GAMBLING COMMISSION

The money laundering and terrorist financing risks within the British gambling industry

December 2020

Contents

GAMBLING COMMISSION

1. Executive summary

1.1 The Gambling Commission's (the Commission) money laundering (ML) and terrorist financing (TF) risk assessment 2020 highlights the key risks associated with each of the sectors within licensed land-based and remote activity in Great Britain's gambling industry. This assessment builds on the previous one (including the ML and TF risks associated with COVID-19) and fulfils the Commission's requirement under Regulation 17 (1) of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) 2017 (the Regulations).

1.2 The purpose of this risk assessment is to:

1. act as a resource for the industry in informing their own ML and TF risk assessments;
2. to provide the Commission's support to HM Treasury's National Risk Assessment and the rating of low risk in the context of the wider regulated financial sector and advise HM Government on risks in the industry; and
3. inform and prioritise our licensing, compliance, and enforcement activity to raise standards in the industry and meet our duties under Regulation 46 (2)(c).

1.3 The Commission has considered a wealth of information and intelligence when assessing the key threats identified within the British gambling industry and providing revised risk ratings in this publication. 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 considered approaches taken by other AML supervisory authorities, such as the Financial Conduct Authority (FCA) and HM Revenue and Customs (HMRC). We have also analysed information from various other sources to inform our understanding of risks such as:

1. The EU Supranational Risk Assessment on Money Laundering and Terrorist Financing (SNRA);
2. HM Treasury's National Risk Assessment (NRA) of Money Laundering and Terrorist Financing 2020;
3. Financial Action Task Force (FATF) recommendations (the global standard setter on combating ML and TF);
4. FATF's Terrorist Financing Risk Assessment Guidance July 2019;
5. The Home Office July 2019 Asset Recovery Action Plan;
6. FATF's Mutual Evaluation Report (MER) of the UK's AML and CTF framework;
7. The UK government's Economic Crime Plan 2019;
8. The Anti-Corruption Strategy 2017;
9. The Serious and Organised Crime Strategy 2018; and
10. The UK's Anti-Money Laundering and Counter-Terrorist Financing Action Plan 2016.

1.4 The reporting period this assessment is based on is from 1st November 2018 to 31st May 2020. The methodology used to assess the risks in Great Britain's gambling industry remains the same as for the previous year's risk assessment. 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 as follows and range from high risk to low risk. The gambling sector, however, in HM Treasury's National Risk Assessment is rated as low, and it is important to understand why this is the rating allocated. The National Risk Assessment captures the risk of money laundering and terrorist financing occurring across all regulated financial sectors and Designated Non-Financial Businesses and Professionals (DNFBPs), which includes: Banks and Credit Institutions, Money Service Businesses, Legal services, High Value Dealers, Art, Accountancy, and many other regulated financial sectors. When gambling is put into the wider financial context of being vulnerable to money laundering and terrorist financing in comparison to other regulated sectors, the risk is lower; thereby explaining HM Treasury's rationale for rating gambling as low risk for ML and TF. However, the Commission in this risk assessment compares individual gambling sub-sector risks of being vulnerable to money laundering and terrorist financing and rates them appropriately in comparison to each other. Whilst some of the ratings have changed in individual sub-sector risk areas, the overall risk ratings for each gambling sector have not changed since the previous risk assessment (with the exception of the overall risk of terrorist financing to Great Britain's gambling industry which has decreased from medium to low risk).

1.6 The following gambling sectors are being assessed separately (compared to previous risk assessments) as they are separate and distinct sectors with differing risk areas and levels:

1. Remote Betting;
2. Remote Bingo;
3. The National Lottery (Remote and Non-Remote);
4. Society Lotteries and External Lottery Managers (Remote and Non-Remote);
5. Gambling Software (Remote and Non-Remote); and
6. Gaming Machine Technical (Remote and Non-Remote).

1.7 External Lottery Managers are being assessed for the first time.

Remote (Casino, Betting, and Bingo)	Casino (Non-Remote)	Betting (Non-Remote, off-course)	Betting (Non-Remote, on-course)	Bingo (Non-Remote)	Adult Gaming Centres	Family Entertainment Centres (FECs)	Society Lotteries and External Lottery Managers (Remote and Non-Remote)	The National Lottery (Remote and Non-Remote)	Gambling Software (Remote and Non-Remote)	Gaming Machine Technical (Remote and Non-Remote)
High	**High**	**High**	**Medium**	**Medium**	**Medium**	**Low**	**Low**	**Low**	**Low**	**Low**

Terrorist financing	Current overall risk rating
	Low

1.8 The assessment of the terrorist financing risk is partially based on information from HM Treasury's National Risk Assessment, which has assessed this area as low risk for gambling. The Commission has also collaborated closely with external stakeholders when arriving at its risk rating, such as the UK's counter terrorism teams, to help us understand the terrorist financing typologies and vulnerabilities that are applicable to the gambling industry.

1.9 This assessment recognises that there are many risks and typologies or *vulnerabilities* in the gambling industry related to ML or TF. The gambling industry is fast paced and is constantly evolving with new innovative products to cater for customer needs. However, with any changes, these can bring new methods for criminals to launder illicit funds which the gambling industry needs to be alert to.

1.10 This document is intended to act as a valuable resource for the industry in informing their own ML and TF risk assessments, and must be taken into account when doing so, as required under Licence Condition 12 of the Licence Conditions and Codes of Practice (LCCP) [1].

1.11 It is mandatory for gambling operators from all gambling sectors to comply with the licensing objective, keeping crime and its proceeds out of gambling as set out in the Gambling Act 2005 (the Act) and the Commission's 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) have an enhanced set of legal responsibilities, as they must comply with the Regulations [2] for casino gaming, gaming machines and money service business activities offered. However, it is imperative for all gambling operators (regardless of gambling sector) to ensure they have effective risk assessments identifying ML and TF risks, along with robust policies, procedures, and controls in place to prevent ML/TF and continue to raise standards in that regard.

[1] Licence Condition 12 requires operators have appropriate policies, procedures, and controls to prevent money laundering and terrorist financing and that such policies, procedures, and controls take into account any applicable learning or guidelines published by the Gambling Commission.

[2] This refers to the Regulations under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ('the Regulations') which are applicable to firms under the 'regulated sector'. Casinos are part of the 'regulated sector'.

2. Introduction

2.1 Regulation 17 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 and 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 and TF risks within that sector), 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 understanding the ML and 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 and 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 June 2019 we published our previous Money Laundering and Terrorist Financing Risk Assessment. The money laundering vulnerabilities in the previous assessment were evidence-based and achieved through analysis of a variety of information sources. Each assessment builds upon the previous one. It its therefore recommended that this year's assessment should be read in conjunction with the previous risk assessment as the previous publications provide further information on the inherent risks within Great Britain's gambling industry by sector.

2.5 This report is set out by firstly reviewing existing inherent and emerging risks, which the previous risk assessment highlighted. Then the report assesses any additionally applicable inherent and new emerging risks.

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

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

3.1 The risk of ML and TF threatens the United Kingdom's (UK) national security, the economy and international standing. Such risks can have a detrimental impact on society, can damage communities and undermines the integrity of both public and private sector organisations. The ML and TF threats that the gambling industry faces are diverse, complex and are rapidly 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.

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. There are various reasons as to why criminals or organised crime groups may engage in ML such as

a. financial trails from offences to criminals are incriminating evidence. They will try and obscure or hide the source of their wealth or funds, or alternatively disguise ownership or control to ensure that illicit proceeds are not used to associate them to a predicate offence.

b. proceeds of crimes can become the target of investigation and seizure. To protect the criminal and their illicit finances from seizure, they will try and conceal their existence or, alternatively, make them look legitimate.

3.4 If left unimpeded, this may result in:

1. significant potential for ML and TF exploitation;
2. significant potential for criminal exploitation and detriment to society;
3. a major threat to the business environment and wider industry;
4. potential for serious breaches that can lead to significant penalties, fines or sanctions which will need punitive outcomes;
5. cost to implement AML and CTF controls anticipated to be a significant percentage of an operator's budget;
6. international concern, resulting in governmental inquiry or sustained adverse national and international media; and
7. critical failure of gambling operations and businesses i.e., the survival of the operator is under imminent or severe threat, ultimately harming consumers and/ or negatively impacting the gambling industry.

4. Regulatory framework

The Gambling Act 2005 ('the Act') and the National Lottery 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 which requires that the National Lottery is (including every lottery that forms part of it) run with all due propriety, and 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 (which replaced the Money Laundering Regulations 2007). The Regulations require remote and non-remote casinos to, for example: identify the source of funds for customers and source of wealth and funds for Politically Exposed Persons; undertake ML and 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 and TF.

4.6 As part of the regulated sector, casinos licensed by the Commission are placed under an enhanced set of legal duties as set out under the Regulations. The Regulations were amended on 10th January 2020 because of the implementation of the 5th Money Laundering Directive into UK law, through the updated Money Laundering Regulation's Statutory Instrument. For further information on casino businesses' legal duties, please refer to our comprehensive casino guidance. Casino businesses are also reminded that they should have already reviewed and accordingly amended their ML and TF risk assessments as well as the associated policies, procedures, and controls because of the 5th Money Laundering Directive's implementation.

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

4.7 The risk of crime affects all gambling operators, including those not specified in the Regulations, and they too 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.

4.8 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 and TF. Licensees must also ensure they have appropriate policies, procedures, and controls to prevent ML and TF, taken into account in their 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.

Financial Action Task Force (FATF)

4.9 The Commission continues to base its framework for this and previous assessments upon FATF's risk assessment methodology. The Financial Action Task Force (FATF) 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 identified us as displaying *"…a very strong understanding of risks both at a sector and firm-specific level."*

The Sanctions and Anti-Money Laundering Act 2018

4.10 At the end of the EU Exit transition period, sanctions will continue to be implemented through the new powers as set out in the Sanctions and Anti-Money Laundering Act 2018 (SAMLA). This will be used to fulfil our international obligations under the UN and impose further sanctions domestically. SAMLA provides the power for the UK to impose sanctions, including against a person involved in gross human rights abuses or anti-corruption violations.

Risk based approach

4.11 A risk-based approach focuses effort where it is most needed and will have the most impact. It requires the full commitment and support of senior management and the active co-operation all employees.

4.12 A risk-based approach involves several steps to assess the most proportionate way to manage and mitigate the risks faced by an operator:

1. identifying the ML and TF risks relevant to the operator;
2. designing and implementing policies, procedures, and controls to manage and mitigate the risks;
3. monitoring and improving the effective operation of these controls; and
4. recording what has been done and why.

4.13 For further information regarding the steps gambling operators should take in applying a risk based approach, please see our guidance for casino operators and other operators.

5. COVID-19

5.1 The Commission has been issuing regular industry alerts to inform and educate the gambling industry regarding the emerging risks we have come across due to the current COVID-19 pandemic (including steps businesses should take to mitigate these risks). Please see here for further information.

6. Casino (Remote)

Remote Casino	Previous overall risk rating	Current overall risk rating
	High	High

Inherent risks

6.1 There has been an increase in the risk levels for the inherent risks for the remote casino sector. For further information relating to the inherent risks (including vulnerabilities, consequences and controls), please refer to the 2018 and 2017 publications of the Commission's risk assessment of the gambling industry.

	Vulnerability	Risk	Previous overall rating (likelihood: impact)	Likelihood of event occurring	Impact of event occurring	Movement
			Current rating			
Casino (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 funds	M:H	L	H	↓
	Licensing and integrity	White label providers	H	H	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:H	H	H	↑
	Customer	Accessibility to multiple remote casinos	H	H	H	↔
	Customer	Customers from high risk jurisdictions using casino facilities to launder criminal funds	L:VH	M	H	↔
	Customer	Customers who appear on sanctions lists laundering criminal funds	L:VH	L	H	↓
	Customer	International politically exposed persons (PEPs) using casinos to launder illicit or criminal funds	M:VH	M	H	↓
	Customer	Domestic PEPs using casinos to clean criminal funds identification & verification	M	L	M	↓
	Customer	Customers making numerous low-level transactions to minimise suspicion and evade CDD requirements at the	H	H	H	↔

		threshold (smurfing)				
	Customers	Use of third parties or agents to obscure the source or ownership of money gambled by customers & their identities	H	H	H	↔
	Means of payment	Pre-paid cards	M	H	H	↑
	Means of payment	E-wallets	M	M	M	↔
	Means of payment	Cryptoasset transactions	M	M	H	↑
	Product	Peer to Peer Gaming (poker)-B2B and B2C	H	H	H	↔

6.2 All of the following areas have been given a high risk rating which signifies the importance of operators carrying out robust due diligence checks on customers.

Additional inherent risks

Organised crime gangs (OCGs)

6.3 There is a significant risk of OCGs infiltrating remote casino businesses using 'mule accounts' (for example). This has been rated high risk.

Mule accounts

6.4 Illicit funds can be transferred (either willingly or unwillingly), through a third party's bank account (known as a 'money mule') to break the audit trail of transactions. This can be used as a primary method of laundering criminal proceeds. There is evidence that mule accounts have been used for gambling purposes with mainly vulnerable individuals or university students being targeted There is evidence that OCGs are using this method, with links to drug and people trafficking, to move large amounts of illicit proceeds through a dispersed network of accounts to ensure financial threshold triggers are not alerted.

6.5 The decrease of international students residing in the UK (due to COVID-19) may have led to reductions in activity through those types of mule accounts, however UK resident [3] students remain vulnerable. There is the risk that OCGs may coerce vulnerable individuals into becoming money mules, as has been observed in the US. This has been given a high risk rating due to both the likelihood and impact of it occurring within gambling and the high collateral impact upon victims. Linked to this risk area, please refer to the remote betting section below for information regarding 'mule' betting accounts.

High monetary thresholds

6.6 Through compliance and enforcement work the Commission carries out, we have seen numerous instances of operators imposing high financial triggers which need to be met before any customer interaction takes place. For example, one remote casino operator had a £3,500 'customer trigger' before any CDD checks would take place. By having high arbitrary financial thresholds in place before CDD or EDD (if required) checks are carried out, means that casino operators are failing to consider any ML and TF risks below these levels. These arbitrary thresholds will not allow the operator to consider any unusual patterns of transactions below these high thresholds (which requires increased monitoring of the business relationship) to determine whether the transaction or business relationship appears to be suspicious [4].

'High value' customer schemes

6.7 There is evidence to suggest that membership schemes provide incentives to high spending customers such as free holidays, bets, cashback, and prizes. Evidence suggests that 'VIP' or high value customers are more likely to be problem gamblers. Some 2.3% of the country's online 47,000 VIPs are estimated to be problem gamblers [5]. From a ML, TF, and problem gambling perspective this raises significant concerns regarding how adequately CDD or KYC checks are conducted by gambling businesses. Operators are repeatedly failing to understand that problem gambling may be interlinked with ML and TF risks in that if sufficient CDD/EDD [6] checks or KYC checks [7] are not undertaken, this is a breach of the Regulations [8], the LCCP and Commission guidance [9]. Problem gambling risk indicators include, but are not limited to:

1. chasing losses;
2. Reluctance to provide their occupation; and
3. spend that is inconsistent with the customer's apparent legitimate income.

6.8 The above is not the exhaustive list and casino operators need to satisfy themselves that they have asked the necessary questions when deciding whether to establish customer relationship, maintaining the relationship or if deciding to terminate the relationship. Further information on operators' legal duties can be found in our comprehensive guidance for casino and all other operators.

6.9 Potential mitigations that operators can implement in this area include setting deposit limits along with a clear risk assessment of this area and effective policies, procedures, and controls in place for high value customers (to include mandating regular, meaningful customer interaction with all high value customers).

---

[3] Gambling Commission data.
[4] As required under Regulation 33(4) of the Regulations.
[5] Gambling Commission data 2020.
[6] Applicable to casino operators only.
[7] Applicable to all other gambling sectors.
[8] Applicable to casino operators only.
[9] LCCP 12.1 (requires operators to conduct an assessment of the ML and TF risks posed in their business). Not applicable to gambling software and gaming machine technical licences.

6.10 The Commission has undertaken a consultation on high value customers, and released guidance in September 2020 setting out areas that gambling businesses must comply with to reduce harm and mitigate risks.

6.11 The Commission holds significant evidence of cases where problem gamblers have stolen monies to fund gambling activities (along with cases where those in positions of trust and high risk professions have fraudulently obtained money from employers or vulnerable victims for gambling purposes due to problems with gambling). Customers may also undertake non-traditional types of crimes such as 'lonely heart' scams to use money derived from this to gamble. These type of gambling typologies are increasing which makes it vital that operators undertake the necessary checks to establish a customer's source of funds and affordability levels to gamble.

6.12 SR code provision 3.4.1 of the LCCP sets out requirements for effective policies and procedures for customer interaction and indicators of problem gaming (including VIP or high-value customers). The Commission's Customer interaction – guidance for remote gambling operators Guidance note also clearly sets out our expectations in this area [10].

6.13 The Commission takes any breaches of social responsibility and AML/CTF provisions seriously. This is evidenced by our recent targeted investigation into online casinos where we have conducted licence reviews under s.116 of the Act and imposed regulatory settlements where we have seen evidence of non-compliance [11]. As part of our remote casino compliance and enforcement work, we have also reviewed 22 Personal Management Licences. This has been given an overall 'high' risk rating due to high customer spending levels and high levels of human collateral impact. The risk in this area also apply to all customer contact operators (casino, betting, bingo, arcade).

Failure to implement a 'closed loop' system

6.14 Where operators do not have a 'closed loop' system in place, there is a significant risk of criminals being able to exploit the use of fraudulent or stolen debit cards across multiple premises of the same operator with monies derived from the proceeds of crime. It is strongly recommended that payments are made to the same customer card to mitigate this risk. This has been given a high risk rating.

Emerging risks

Payment providers

6.15 Operators are reminded not to rely on payment providers to conduct KYC checks. Further information on this risk can be found on the Commission's website.

High-stakes gambling/Feature buy-in slots

6.16 These are online slot games which allow players to stake significant amounts of money to access a bonus feature without playing the initial stages of the game. There is significant concern about this bonus feature as it appears to encourage higher stake gambling with reports that players can stake £1000+ at a time to directly access bonus features. There

[10] Gambling Commission: Customer interaction-formal guidance for remote gambling operators: <www.gamblingcommission.gov.uk/PDF/Customer-Interaction-Formal-Guidance-Remote-July-2019.pdf> : see section 2.18 and section 4 of the guidance (accessed 23rd June 2020, updated July 2019)

[11] Gambling Commission: www.gamblingcommission.gov.uk/news-action-and-statistics/News/betway-to-pay-116m-for-failings-linked-to-vip-customers (accessed 11th August 2020, updated March 2020).

was evidence that one game was charging more than £3,000 to enter the bonus feature. As well as appearing to be potential breaches of the Remote Technical Standards (RTS) [12], it also raises concerns regarding how customer due diligence (CDD) checks (or if needed, EDD checks) are carried out to ensure compliance with the Regulations if customers are permitted to play for high stakes in short periods of time as online games are instantaneous and can encourage fast, addictive play. All high-stakes gambling is susceptible to abuse because it is common for players to gamble with large volumes of cash, the source and ultimate ownership of which may not be readily discernable.

6.17 The Commission regularly issues industry alerts so that operators are aware of the standards expected of them in relation to gambling law [13]. The Commission has actively pursued these operators so that these features are removed, and they subsequently have been. This area has been given a 'high' risk rating due to the significant ML and TF risks due to the high spending potential.

[12] RTS 14A (need to ensure that products are designed responsibly and to minimise the likelihood that they exploit or encourage problem gambling behaviour and RTS 3A: An explanation of the applicable rules must be easily available to the customer before they commit to gamble.

[13] 'Games warning for online operators': www.gamblingcommission.gov.uk/news-action-and-statistics/news/2020/Games-warning-for-online-operators.aspx (updated 17th January 2020, accessed 1st March 2020).

7. Casino (Non-Remote)

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

Existing inherent risk rating

7.1 There has been an increase in the risk levels for some of the inherent risks for the non-remote casino sector. For further information relating to the inherent risks (including vulnerabilities, consequences and controls), please refer to the 2018 and 2017 publications of the Commission's risk assessment of the gambling industry.

	Vulnerability	Risk	Previous overall rating (likelihood: impact)	Likelihood of event occurring	Impact of event occurring	Movement
				Current rating		
Casino (Non-Remote)	Operator Control	Operators failing to comply with prevention of money laundering and terrorist financing legislation and guidance	H	H	H	↔
	Operator Control	Undermining of the Money Laundering Reporting Officer (MLRO) role which can intentionally/unintentionally lead to exploitation by money launderers	H	H	H	↔
	Operator Control	Lack of competency of key personnel and licence holders which can then be exploited by criminals seeking to launder the proceeds of crime	L:H	H	H	↑
	Operator Control	Lack of adequate and relevant due diligence checks conducted resulting in criminals laundering money	M:H	H	H	↑
	Licensing & Integrity	Gambling operations being acquired by organised crime to	M:H	M	H	↔

		launder criminal proceeds				
	Licensing & Integrity	Ultimate Beneficial Ownership	M:H	M	H	↔
	Licensing & Integrity	Employees colluding with criminals	M:H	H	H	↑
	Licensing and integrity	Individuals with known criminal records/or suspected criminal activities	H	H	H	↔
	Customer	Customer from high-risk jurisdictions using casino facilities to launder money	M: VH	M	H	↓
	Customer	Customers appearing on international sanctions list laundering corrupt or criminal funds	M: VH	L	H	↓
	Customer	International politically exposed persons (PEPs) using casinos to clean criminal funds	H: VH	M	H	↓
	Customer	Domestic PEPs using casinos to clean criminal funds	M	L	M	↓
	Customer	False/fraudulently obtained or stolen ID docs used to bypass controls	M:H	M	H	↔
	Customer	Customers breaking up large amounts of cash into small transactions to minimise suspicion and evade CDD requirements at the threshold ('smurfing')	H	M	H	↓
	Customers	Use of third parties or agents to obscure the source or ownership of money gambled by customers & their identities	H	M	H	↓
	Means of Payment	Cash Transactions	H	H	H	↔
	Means of Payment	Casinos acting as money service businesses (MSBs)	H	H	H	↔
	Means of Payment	TITO enabled gaming machines used to launder funds when used with ATR machine	H	M	H	↓

	Product	Electronic roulette - when used with TITO & ATRs	H	M	H	↓
	Product	Gaming Machines (all)	H	H	H	↔
	Product	Peer to peer gaming (poker) B2C	H	H	H	↔

Additional inherent risks

Cashless payments

7.2 The use of cashless payments in general has increased in popularity in recent years. This presents a risk where ML or TF 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 employee's effective application and there is a monetary cap on each transaction (currently £45). The associated risks with cashless payment include:

1. operators failing to undertake KYC checks on customers;
2. transactions not being monitored in real time; and
3. 'smurfing': a common ML method where a customer will make numerous low level transactions to avoid suspicion.

7.3 The above risks associated with cashless payments further increase where a customer uses multiple premises and there is a lack of customer interaction. However due to cashless payments increasing in popularity (especially due to COVID-19), this has been given a high risk rating in relation to the casino sector.

Emerging risks

Cryptoasset payments

7.4 The Commission has become aware of instances of non-remote casinos accepting cryptoassets as a form of customer payment. Operators are reminded that their ML and TF risk assessment must be reviewed if certain circumstances change (including new methods of payment by customers) [14]. This has been rated medium risk as there is no widespread evidence of this specific risk area. For further information on this risk area, please see the Commission's website for further information.

Bank drafts

7.5 Bank drafts are being viewed as the latest ML method for criminals. These are guaranteed cheques issued by a bank and are being used as a form of customer payment by some remote casino operators. Cash payments have typically been favoured by criminals for money laundering purposes (this may be because criminal activities generate cash profits or because cash is used as an instrument to disguise the criminal origin of profits) as the benefits of this method include lack of traceability. There is a risk that there could be a shift from cash payments to bank drafts as a form of payment due to the following reasons:

[14] As required under Licence Condition 12.1.1 of the LCCP.

1. they are an inconspicuous payment method compared to carrying bulk cash in non-remote casinos; and

2. cash payments are viewed less favourably by criminals due to increased media and government intervention.

7.6 Other countries have recently seen a surge in the number of suspicious related casino transactions involving bank drafts and operational alerts regarding the money laundering risks of this have been issued. The alert includes evidence that bank drafts have been associated to 'mule bank accounts' (please see above for further information on 'mule accounts') [15]. In this regard, it is vital that gambling businesses are alert to customers who regularly use this as a payment method or deposit a high volume of bank drafts.

7.7 Licence Condition 5.1.1. of the LCCP mandates that there needs to be appropriate policies and procedures concerning the use of cash equivalents (including bank drafts). Furthermore, bank drafts can increase the risk of 'smurfing'.

7.8 The use of bank drafts has been given a medium risk rating as the Commission is not aware of widespread use by Commission licensed casino operators accepting bank drafts as a form of customer payment.

'Bring your own devices' (BYODs)

7.9 Recent product innovations in the gambling industry include cashless apps that can be used on analogue and digital machines. The advantages for customers include ease of play and convenience, however there are associated risks. These include:

1. operators failing to undertake KYC checks on customers.
2. transactions not being monitored in real time;
3. anonymity: customers could place bets without needing an account or interacting with employees of the operator; and
4. 'smurfing': a common ML method where a customer will make numerous low level transactions to avoid suspicion.

7.10 The above risks associated with cashless apps further increase where a customer uses multiple premises and there is a lack of customer interaction. The Commission is not aware of any licensed casino operator currently providing this facility. However due to cashless payments (along with digital payment methods) increasing in popularity due to continuing innovation in the industry (as well as the drive towards cashless payment due to COVID-19), this has been given a high risk rating should this be implemented in the future in relation to the casino sector.

Transfer of funds between casino customers

7.11 There is evidence that in the non-remote casino sector, customers can transfer funds between themselves via their gambling accounts. Operators should have policies, procedures, and controls in place to mitigate the risk of money lending between customers[16]. This has been rated medium risk .

---

[15] Financial Transactions and Reports Analysis Centre of Canada: '*Operational alert: Laundering the proceeds of crime through a casino-related underground banking scheme*': https://www.fintrac-canafe.gc.ca/intel/operation/casino-eng (accessed 25the February 2020, updated December 2019).

[16] Ordinary Code Provision 3.8.1 of the LCCP states that operators should take steps to prevent systematic or organised money lending between customers on their premises.

Unlicensed employees carrying out ID checks

7.12 There is growing evidence that non-licensed employees e.g., casino receptionists ((who are not required to hold Personal Licences under the LCCP) are carrying out customer ID checks. Casino operators are reminded that they are ultimately responsible for compliance with the LCCP, the Act and the Regulations. This is rated high risk.

Key person responsible for regulatory compliance

7.13 A requirement of the Regulations 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. This could be the same person as the nominated officer if the operator considers this a suitable arrangement [17]. The Commission has received evidence that some casino operators are not complying with this requirement and will view any non-compliance with the Regulations seriously. This has been rated as high risk.

8. Casinos offering money service businesses

8.1 The Regulation's designate the Commission as the supervisory authority for casinos in the UK. While under the Regulations HMRC is the supervisory authority for money service businesses (MSB) activities, the Commission and HMRC have agreed, under Regulation 7(2), 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 Commission found that around 14% of business to customer remote casinos offered some form of MSB activity. In the same period around 79% of non-remote casinos offered some form of MSB activity [18]. Commission-based research found that the following types of MSBs were offered by casinos:

8.2 33 casinos offered cheque cashing
54 casinos offered foreign currency exchange
35 offered third party money transfer
20 casinos offered all the above three types

8.3 Some red flag risk indicators identified with MSB activity were:

- Casino operators with weak KYC policies and/or implementation of those policies;
- Casino operators who demonstrate a lack of curiosity concerning customers' source of funds;
- Operators with a high turnover of staff, especially those working in Compliance teams, the Money Laundering Reporting Officer (MLRO) and staff of the MLRO's office;
- Operators with an MLRO, who is not a personal management licence holder with the Commission or professionally qualified (MLROs do not have to be PML holders, though we

[17] Regulation 21(1)(a).
[18] In the period between 1st January 2018 to 31st December 2018.

strongly advise this as it allows us to perform criminality, identity, integrity, and competency assessments on the individual);

- Operators who do not demonstrate a risk based approach to their interactions and checks relating to customers; and
- Customers from high risk jurisdictions using MSBs. Operators must be considering geographical risk in their risk assessments.

8.4 Example case study:

Third party payment MSB activity for online casinos might include cases of a spouse's card being used to fund the gambler's account, or the money is paid out from the account to the third party. Clearly there are risks associated with this and we expect operators to have measures in place such as identification and source of fund checks.

8.5 The Commission found that some remote casino operators were unable to separate their financial data accurately in relation to MSB activity and other activity in customers' e-wallets. Failing to do so means that operators are not sufficiently assessing, monitoring, and controlling the risks associated with MSB activity.

8.6 The above highlights the importance of operators adopting a risk-based approach in order mitigate the potential ML and TF risks associated with MSB activity.

9. Betting (Remote)

Betting (Remote)	Previous overall risk rating	Current overall risk rating
	High	High

Existing inherent risk rating

9.1 There has been an increase in the risk levels for several the inherent risks for the remote betting sector. For further information relating to the inherent risks (including vulnerabilities, consequences and controls), please refer to the 2018 and 2017 publications of the Commission's risk assessment of the gambling industry.

Betting (Remote)	Vulnerability	Risk	Previous overall rating (likelihood: impact)	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	L	M	↓
	Operator Control	Lack of competency of key personnel and licence holders which can then be exploited by criminals seeking to launder the proceeds of crime	H	H	H	↔
	Operator Control	Inadequate/lack of 'know your customer' (KYC) checks resulting in criminals laundering criminal proceeds or risk of this occurring	M:H	H	H	↑

	Licensing and integrity	Gambling operations run by organised criminals to launder criminally derived funds	M:H	M	H	↔
	Licensing and integrity	White label providers	H	H	H	↔
	Customer	Customer not physically present for identification	M:H	H	H	↑
	Customer	False or stolen documentation used to bypass controls to launder criminally derived funds	M:H	H	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	M: VH	H	H	↓
	Customer	Customers who appear on international sanctions lists laundering criminally derived funds	VL:H	L	H	↑
	Means of payment	E-wallets	N/A (no risk rating provided in previous risk assessment)	M	M	N/A
	Means of payment	Cryptoasset transactions	M	M	H	↑
	Means of payment	Pre-paid cards	M	H	H	↑

9.2 The below additional inherent and new emerging risks highlight the importance of operators conducting robust due diligence checks on customers. The new or additional areas have their own individual risk ratings below.

Additional inherent risks

Peer to peer betting

9.3 This method of gambling allows customers to bet directly against each other. There is the potential for betting sites to be used by criminals to facilitate match fixing and therefore generate criminal proceeds [19]. The risks in this area have been further compounded over recent years with the introduction of peer to peer betting applications which allows for instantaneous, convenient play. Betting exchanges are typically a global product meaning customers located within Great Britain can be matched with customers from different countries who may not be necessarily be subject to same, stringent AML checks as those in Britain. This means that criminal monies may be filtering into Britain. This risk in this area increases where a customer is from a high risk geographical area [20]. This has been given a medium risk rating.

'Closed loop' system

9.4 With COVID-19 seeing an increase in cashless payments, there is the risk of operators not operating a 'closed loop' system i.e., payment to the customer is made on the same card that was used by the customer to deposit funds. This coupled with the increased evidence the Commission is seeing of card fraud/theft means that operators should implement effective policies, procedures and controls involving a 'closed loop system'. This has been rated high risk.

Use of third parties or agents to obscure the source or ownership of money gambled by customers & their identities

9.5 There have been examples in the remote betting sector of customers' gambling being funded by third parties which has facilitated ML. This highlights the importance of operators having a robust ML and TF risk assessment in place to mitigate such risks. This has been given a high risk rating.

'High value' customer' schemes

9.6 This has been given a high risk rating as previously discussed. Please refer above for further information.

High monetary thresholds

9.7 There is substantial evidence that remote betting operators have high customer spending triggers in place before conducting any due diligence checks on customers. This means

[19] RUSI: Occasional paper: 'Play Your Cards Right: Preventing Criminal Abuse of Online Gambling': < www.rusi.org/sites/default/files/201911_op_rusi_playyourcardsright_moiseienko_web.pdf> (accessed 7th March 2020, updated November 2019). Author: Anton Moiseienko.

[20] For a list of high risk third countries please see: European Commission: 'EU policy on high-risk third countries': <ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terrorist-financing/eu-policy-high-risk-third-countries_en> (accessed 6th July 2020, updated May 2020).

that for customers that do not hit this threshold, it has been found that only basic checks are being carried out i.e., proof of name, address, and date of birth. Operators are reminded that this is a potential breach of Licence Condition 12.1.1.(1) which requires that licensees must assess the risks of their business being used for ML and TF. This is a high risk area.

Emerging risks

Unregulated betting events

9.8 The Commission has received reports from licenced operators relating to suspicious betting activity on sporting events taking place predominantly outside of Britain. A number of these events were organised as 'friendly' or 'exhibition' matches outside of the jurisdiction of a recognised Sports Governing Body (SGB). Media reports indicated that some of these events had been set up purely for betting purposes, with confusion over whether some of the matches had taken place at all. It is vital to maintain and protect the integrity of betting and with no SGB oversight, these unregulated events present a much greater risk for corruption and match fixing. We expect licensees to have robust systems in place to manage these risks. They should also ensure that markets are offered on events that are genuine and are settled fairly. This has been rated high risk. For further information, please see here.

Customer identity verification

9.9 Licence Condition 17 of the LCCP stipulates that online gambling businesses are not permitted to allow a customer to gamble before they have verified the customer's identity [21]. This LCCP change is consistent with our guidance to operators which states that operators need to give due consideration to '*whether it is necessary to do KYC or due diligence checks on the customer'* [22]. The Commission has seen evidence in the remote betting sector that licensees are asking for customer ID when a withdrawal request for winnings is submitted by the customer. From a ML perspective, this has been given an overall 'high' risk rating as it means that insufficient due diligence checks are being carried out early enough in the consumer's gambling journey.

'Smurfing'

9.10 There is evidence of customer 'smurfing' in the remote betting sector. 'Smurfing' is a common ML method where multiple launderers will make numerous small transactions to minimise suspicion and evade KYC requirements at the threshold of gambling. This has been given a medium risk rating.

'Mule' betting accounts

9.11 "Mule" accounts are the creation of online betting accounts via the misuse of personal details belonging to third parties. This can be done both with or without third-parties' knowledge and their personal data can be used to open both online betting accounts and e-wallet accounts with payment service providers. Large numbers of mule accounts are

[21] Except for low frequency or subscription lotteries, gaming machine technical, gambling software, host, ancillary remote casino and ancillary remote bingo.

[22] duties-and-responsibilities-under-the-proceeds-of-crime-act-2002, updated October 2020, accessed December 2020

typically controlled by individuals or groups for the purposes of placing large volumes of bets and/or to disguise who is placing the bets and/or disguise the sources of funds being gambled.

Third-party or “mule” accounts could arguably be used by the following groups to name but a few:

1. Bonus abusers;
2. Affiliate commission agents;
3. Professional gamblers/Betting syndicates/Courtsiders/Arbitrage bettors;
4. Problem gamblers;
5. Money launderers (including organised criminal groups: OCGs); and
6. Match fixers.

It is a well-known gambling typology that OCGs have targeted students and the vulnerable for setting up mule accounts.

Mule accounts can be used to:

1. to facilitate **money laundering** (i.e., enabling criminal groups to spread large amounts of money over numerous accounts on relatively low-risk bets);

2. to monetise **match-fixing** (getting as much money on as possible [via mule accounts] to capitalise on the knowledge of known sporting outcomes); and

3. to support **pro-gambling** (i.e., courtsiders providing fast data feeds and the use of mule accounts by savvy gamblers to capitalise on this knowledge).

The following are some red flag indicators for the use of mule betting accounts:

Case example 1:

- An 85-year-old female opening a new betting account at 3am (placing large or max bets on obscure markets relating to a third-tier South American basketball match). Large deposits and withdrawals are made via online payment providers. This can lead to a possible suspicion that the customer details may have been subject to ID theft.

Case example 2:

- During a house search, Police identify a carrier bag of approximately 7000 pre-paid payment cards. A dip sample of 200 of the cards identifies all are registered in different people’s names. A review of the transactions identifies all have been used to fund online gambling activity (not known at this stage whether sports betting or another online games/casino). It is suspected that large volume of personal data is likely to have been harvested, via unknown means, for the purpose of opening multiple betting accounts.

Case example 3:

- Multiple betting accounts in different names identified placing suspicious bets on sporting outcomes. The betting on all accounts is linked to the same device and IP address with all accounts appearing to be related to university students. It is suspected that students’ details may have been used or purchased, in some cases with their knowledge, to facilitate large-scale online betting.

Other ‘red-flag’ indicators that operators should be aware of include (but not limited to):

1. newly opened accounts with a third party payment set-up;
2. first and only bets placed using the accounts on this fixture;

3. using total funds deposited to place the bets;
4. disguising the main bet by creating an accumulator with short odds selection; and
5. taking an early cash-out before the settlement and (attempted to) withdraw their funds.

9.12 Whilst the above relates to betting accounts, it is easy to see how some of the above examples could also equally apply to the other remote sectors (casino, bingo). This has been given a high risk rating.

Politically exposed persons (PEP)

9.13 There is evidence in the remote betting sector of insufficient controls in place to identify PEPs, which is concerning as they can present (although not always) a higher risk of ML. A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold. Due to the risks associated with PEPs, the FATF recommendations require the application of additional AML/CTF measures to business relationships with PEPs [23]. These requirements are preventive (not criminal) in nature and should not be interpreted as meaning that all PEPs are involved in criminal activity. Operators are required to have effective controls in place to manage high risk customers and this should form part of their ML and TF risk assessment. Suggested mitigations in this area include (but are not limited to) operators comparing new and existing customers against PEP databases and sanctions lists. Currently there is limited evidence of the risk of PEPs using remote betting facilities to launder funds and has been given a medium risk rating.

[23] FATF Guidance: Politically exposed persons (Recommendations 12 and 22) www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf (accessed 11th August 2020, updated June 2013).

10. Betting (Non-Remote)

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

Off-course	High	High
On-course	Medium	Medium

Existing inherent risk rating

10.1 There has been an increase in the risk levels for some of the inherent risks for the non-remote betting sector. For further information relating to the inherent risks (including vulnerabilities, consequences and controls), please refer to the 2018 and 2017 publications of the Commission's risk assessment of the gambling industry.

Betting (Non-Remote)	Vulnerability	Risk	Previous overall rating (likelihood: impact)	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 **(off-course only)**	H	H	H	↔
	Operator Control	Operators failing to comply with prevention of money laundering and terrorist financing legislation and guidance **(on-course only)**	H	M	M	↓
	Operator Control	Lack of effective customer interaction resulting in a failure to prevent/detect ML	M:H	M	H	↔

		or TF **(off course only)**				
	Operator Control	Lack of effective customer interaction resulting in a failure to prevent/detect ML or TF **(on course only)**	M:H	M	M	↓
	Operator Control	Inadequate/lack of 'know your customer' (KYC) checks resulting in criminals laundering criminal proceeds **(off course only)**	M:H	H	H	↑
	Operator Control	Inadequate/lack of 'know your customer' (KYC) checks resulting in criminals laundering criminal proceeds **(on course only)**	M:H	M	M	↓
	Licensing & Integrity	Betting operations being acquired by organised crime to launder criminal proceeds **(off course only)**	M:H	L	H	↓
	Licensing & Integrity	Betting operations being acquired by organised crime to launder criminal proceeds **(on course only)**	M:H	L	H	↓
	Licensing & Integrity	Betting employees acting in collusion with organised criminals to launder criminal funds **(off course only)**	M:H	M	H	↔
	Licensing and Integrity	Betting employees acting in collusion with organised criminals to launder criminal funds **(on course only)**	M:H	L	M	↓
	Customers	Unverified customers laundering proceeds of crime through betting **(off-course only)**	H	H	H	↔

	Customers	Unverified customers laundering proceeds of crime through betting **(on-course only)**	H	M	M	↓
	Customer	Accessibility to multiple premises/operators **(off-course only)**	H	H	H	↔
	Customer	False or stolen identification documentation used to bypass controls to launder criminal funds **(off-course only)**	M	M	M	↔
	Product	Gaming machines used to launder criminal funds **(off course only)**	H	H	H	↔
	Product	Self Service Betting Terminals and Ticket-in-Ticket Out Machines used to launder criminal funds **(off-course only)**	H	M	H	↓
	Means of Payment	Cash Transactions	H	H	H	↔
	Means of Payment	Cashless Transactions	M	M	M	↔

Additional inherent risks

Dyed notes

10.2 There have been reported instances that betting shops have noticed dyed notes in gaming machines. It is vital that operators remain vigilant in this area. The Commission has recently issued an industry alert to operators to report this to the relevant local police force (through non-emergency contact options) where they have found dyed notes on their premises. At the same time, it is a mandatory requirement that operator's submit suspicious activity reports (SARs) to the National Crime Agency (NCA) in all cases where they have knowledge or suspicion of money laundering or terrorist financing where dyed bank notes are detected. This has been given an overall 'medium' risk rating.

New emerging risks

'Closed loop' system

10.3 As discussed earlier in this document, the pandemic has seen an increase in cashless payments. There is the risk of non-remote operators not operating a 'closed loop' system i.e., payment to the customer is made on the same card that was used by the customer to deposit funds. This coupled with the increased evidence the Commission is seeing of card fraud/theft means that operators should implement effective policies, procedures and controls involving a 'closed loop system'. Whilst there is a limit placed on contactless transactions (currently maximum of £45), there is also the risk of 'smurfing'. This has been given a high risk rating.

Organised Criminal Gangs (OCGs)

10.4 There is a risk that OCGs are using multiple land based betting premises to place bets with funds that have been derived from the proceeds of crime. Operators are reminded to remain vigilant and report any such matters to the police as well as submit SARs to the UKFIU where there is knowledge or suspicion of ML (including criminal spend) or TF. This has been given a medium risk rating.

Unlicensed gambling activities

10.5 There is the risk of on-course bookmakers providing gambling facilities that they are not licensed to provide i.e., accepting bets over the phone without having the required ancillary betting licence. Operators are reminded that where the Commission finds evidence of non-licensed activities, we will undertake compliance and enforcement action which might then lead to a review of the licence and possible revocation under s.116 of the Act. This has been given a low risk rating.

Scottish notes

10.6 The Commission has become aware of instances in this time-period where betting customers have tried to provide large quantities of Scottish notes to place their bets, which have well established ML vulnerabilities. Operators must remain vigilant in identification of customers depositing large quantities of Scottish notes, and if suspicious report their concerns to law enforcement and the UKFIU [24]. This has been given a medium risk rating.

Existing emerging risks

'Bring your own devices' (BYODs)

10.7 There is the technology available for customers to use their own device (e.g., mobile phone) to place bets through non-account based play either in off-course or on-course venues. Recent product innovations include cashless apps that can be used on analogue and digital machines. The advantages for customers include ease of play and convenience, however there are associated risks. These include:

[24] NB: large numbers of Scottish notes have been known to be linked to cash seizures in drug investigations.

1. operators failing to undertake KYC checks on customers;
2. transactions not being monitored in real time;
3. anonymity: customers could place bets without needing an account or interacting with employees of the operator; and
4. 'smurfing': a common ML method where a customer will make numerous low level transactions with the proceeds of crime to avoid suspicion.

10.8 The above risks associated with cashless apps further increase where a customer uses multiple land based premises and there is a lack of customer interaction. The Commission currently understands that licensed betting operator are not providing this facility, therefore our below risk rating must be taken account of should operators choose to offer this facility. Due to cashless payments (along with digital payment methods) increasing in popularity and due to continuing innovation in the industry (as well as the drive towards cashless payment due to COVID-19), this has been given a theoretical high risk rating in relation to the betting sector and will be kept under review through this publication.

11. Bingo (Remote)

Bingo (remote)	Previous overall risk rating	Current overall risk rating
	High	High

11.1 The remote bingo and betting sector will be assessed separately for the purposes of this publication as the risks differ for both sectors.

Existing inherent risks

11.2 There has been an increase in the risk levels for some of the inherent risks for the remote bingo sector. For further information relating to the inherent risks (including vulnerabilities, consequences and controls), please refer to the 2018 and 2017 publications of the Commission's risk assessment of the gambling industry.

	Vulnerability	Risk	Previous overall rating (likelihood: impact)	Likelihood of event occurring	Impact of event occurring	Movement
				Current rating		
Bingo (Remote)	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	L	M	↓
	Licensing and integrity	Gambling operations run by organised criminals to launder criminally derived funds	M:H	L	H	↓
	Customer	Customer not physically present for identification	M:H	H	H	↑
	Customer	False or stolen documentation used to bypass controls to launder criminally derived funds	M:H	M	H	↔
	Customer	Accessibility to multiple remote accounts	H	H	H	↔
	Means of payment	Cryptoasset transactions	M	M	H	↑
	Means of payment	Pre-paid cards	M	H	H	↑
	Means of payment	E-wallets	N/A (no risk rating provided in previous risk assessment)	M	M	N/A

11.3 The below additional inherent and new emerging risks all highlight the importance of operators conducting sufficient due diligence checks on customers and have all been given a high risk rating due to potential for significant monies to be laundered online.

Additional inherent risks

Poor source of funds checks

11.4 There is evidence of instances where customers have used stolen or fraudulently obtained money for gambling with remote bingo operators. Operators need to ensure that they have robust policies and procedures in place to establish source of funds. This has been given a high risk rating.

Smurfing

11.5 'Smurfing' is a common ML method where money launderers break up large amounts of illicit money into smaller transactions to evade suspicion. There is evidence that this has been occurring in the remote bingo sector and has been given a high risk rating due to the potential monies that can be laundered if due diligence checks are not carried out by operators. This has been given a high risk rating.

Customers on the sanctions list

11.6 The Commission has become aware of isolated instances where remote bingo operators have had customers that have been on a sanctions list, although the sanctioned individual did not deposit monies. Operators must be vigilant in identifying customers who appear on relevant sanction lists and if breaches have occurred report this to the Commission and the Office of Financial Sanctions Implementation (OFSI), they must prevent financial transactions and report suspicions of ML or TF to the UKFIU. This has been rated as low risk.

Inadequate/lack of 'know your customer' (KYC) checks

11.7 There is evidence that remote bingo operators are failing to undertake sufficient KYC checks which can result in operators accepting illicit funds. Failure to undertake adequate affordability checks, including knowledge of customers' occupations and delayed identification checks, i.e., at the point of withdrawing winnings, all contribute towards illicit finance washing through gambling accounts online. This is viewed as a high risk area.

New emerging risks

Use of third parties or agents to obscure the source or ownership of money gambled by customers & their identities

11.8 There have been examples in the remote bingo sector of customers' gambling being funded by third parties which has facilitated ML. This highlights the importance of operators having a robust ML and TF risk assessment in place to mitigate such risks. This has been given a medium risk rating.

12. Bingo (Non-Remote)

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

Existing inherent risk ratings

12.1 There has been some change in the risk levels for the inherent risks for the non-remote bingo sector. For further information relating to the previous inherent risks (including vulnerabilities, consequences and controls), please refer to the 2018 and 2017 publications of the Commission's risk assessment of the gambling industry.

Bingo (Non-Remote)	Vulnerability	Risk	Previous overall rating (likelihood: impact)	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	↔
	Operator Control	Removal of membership schemes	M	L	M	↓
	Operator Control	Lack of or inadequate 'know your customer' (KYC) checks conducted resulting in criminals laundering criminal proceeds	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	L	M	↓
	Means of Payment	Ticket-in-ticket-out (TITO) facilities used to launder funds when used in conjunction with ATR machines	M	M	M	↔
	Product	Electronic Betting Terminals (EBTs) incl. table-top gaming (either traditionally or via EBT content)	L:M	L	M	↔
	Product	Gaming Machines, Cat B3	M	L	M	↓

Additional inherent risks

Cash payments

12.2 Cash is globally recognised as being attractive for money launderers because of its anonymity, being difficult to trace and it is easily transferrable. The Financial Action Task Force (FATF) recognises that cash is widely used in the criminal economy [25]. The vulnerability associated with cash transactions include; criminal lifestyle spending, use of Scottish and Irish notes, and fraudulent notes and coins. However, the shift to cashless payment due to COVID-19 mitigates the risks associated with cash payments to a certain extent. This has been given a medium risk rating in relation to the non-remote bingo sector [26].

Cashless payment

12.3 As discussed previously, the use of cashless payments in general has increased in popularity in recent years. This presents a risk where ML 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 employee's effective application and there is a monetary cap on each transaction (currently £45). The associated risks with cashless payment include:

1. operators failing to undertake KYC checks on customers;
2. transactions not being monitored in real time; and
3. 'smurfing': a common ML method where a customer will make numerous low level transactions to avoid suspicion.

12.4 The above risks associated with cashless payments further increase where a customer uses multiple premises and there is a lack of customer interaction. Due to cashless payments increasing in popularity (especially due to COVID-19), this has been given a medium risk rating in relation to the non-remote bingo sector.

[25] FATF Report, 'Money Laundering through the physical transportation of cash': www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf (accessed 27th July 2020, updated October 2015).

[26] Licence Condition 5.1.1. of the LCCP (cash handling) places AML obligations on operators around the use of cash and cash equivalents by customers designed to minimise the risk of crimes such as money laundering.

13. Arcades

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

Existing inherent risk ratings

13.1 There has been some change in the risk levels for the inherent risks for the arcade sector. For further information relating to the inherent risks (including vulnerabilities, consequences and controls), please refer to the 2018 and 2017 publications of the Commission's risk assessment of the gambling industry.

Arcades	Vulnerability	Risk	Previous overall rating (likelihood: impact)	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	L	M	↓
	Licensing & Integrity	Arcade businesses being acquired by organised crime to launder criminal proceeds **(AGCs only)**	L:M	L	M	↔
	Licensing & Integrity	Arcade businesses being acquired by organised crime to launder criminal proceeds **(FECs only)**	L:M	L	L	↓

	Operator Control	Lack of competency of key personnel and licence holders which can then be exploited by criminals seeking to launder the proceeds of crime **(AGCs only)**	L:M	L	M	↔
	Operator Control	Lack of competency of key personnel and licence holders which can then be exploited by criminals seeking to launder the proceeds of crime **(FECs only)**	L:M	L	M	↔
	Customer	Anonymous customers laundering proceeds of crime through gaming machines **(AGCs only)**	M	M	M	↔
	Customers	Anonymous customers laundering proceeds of crime through gaming machines **(FECs only)**	M	L	L	↓
	Product	Automated ticket redemption (ATR) machines used to facilitate the laundering of criminally derived funds **(AGCs only)**	M	L	M	↓

	Product	Gaming machines, category B3 being used to launder criminally derived funds **(AGCs only)**	M	M	M	↔
	Product	Privacy booths **(AGCs only**)	M	M	M	↔
	Product	Privacy booths **(FECs only)**	M	M	L	↓
	Means of Payment	Cash transactions	M	L	M	↓
	Means of Payment	Cashless payments	N/A (no rating provided in previous Risk Assessment)	M	M	N/A
	Means of Payment	Ticket-in-ticket-out (TITO) facilities used to launder funds when used in conjunction with ATR machines **(AGCs only)**	M	L	M	↓

Additional inherent risks

Dyed notes

13.2 As mentioned previously, there have been reported instances where AGCs have noticed dyed bank notes in gaming machines. As well as the importance of reporting any dyed notes found on premises to the relevant local police force, it is also a mandatory requirement to submit suspicious activity reports (SARs) to the UKFIU in all cases where there is knowledge or suspicion of ML or TF in relation to any dyed bank notes detected. This has been given a 'medium' risk rating.

New emerging risks

'Bring your own devices' (BYODs)

13.3 Recent product innovations in the gambling industry include cashless apps that can be used on analogue and digital machines. The advantages for customers include ease of play and convenience, however there are associated risks. These include:

1. operators failing to undertake KYC checks on customers;
2. transactions not being monitored in real time;
3. anonymity: customers could gamble without needing an account or interacting with employees of the operator;
4. 'smurfing': a common ML method where a customer will make numerous low level transactions with illicit monies to avoid suspicion.

13.4 The above risks associated with cashless apps further increase where a customer uses multiple premises and there is a lack of customer interaction. The Commission sees cashless payments (along with digital payment methods) increasing in popularity due to continuing innovation in the industry (as well as the drive towards cashless payment due to COVID-19). This has been given a medium risk rating in relation to the arcade sector.

14. Society Lotteries and External Lottery Managers (Remote and Non-Remote)

Society Lotteries (Remote and Non-Remote)	Previous overall risk rating	Current overall risk rating
	Low	Low
External Lottery Managers (Remote and Non-Remote)	N/A: Not assessed previously	Low

14.1 Society lotteries and The National Lottery are being assessed separately for the purposes of this publication as they are two separate sectors and the risks posed in both differ. External Lottery Managers (ELMs) are being assessed for the first time as part of this risk assessment.

Existing inherent risk rating

14.2 The inherent risk ratings have changed for this assessment. For further information relating to the inherent risks (including vulnerabilities, consequences and controls), please refer to the 2018 publication of the Commission's risk assessment of the gambling industry.

Society Lotteries and ELMs (Remote and Non-Remote)	Vulnerability	Risk	Previous overall rating (likelihood: impact)	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	M	L	↑
	Licensing and integrity	Operator being acquired by organised crime to launder criminal funds	L:M	L	L	↓
	Customer	Anonymous customers **(non-remote)**	M:VL	L	VL	↓
	Customer	False and stolen identity documentation	L	L	L	↔

	Customer	Customer not physically present **(remote only)**	L	L	L	↔
	Products	Scratch cards/interactive instant win games	L:VL	L	VL	↔
	Means of Payment	Cash transactions **(non-remote only)**	L:M	L	L	↓

14.3 NB: previous overall risk ratings and the section in the table above relating to 'movement' are not applicable to ELMs as this is the first time this sector is being assessed separately.

New emerging risks (applicable to ELM sector only)

Failure to transfer lottery proceeds

14.4 ELMs make arrangement for a lottery on behalf of a society. The potential ML/TF risks are that lottery proceeds might not be passed on by the ELM to the society lottery they are working on behalf of, however some of these risks are partially mitigated as ELMs are required to be licensed by the Commission and by the scrutiny the society will implement for lottery proceeds between itself and the ELM. As there is no widespread evidence of this occurring, this has been given an overall low risk rating with a further update to be provided in the next risk assessment.

15. National Lottery (Remote and Non-Remote)

National Lottery	Previous overall risk rating	Current overall risk rating
	Low	Low

15.1 For this publication, The National Lottery and society lotteries have been assessed separately.

Existing inherent risk rating

15.2 There have been a few changes to the inherent risk ratings this year for the National Lottery. For further information relating to the inherent risks (including vulnerabilities, consequences and controls), please refer to the 2018 publication of the Commission's risk assessment of the gambling industry.

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

New emerging risks

KYC checks

15.3 There is a risk of insufficient KYC checks being carried out on high spending customers which could potentially breach the requirement for Camelot to guard against excessive customer play, however due to limited evidence this has been given a low risk rating.

16. Gambling Software (Remote and Non-Remote)

Gambling Software (Remote and Non-Remote)	Previous overall risk rating	Current overall risk rating
	Low	Low

16.1 The gambling software and gaming machine technical sectors have been assessed separately for this document as they are two separate gambling sectors.

Existing inherent risk rating

16.2 For further information relating to the inherent risks (including vulnerabilities, consequences, and controls), please refer to the 2018 publication of the Commission's risk assessment of the gambling industry.

	Vulnerability	Risk	Previous overall rating	Likelihood of event occurring	Impact of event occurring	Movement
				Current rating		
Gambling Software (Remote and Non-Remote)	Operator Control	Operators failing to comply with prevention of money laundering and terrorist financing legislation and guidance	L	L	L	↔
	Operator Control	Inadequate/lack of due diligence checks on any third party providers (e.g., test houses	N/A (no risk rating provided in previous risk assessment)	M	L	N/A

16.3 There are no emerging or additional inherent risks for this sector.

17. Gaming Machine Technical (Remote and Non-Remote)

Gaming Machine Technical (Remote and Non-Remote)	Previous overall risk rating	Current overall risk rating
	Low	Low

Existing inherent risk rating

17.1 As explained above, the gambling software and gaming machine technical sectors have been assessed separately for this document as they are two separate gambling sectors.

17.2 For further information on the inherent risks (including consequences and controls), please refer to the 2018 publication of the Commission's risk assessment of the gambling industry.

	Vulnerability	Risk	Previous overall rating	Likelihood of event occurring	Impact of event occurring	Movement
				Current rating		
Gaming Machine Technical (Remote and Non-Remote)	Operator Control	Operators failing to comply with prevention of money laundering and terrorist financing legislation and guidance	L	L	L	↔
	Product	Gaming machines Cat B, C and D, 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	↔
	Means of Payment	Cashless payments	N/A (no risk rating provided in previous risk assessment)	M	L	N/A

	Operator Control	Inadequate/lack of due diligence checks on any third-party providers (e.g., test houses)	N/A (no risk rating provided in previous risk assessment)	M	L	N/A

New emerging risks

Lack of adherence with Technical Standards

17.3 All gaming machine technical licensees are required to comply with the Commission's Technical Standards [27]. The purpose of these Standards is to set out in detail the Commission's requirements with respect to game features, display notices and general machine operation. These have been developed to help ensure the three licensing objectives under the Act are met (which includes 'keeping crime out of gambling'). The Technical Standards state that gaming machines must have an ID plate permanently attached (which must include the manufacturer's details) [28]. There is evidence that some gaming machines are being supplied without any ID plates attached to them which raises ML and TF concerns as there is no verified information regarding where these machines originated from i.e., if they have been purchased from the proceeds of crime. This has been given a low risk rating as there is no current widespread evidence of this practice.

[27] See Licence Condition 2.3.1. of the LCCP.

[28] See Para 1.2 ('Machine identification') of the Technical Standards.

18.Terrorist financing in gambling

Terrorist financing	Previous overall risk rating	Current overall risk rating
	Medium	Low

Existing inherent risks

18.1 This year's risk assessment builds upon the previous one relating to the current terrorist financing vulnerabilities the gambling industry faces.

18.2 There is a change in the overall risk rating relating to terrorist financing in Great Britain's gambling industry. This is due to evidence the Commission is aware of to support the change in risk levels (including HM Treasury's National Risk Assessment which was published in December 2020).

18.3 For further information on the inherent risks (including consequences and controls), please refer to the 2018 publication of the Commission's risk assessment of the gambling industry.

	Vulnerability	Risk	Sector	Previous overall rating (likelihood: impact)	Likelihood of event occurring	Impact of event occurring	Movement
					Current rating		
All sectors	Operator Control	Operators failing to understand or take consideration of terrorist financing vulnerabilities and applicable legislation	All	L:H	L	M	↓

Additional inherent risks

18.4 The risk levels and typologies relating to terrorist financing differ in comparison to ML. For this reason, even though some of the below risks (such as pre-paid cards and cryptoasset transactions) are high for ML purposes, they have been rated lower in relation to TF.

18.5 As discussed previously, criminals and terrorists have changed the way they operate to take advantage of the vulnerabilities that have emerged as a result of COVID-19. The current situation has seen an increase in the use of pre-paid cards, mule accounts and cryptoassets being used for ML purposes. For further information, please see the

Commission's website. However, these risks can be transferrable in relation to TF and the United Nations has warned that terrorist groups may see opportunities for increased TF activity while government attention is focused on COVID-19 [29]. However, the known risks within the UK for gambling and TF remains low as demonstrated within HM Treasury's current National Risk Assessment 2020.

Cash transactions

18.6 It is well known that terrorist financers use mechanisms such as bulk cash smuggling to move money [30]. Even though the pandemic has seen a restriction in cash movements, it is still vital that gambling businesses remain curious and be alert to large cash transactions. This has been rated low risk currently.

Money Service Businesses

18.7 It has been recognised that terrorist financers have used different channels to move funds and assets including money service businesses (MSBs) [31]. However, due to current limited evidence levels for this typology in gambling this has been given a low risk rating.

Pre-paid cards

18.8 'Smurfing' (using pre-paid cards) has been known to be used to fund terrorist activities. Here OCGs and those supporting terrorism can employ people ('smurfs') to purchase pre-paid cards which are then loaded with illicit money. Such money can then be legalised through transfer to a bank account. The 'smurfs' are careful to deal with amounts below the legal monetary thresholds. This money can then be used to fund terrorism and other legitimate activities, for example gambling. Due to current limited evidence levels this has been given an overall low risk rating.

'Mule' accounts

18.9 Illicit funds can be transferred (either willingly or unwillingly), through a third party's bank account (known as a 'money mule') to break the audit trail of transactions. This can be used as a primary method of laundering criminal proceeds. As previously discussed, the pandemic has seen an increase in mule account activity with criminals seeking to recruit money mules through social media to launder cash from human trafficking, terrorist financing or drug dealing. The Commission has become aware of instances where money from mule accounts have been used for gambling purposes. Whilst this has been given a high risk rating in relation to ML (where criminals have then laundered money through gambling activities), there is limited current evidence that mule account gambling activities have been used for TF purposes. Therefore, this has been given a low risk rating.

---

[29] United Nation's Secretary-General: Secretary-General's remarks to the Security Council on the Covid-19 Pandemic: <www.un.org/sg/en/content/sg/statement/2020-04-09/secretary-generals-remarks-the-security-council-the-covid-19-pandemic-delivered> (accessed 5th July 2020, updated 9th April 2020).

[30] OECD (2019), 'Money Laundering and Terrorist Financing Awareness handbook for Tax Examiners and Tax Auditors, OECD, Paris < www.oecd.org/tax/crime/money-laundering-and-terrorist-financing-awareness-handbook-for-tax-examiners-and-tax-auditors.pdf> (accessed 5th July 2020, updated 2019).

[31] FATF Report: Terrorist Financing Risk Assessment Guidance (July 2019): <www.fatf-gafi.org/media/fatf/documents/reports/Terrorist-Financing-Risk-Assessment-Guidance.pdf> (accessed 5th July 2020, updated July 2019).

Cryptoasset transactions

18.10 There is evidence that some terrorist groups use cryptoassets for funding purposes [32]. This digital currency is likely to be used due to lack of options for cashing out funds in or near conflict locations and the anonymity this product supports individuals or groups [33]. Before the pandemic, there were reports of terrorist groups increasingly using cryptoassets for funding purposes. The pandemic has also reported increases in the use of cryptoasset transactions in South Asia to fund terrorist-related activity. Whilst there is currently limited evidence that the use of cryptoassets for terrorist financing purposes in the UK is widespread, gambling businesses are reminded not to be complacent in fulfilling their legal duties to report suspicion or knowledge of terrorist financing to the UKFIU under the Terrorism Act 2000.

Charities and terrorist financing

18.11 The abuse of charities for terrorist financing is a well-known methodology and can occur in the following ways [34]:

1. abusing charity assets;
2. infiltration by members of terrorist groups within organisations;
3. cash and asset exchange within conflict zones from the charity;
4. misusing a charity name and status;
5. setting up a charity for an illegal or improper purpose; and
6. inappropriate expressions of support by a trustee for a proscribed terrorist organisation or designated person or entity.

18.12 Lotteries are often associated with charities and may share board structures, aims and employees, they therefore need to ensure that they have strong governance arrangements, financial controls and risk management policies and procedures in place that fit their needs, and will better safeguard them against a range of potential abuse, including the financing of terrorism. Trustees must also consider and manage risks to the lotteries (whether operational, financial, or reputational) ensuring they exercise proper control over financial affairs and keeping accurate records. Trustees must also ensure they and their charity comply with the law, including counter-terrorist financing law. Due to current evidence levels in this area for gambling, it has been given an overall low risk rating.

18.13 All of the above risk areas relating to terrorist financing highlights the importance of operators ensuring they conduct sufficient KYC checks along with SAR submissions where there is knowledge or suspicion of terrorist financing and submitting Defence Against Terrorist Financing SARs (DATF) if operators suspect they have received, kept, or transferred monetary sums associated with terrorism.

---

[32] FATF (2018), 'Financing of Recruitment for Terrorist Financing Purposes': <www.fatf-gafi.org/publications/methodsandtrends/documents/financing-recruitment-terrorist-purposes.html> (updated January 2018, accessed March 2nd, 2020).

[33] Tom Keatinge, David Carlisle, Florence Keen: 'Virtual currencies and terrorist financing: assessing the risks and evaluating responses': www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf (updated June 4th 2018, accessed March 2nd, 2020).

[34] The Charity Commission for Northern Ireland: 'Controlling against terrorist financing and money laundering': <www.charitycommissionni.org.uk/charity-essentials/controlling-against-terrorist-financing-and-money-laundering/> (accessed 27th April 2020, updated 2014).

Domestic and international terrorism

(a) Increase in right wing terrorism

18.14 There is a growing threat of right-wing extremism in the UK [35]. It has been reported that out of the six terror plots foiled by the UK intelligence agencies in 2019, half involved those on the far-right wing of extremism. It has been reported that far-right extremists are building international funding networks including funding from high risk geographical areas, which makes it even more vital for gambling businesses to ensure that they conduct sufficient checks on the origin of customer funds upon deposit and withdrawal and identify their customers.

(b) International terrorism

18.15 International terrorism remains a dominant threat in the UK. However, there is limited current evidence that funding is entering the UK from hostile locations for attack planning (page 44 paragraph 5.9 HM Treasury's National Risk Assessment 2020).

18.16 Both of the above risk areas (right wing and international terrorism) have been given a low risk rating in relation to their impact on the gambling industry due to evidence levels.

Terrorism 'red flag' indicators

18.17 Some potential 'red flag' indicators that operators should be alert to, based on evidence reviewed regarding the risk of TF are:

1. a customer's income or expenditure which is inconsistent with their occupation;
2. unusual or suspicious religious quotes, or single words/phrases relating to known terrorist ideology or known numerical associations to terrorism in financial transactions and customer details (social media 'handle,' web chat, email addresses etc);
3. use of multiple foreign bank accounts to conduct transactions;
4. unexpected large withdrawals or complete withdrawal of sums and sudden account closure;
5. transactions are structured to avoid internal threshold or SAR reporting ('smurfing');
6. MSB usage, including indicators such as: multiple overseas geographical locations destination for transfers, use of third parties in the transaction chain, open loop for foreign exchange transactions i.e., deposits in one currency and requests to withdraw in a different currency and missing details on money transfers;
7. accounts linked to pre-paid cards;
8. customer IP address being used by other customers.

[35] Gov.uk: 'Factsheet: right-wing terrorism < homeofficemedia.blog.gov.uk/2019/09/20/fact-sheet-right-wing-terrorism/ > (accessed 5th July 2020, updated 20th September 2019).

19. Methodology

19.1 As per our last published risk assessment 2018**,** the methodology we have adopted to analyse the risks in the gambling industry remains the same. The methodology uses an approach that can be represented as **likelihood X impact = risk rating. Please refer to our previous risk assessment for further information about our methodology.**

December 2020