adequate KYC checks, including the verification of customer identities and source of funds, which should limit the risk of exposure to money laundering. • Ensuring effective monitoring of sanction lists, both country and individual specific, taking note of the restrictions and acting accordingly to mitigate the risk of criminally derived cash infiltrating the UK financial and associated sectors.	Detective
• Policies, procedures and controls implemented effectively should minimise the risk of ML/TF through effective risk assessments, monitoring, training and revision of risk assessments. • This includes adequate staff supervision of customer accounts and automated triggers derived from transactional data assist in identifying and reporting suspicious behaviour by customers to law enforcement.	Preventive
• Account-based play increases the operators' ability to know their customers, confirm their details and verify their identity, ascertain their source of funds and check their PEP and sanctions list status. This decreases the risk of money laundering and terrorist funding in the sector. • The operator should assess the threat of criminals utilising VPN to mask identification on location and implement relevant controls to mitigate this risk.	Preventive

New emerging risks

12.10 No new emerging risks in the betting & bingo remote sector.

Terrorist financing vulnerabilities

13 Terrorist financing in gambling

13.1 Risks and typologies of terrorist financing (TF) differ considerably in comparison to money laundering. Whilst there is little evidence of terrorists manipulating or taking advantage of the gambling industry; there is no room for complacency or assumption that there is no TF risk.

13.2 The Commission expects operators to consider vulnerabilities in their business which can be exploited by potential terrorists. Therefore, a catch-all inherent risk is described below:

Issue / Threat	Sector	Type of Vulnerability	Likelihood of event occurring	Impact of event occurring	RAG
Vulnerability Operators failing to understand or take consideration of terrorist financing vulnerabilities and applicable legislation. Rated overall as 'medium', having taken into consideration the nature of the risk and the impact of the event occurring. **Consequences** The Commission is not aware of any imminent threat posed to the gambling industry from terrorist financing. However, due to the current threat that terrorism poses to the UK; everyone has a responsibility to remain vigilant and report any suspicious activity. Consideration must be given to the following: • Operators and employees may not be aware of this vulnerability or may believe they are not at risk • criminals/ potential terrorists exploiting operators based on location. Being city-centre based or in a crowded area may carry a higher risk • criminals who may openly discuss their wrong-doing, ownership of weapons or demonstrate extremist views or have access to terrorist propaganda • it is known that some terrorists conduct 'hostile reconnaissance' i.e. they conduct research on a target such as determining the best method of attack, assessment of the level or security and at what time to conduct the attack. The information they gather can be from online materials, onsite or from an 'insider' • terrorists can be employed by businesses by concealing their identities and/ or their intentions in order to conduct hostile reconnaissance • operators and their employees may come across barriers to reporting suspicious behaviour such as embarrassment, they do not want to be involved, they may have concerns they may be wrong, or they are not	All	All	L	H	8

sure of where to go for help and support.					

Controls / Mitigations	
• Operators and employees must familiarise themselves with guidance and protective security around the risk of terrorism, domestic extremism and terrorist financing. • For further support and guidance please visit: ○ National Counter Terrorism Security Office www.gov.uk/NaCTSO ○ Centre for Protection of Critical National Infrastructure www.gov.uk/CPNI ○ Citizen AID www.citizenaid.org For reporting suspicious behaviour, please call the Anti–Terrorism Hotline confidentially on 0800 789 321 the line is open 24 hours, 365 days and all calls will be treated seriously. Or, alternatively, complete the online form at www.act.campaign.gov.uk • Please use the UKFIU's existing SAR process for all reporting of suspicions of terrorism funding. • If you have specific questions around suspected terrorism & extremism in gambling, please contact the AML Team in the Commission AMLCTFEnquiries@gamblingcommission.gov.uk. • If you have specific questions about domestic extremism or terrorism, please contact Counter Terrorism Policing: CTP-NOCMailbox-.ILO@met.pnn.police.uk.	Preventive
• Gambling operators should gather knowledge and understanding of the threats and vulnerabilities around terrorism and the funding of terrorism. This includes the awareness of high-risk jurisdictions such as those where terrorist groups may be in government. • There are a number of key phrases, terminology and numerical combinations, which terrorists and extremist groups use to communicate between themselves. Mitigation around this, is having awareness of the types known and factoring this information into internal controls and algorithms. This, together with informing staff to remain vigilant, will enable the detection of suspicious behaviour. • Another mitigation is to ensure there are mechanisms in place to detect sudden changes in customer behaviours that corresponds with typologies known to be demonstrated by terrorists and to ensure risk triggers in internal controls are able to identify these events.	Detective

14 Methodology

14.1 Our methodology defines risk to be the potential that an event, action, or series of events or actions will have an adverse effect on the Regulations, POCA, TACT, the Act's licensing objectives or the LCCP.

14.2 The reporting period this assessment is based on is from the 1 November 2017 to the 31 October 2018. This assessment of ML/TF risk has been developed in consultation with sector and/or industry specialists. The Commission has liaised with law enforcement, including the National Crime Agency (NCA), and considered approaches taken by other AML supervisory authorities such as the Financial Conduct Authority (FCA). The Commission also supports HM Treasury's National Risk Assessment of ML/TF 2017 as guidance, when considering key threats posed by the risks identified to the British gambling market and its consumers.

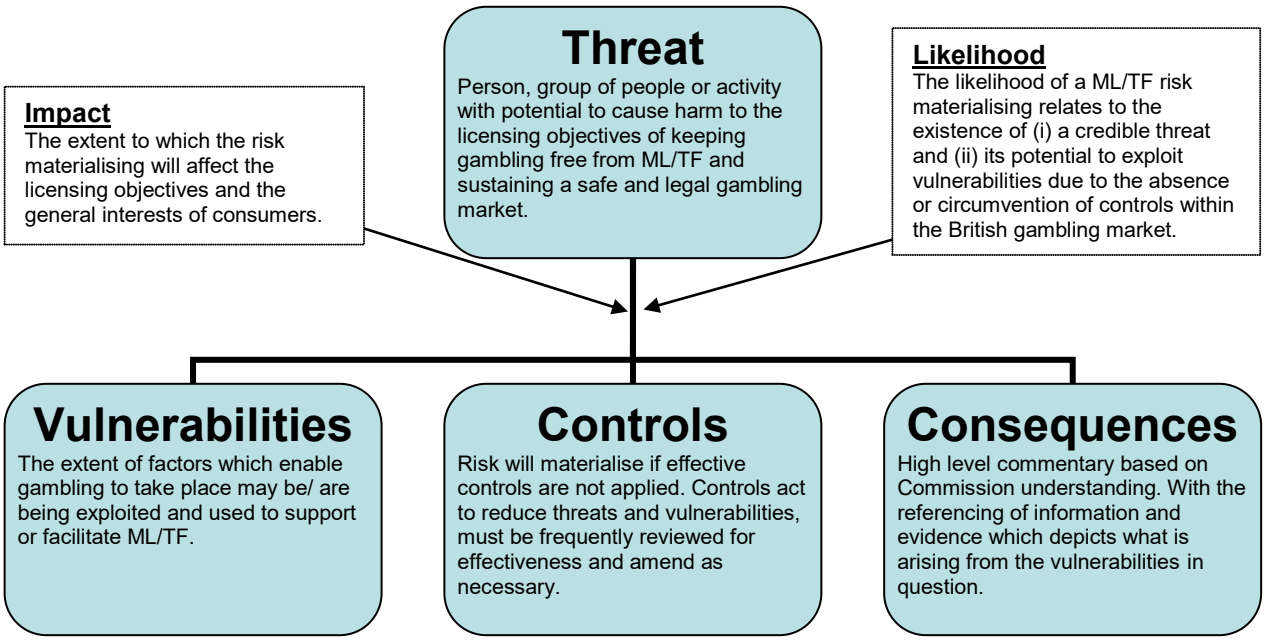
14.3 The Commission recognises the methodology used by the Financial Action Task Force (FATF) which sets the global standard for anti-money laundering and counter-terrorist financing and adopts a similar framework upon which to base our analysis.

14.4 In addition to considering risk in the context of individual licensees we consider risk in the context of the collective actions or vulnerabilities in sectors, thematic indicators or the wider industry. We refer to this as systemic risk, in that the events or actions will have a widespread negative consequence across a sector impacting widely upon consumers.

14.5 It is also important to note that the Commission's assessment of risk within each sector or theme are considered in the context of the British gambling industry not in comparison to other British regulated industries, for example, the retail banking sector. Furthermore, the Commission may not have access to the confidential source materials available to HMT, limiting our assessment to our own data and specialists, and external available sources.

14.6 The methodology uses an approach that can be represented as **likelihood X impact = risk rating.**

The Commission's risk assessment methodology:



14.7 The Commission's methodology considers risk to be a function of threat, vulnerabilities, controls and consequences. From this, we assess the likelihood of ML/TF taking place and the subsequent impact upon the strategy of keeping gambling free from the proceeds of criminality. The Commission forms a view from evidence, intelligence and Commission specialists to assess the level of risk involved, and makes judgements, as to both the likelihood and impact of money laundering, enabling the identification of controls to address its causes or to minimise its consequences.

Application of approach:

<table>
<tr>
<td>Threats:

The threat can manifest itself through the intentional 'washing' of criminal funds, through criminal spending or terrorist financing. It can relate to people seeking control of gambling businesses for illegal purposes or responsible people recklessly or unwittingly facilitating ML/TF through their failures to discharge their responsibilities effectively.</td>
<td>Vulnerabilities:

The Commission has grouped the relevant factors that are assessed as vulnerabilities into five categories. These are:

• Licensee controls and vulnerabilities (including the levels of awareness and compliance with Money Laundering Regulations, POCA, TACT, MSBs (where applicable) LCCP and Commission guidance and public learning)
• Licensing and integrity related vulnerabilities
• Customer related vulnerabilities
• Product related vulnerabilities
• Means of payment related vulnerabilities.</td>
<td>Controls:

The assessment of vulnerabilities requires assessment of the effectiveness of the controls in place. The absence of, or ineffectual application of controls would indicate a high level of vulnerability.
The Commission considers controls to include:

• ongoing employee training
• the design, application and review of policies and procedures
• the monitoring of their effectiveness
• for licensees to act upon identified threats and vulnerabilities to reduce the likelihood of ML/TF risks materialising.

Controls are primarily the responsibility of the Licensee but may also include actions taken by the Commission through its licensing, compliance or enforcement actions and its supervisory authority role.</td>
<td>Consequences:

This is a high-level commentary as to what the Commission is seeing, to support the risk assessment produced by Commission specialists. It references information and evidence which depicts what is arising from the vulnerabilities in question.</td>
</tr>
<tr>
<td colspan="2">Likelihood:

In assessing the likelihood of a threat materialising the Commission may also consider:

• The volume, variety (from different gambling activities) and the speed of monetary transactions
• The levels of SAR submissions by licensees
• The complexity of products and services present within each sector
• The sectors global connectivity.</td>
<td colspan="2">Impact:

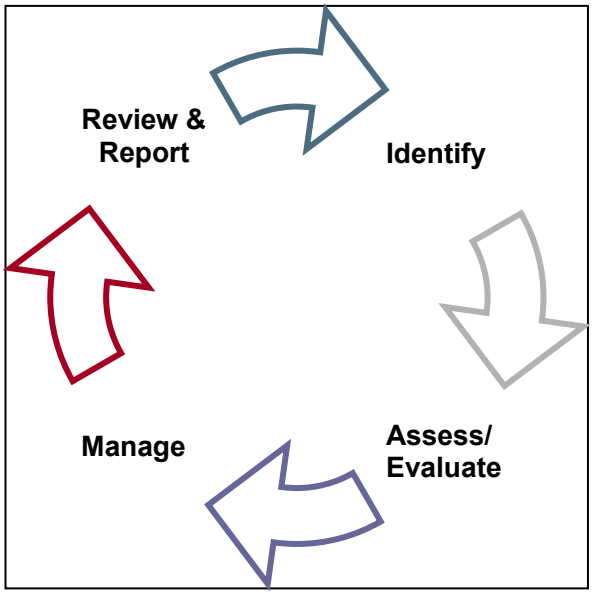
The impact is assessed to be the extent at which the risk materialising will influence the licensing objectives and the general interest of consumers. It also allows the Commission (as supervisory authority) to:

• assess, review and monitor the effectiveness of the regulatory framework in place to minimise ML/TF in the British gambling market and provides evidence and information
• enable its approach to be adapted to the highest risks being posed by organised criminal gangs or individual perpetrators of ML/TF</td>
</tr>
</table>

14.8 The methodology has developed since the previous risk assessment published in March 2017 due to the evolving nature of our risk-based approach. This is to further ensure risks and vulnerabilities are captured and evaluated in a controlled manner, that is transparent and consistent across the gambling industry.

14.9 The improved risk-based approach adopted, has the following risk management cycle. Managing risk is an integral AML/CTF measures, and as such, should not be treated as a one-off exercise, but instead be embedded within working practices.

14.10 The process should be a continual and dynamic identification, assessment, management and review of risk and threats, outlined in the following diagram:



14.11 The improved risk-based approach adopted the risk management cycle in the following manner:

Identification

14.12 The identification of new inherent and emerging risks relating to money laundering and terrorist financing to the specific sectors within the gambling industry. Risks identified in this paper were gathered from a variety of sources, including: the industry, research led by in-house qualified professionals, findings from reported data, intelligence, licensing, compliance and enforcement casework, media sources, Government, regulatory partners, law enforcement agencies, European Commission and FATF; our identification of risk extends to both domestic and international evidence and best practice.

Assessment/ Evaluation

14.13 The evaluation process involved the assessment of the likelihood of those risks occurring and their impact, should they happen. This was conducted using the Commission's ML/TF Risk assessment matrix (ML/TF RAM) which can be found below. A moderation process, including review by qualified professionals, is utilised to evaluate the scores allocated to each risk, its likelihood of occurring and the impact should this occur.

Management

14.14 The management process was conducted through reviewing the previous risk assessment and reporting on the current status of the risks previously identified. Each of the risks have been assessed using information sources as referred to above in the assessment section. Secondly, new inherent risks identified during the time parameter of this report have been assessed using the same methodology. Lastly, new emerging risks within the time parameter of this report has also undergone assessment using consistent methodology.

Review & Report

14.15 This paper seeks to embed a culture of risk awareness throughout the gambling industry through:

- the regular collection of risk and the maintenance of risk profiles for the casino industry as required under the regulations

- directing the collection of risk factors and risk profiles to drive compliance intensity and frequency as required by the Regulations
- feeding into amending legal framework i.e. LCCP changes, based on revealed risk
- driving strategic focus for the AML team for example recent call for information relating to MSB or enforcement casework
- driving risk factors considered when considering licence applications
- developing intelligence understanding of financial crime in the UK associated with gambling
- driving the Commission's evidence reporting on an annual basis to HM Treasury through the annual supervisor's return
- improving the Commission's evidence base which shapes reporting to HM Treasury for their National Risk Assessment
- driving evidence reported to Home Office to contribute towards the UK Economic Crime Plan
- driving evidence provided to FATF during mutual evaluations and follow-up evaluation.

Gambling Commission's ML/TF Risk assessment matrix (ML/TF RAM)

ML/ TF Risk Assessment Matrix

Likelihood of risk occuring	Very Low (VL)	Low (L)	Medium (M)	High (H)	Very High (VH)
Very High (VH - 1): >80%	AMBER/RED 5	AMBER/RED 4	RED/RED 3	RED/RED 2	RED/RED 1
High (H - 2): 60%-80%	AMBER/AMBER 10	AMBER/AMBER 8	AMBER/RED 6	AMBER/RED 4	RED/RED 2
Medium (M - 3) 40%-60%	GREEN/AMBER 15	GREEN/AMBER 12	AMBER/AMBER 9	AMBER/RED 6	RED/RED 3
Low (L - 4): 20%-40%	GREEN/GREEN 20	GREEN/AMBER 16	GREEN/AMBER 12	AMBER/AMBER 8	AMBER/RED 4
Very Low (VL - 5): <20%	GREEN/GREEN 25	GREEN/GREEN 20	GREEN/AMBER 15	AMBER/AMBER 10	AMBER/RED 5
Type of vulnerability	Very Low (VL)	Low (L)	Medium (M)	High (H)	Very High (VH)

Impact of risk (for further detail – please below)

	Very Low (VL)	Low (L)	Medium (M)	High (H)	Very High (VH)
Operator Control Vulnerability	• Remote potential for terrorist financing exploitation. • Remote potential for criminal exploitation and detriment to society. • Little or no impact on business environment/ wider industry. • Little or no potential for compliance or legal violations, if occurs is minor and very limited in nature - Self-improvement review required. • Very little or no potential cost to implement AML/ CTF controls.	• Little potential for links to terrorist financing exploitation. • Little potential for criminal exploitation and detriment to society. • Some impact on business environment/ wider industry. • Potential for minor breaches that are easily addressed, may be short term or very little compliance action. • Potential cost (small, short term) to implement AML/CTF controls. • May result in 'low level' adverse media coverage - local mention only, quickly forgotten/ short term media	• Some potential for terrorist financing exploitation. • Some potential for criminal exploitation and detriment to society. • Impact on business environment/ wider industry. • Potential for breaches that are more difficult/ time consuming to address, may be long term or some compliance action needed. • Cost to implement AML/CTF controls anticipated to be 5-10% of operator's budget. • May result in some adverse media coverage - persistent national concern.	• Potential links to terrorist financing exploitation. • Potential links to criminal exploitation and detriment to society. • Increased threat to business environment/ wider industry. • Potential for breaches of a material nature that can lead to penalties, fines or sanctions which will need compliance action. • Cost to implement AML/CTF controls anticipated to be >10% of	• Significant potential for terrorist financing exploitation links. • Significant potential for criminal exploitation and detriment to society. • Major threat to business environment/ wider industry. • Potential for serious breaches that can lead to significant penalties, fines or sanctions which will need heavy compliance action. • Cost to implement AML/CTF controls anticipated to be >30% of operator's budget. • International concern, Governmental inquiry or sustained adverse national/international media. • Critical failure, operator's survival

	• None or very little potential for adverse media coverage. • The impact can be dealt with by routine operations.	concern. • Minimal impact on non-core operations.	• Increased impact on non-core operations, further negatively impacting consumers and may subject the operator to review.	operator's budget. • Persistent, intense national public, political and media scrutiny - long term 'brand' impact. • Major operations severely restricted, operator's existence is threatened, potentially harming consumers.	threats are imminent/ severe, harming consumers.
Customer Vulnerability	• Remote potential for terrorist financing exploitation. • Remote potential for criminal exploitation and detriment to society. • Little or no impact on business environment/ wider industry. • Little or no impact based on anonymity. • Very little or no potential cost to implement AML/ CTF controls. • None or very little potential for adverse media coverage. • The impact can be dealt with by routine operations.	• Little potential for links to terrorist financing exploitation. • Little potential for criminal exploitation and detriment to society. • Some impact on business environment/ wider industry. • Some impact based on anonymity. • Potential cost (small, short term) to implement AML/CTF controls. • May result in 'low level' adverse media coverage - local mention only, quickly forgotten/ short term media concern. • Minimal impact on non-core operations.	• Some potential for terrorist financing exploitation. • Some potential for criminal exploitation and detriment to society. • Impact on business environment/ wider industry. • Impact based on anonymity. • Cost to implement AML/CTF controls anticipated to be 5-10% of operator's budget. • May result in some adverse media coverage - persistent national concern. • Increased impact on non-core operations, further negatively impacting consumers and may subject the operator to review.	• Potential links to terrorist financing exploitation. • Potential links to criminal exploitation and detriment to society. • Increased threat to business environment/ wider industry. • ML concerns around anonymous nature of the payment. • Cost to implement AML/CTF controls anticipated to be >10% of operator's budget. • Persistent, intense national public, political and media scrutiny - long term 'brand' impact. • Major operations severely restricted, operator's existence is threatened, potentially harming consumers.	• Significant potential for terrorist financing exploitation links. • Significant potential for criminal exploitation and detriment to society. • Major threat to business environment/ wider industry. • Major ML concerns around anonymous nature of the payment. • Cost to implement AML/CTF controls anticipated to be >30% of operator's budget. • International concern, Governmental inquiry or sustained adverse national/international media. • Critical failure, operator's survival threats are imminent/ severe, harming consumers.
Licensing & Integrity Vulnerability	• Remote potential for terrorist financing exploitation. • Remote potential for criminal exploitation and	• Little potential for links to terrorist financing exploitation. • Little potential for criminal exploitation and detriment to society.	• Some potential for terrorist financing exploitation. • Some potential for criminal exploitation and detriment to society.	• Potential links to terrorist financing exploitation. • Potential links to criminal exploitation and	• Significant potential for terrorist financing exploitation links. • Significant potential for criminal exploitation and detriment to society.

	detriment to society. • Little or no impact on business environment/ wider industry. • Little or no potential for compliance or legal violations, if occurs is minor and very limited in nature. • Very little or no potential cost to implement AML/ CTF controls. • None or very little potential for adverse media coverage. • The impact can be dealt with by routine operations.	• Some impact on business environment/ wider industry. • Potential for minor breaches that are easily addressed or very little compliance action. • Potential cost to implement (small, short term) AML/CTF controls. • May result in 'low level' adverse media coverage - local mention only, quickly forgotten/ short term media concern. • Minimal impact on non-core operations.	• Impact on business environment/ wider industry. • Potential for breaches that are more difficult/ time consuming to address or some compliance action needed. • Cost to implement AML/CTF controls anticipated to be 5-10% of operator's budget. • Increased impact on non-core operations, further negatively impacting consumers and may subject the operator to review.	detriment to society. • Increased threat to business environment/ wider industry. • Potential for breaches of a material nature that can lead to penalties, fines or sanctions which will need compliance action. • Cost to implement AML/CTF controls anticipated to be >10% of operator's budget. • Persistent, intense national public, political and media scrutiny - long term 'brand' impact. • Major operations severely restricted, operator's existence is threatened, potentially harming consumers.	• Major threat to business environment/ wider industry. • Potential for serious breaches that can lead to significant penalties, fines or sanctions which will need heavy compliance action. • Cost to implement AML/CTF controls anticipated to be >30% of operator's budget. • International concern, Governmental inquiry or sustained adverse national/international media. • Critical failure, operator's survival threats are imminent/ severe, harming consumers.
Means of Payment Vulnerability	• Remote potential for terrorist financing exploitation. • Remote potential for criminal exploitation and detriment to society. • Little or no impact on business environment/ wider industry. • Little or no impact based on anonymity. • Very little or no potential cost to implement AML/ CTF controls. • None or very little potential for adverse media coverage.	• Little potential for links to terrorist financing exploitation. • Little potential for criminal exploitation. • Some impact on business environment/ wider industry. • Some impact based on anonymity. • Potential cost (small, short term) to implement AML/CTF controls. • May result in 'low level' adverse media coverage - local mention only, quickly forgotten/ short term media concern. • Minimal impact on non-core	• Some potential for terrorist financing exploitation. • Some potential for criminal exploitation and detriment to society. • Impact on business environment/ wider industry. • Impact based on anonymity. • Cost to implement AML/CTF controls anticipated to be 5-10% of operator's budget. • May result in some adverse media coverage - persistent national concern. • Increased impact on non-core operations, further negatively impacting consumers and may subject the	• Potential links to terrorist financing exploitation. • Potential links to criminal exploitation and detriment to society. • Increased threat to business environment/ wider industry. • ML concerns around anonymous nature of the payment. • Cost to implement AML/CTF controls anticipated to be >10% of operator's budget. • Persistent, intense	• Significant potential for terrorist financing exploitation links. • Significant potential for criminal exploitation and detriment to society. • Major threat to business environment/ wider industry. • Major ML concerns around anonymous nature of the payment. • Cost to implement AML/CTF controls anticipated to be >30% of operator's budget. • Critical failure, operator's survival threats are imminent/ severe, harming consumers.

	• The impact can be dealt with by routine operations.	operations.	operator to review.	national public, political and media scrutiny - long term 'brand' impact. • Major operations severely restricted, operator's existence is threatened, potentially harming consumers.	
Product Vulnerability	• Remote potential for terrorist financing exploitation. • Remote potential for criminal exploitation and detriment to society. • Little or no impact on business environment/ wider industry. • Little or no impact based on anonymity. • Very little or no potential cost to implement AML/ CTF controls. • None or very little potential for adverse media coverage. • The impact can be dealt with by routine operations.	• Little potential for links to terrorist financing exploitation. • Little potential for criminal exploitation and detriment to society. • Some impact on business environment/ wider industry. • Some impact based on anonymity. • Potential cost (small, short term) to implement AML/CTF controls. • May result in 'low level' adverse media coverage - local mention only, quickly forgotten/ short term media concern. • Minimal impact on non-core operations.	• Some potential for terrorist financing exploitation. • Some potential for criminal exploitation and detriment to society. • Impact on business environment/ wider industry. • Impact based on anonymity. • Cost to implement AML/CTF controls anticipated to be 5-10% of operator's budget. • May result in some adverse media coverage - persistent national concern. • Increased impact on non-core operations, further negatively impacting consumers and may subject the operator to review.	• Potential links to terrorist financing exploitation. • Potential links to criminal exploitation and detriment to society. • Increased threat to business environment/ wider industry. • ML concerns around anonymous nature of the payment. • Cost to implement AML/CTF controls anticipated to be >10% of operator's budget. • Persistent, intense national public, political and media scrutiny - long term 'brand' impact. • Major operations severely restricted, operator's existence is threatened, potentially harming consumers.	• Significant potential for terrorist financing exploitation links. • Significant potential for criminal exploitation and detriment to society. • Major threat to business environment/ wider industry. • Major ML concerns around anonymous nature of the payment. • Cost to implement AML/CTF controls anticipated to be >30% of operator's budget. • International concern, Governmental inquiry or sustained adverse national/international media. • Critical failure, operator's survival threats are imminent/ severe, harming consumers.

Keeping gambling fair and safe for all

www.gamblingcommission.gov.uk