GAMBLING COMMISSION

Money laundering and terrorist financing risk within the British gambling industry

Risk assessment

November 2017

Contents

1 Executive summary

1.1 The Gambling Commission's money laundering and terrorist financing risk assessment 2017 highlights the core risks associated with each of the sectors within Great Britain's (GB) licensed gambling industry.

1.2 The purpose of this risk assessment is to:

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

1.3 This assessment has been developed in consultation with sector and industry specialists. The Commission has liaised with law enforcement, including the National Crime Agency (NCA), and considered approaches taken by other AML supervisory authorities, such as the Financial Conduct Authority (FCA). The Commission also considers HM Treasury's National Risk Assessment (NRA) of money laundering and terrorist financing 2017 when assessing the key threats posed by the risks identified in the GB gambling industry.

1.4 In summary, the risk ratings for each gambling sector are as follows. Note that the overall risk ratings have not changed since the previous risk assessment, published in March 2017:

Arcades (non-remote)	Betting (non-remote)	Bingo (non-remote)	Casinos (non-remote)	Gaming machines (remote and non-remote)	Lotteries (remote and non-remote)	Remote (casinos, betting and bingo)
Medium	Higher	Medium	Higher	Lower	Lower	Higher

1.5 The gambling industry is not immune to ML/TF. It is highly segmented, with a wide range of operators based both domestically and overseas, offering diverse products, in different environments, to different types of customers, with various payment methods. Criminals are increasingly looking for alternative ways to launder criminal proceeds and the gambling industry needs to be alert to this.

1.6 This assessment is a key tool in ensuring that the Commission is focussing its resource and expertise on the highest risk areas of ML/TF in the GB gambling market. We expect all operators to have an awareness of the vulnerabilities, controls and consequences associated with the ML/TF risks in gambling. This document is intended to act as a valuable resource for the industry in informing their own ML/TF risk assessments.

1.8 It is imperative that gambling operators comply with the requirements of the Gambling Act 2005 (the Act) and the Licence Conditions and Codes of Practice (LCCP) to ensure that they have effective policies, procedures and controls in place to prevent ML/TF, and continue to raise standards in that regard.

2 Introduction

2.1 A risk assessment is widely seen as the foundation of any system to manage and prevent ML/TF. By knowing and understanding the risks to which the gambling industry is exposed, HM Government, law enforcement, the Commission and operators can work together to ensure that gambling in GB is a hostile place for money launderers and terrorist financers seeking to exploit it.

2.2 In March 2017, we published our previous Money Laundering and Terrorist Financing Risk Assessment. This identified a number of money laundering vulnerabilities and drew on a wide range of information sources to develop a clear evidence-based understanding. This edition of the risk assessment builds on the previous one and seeks to again highlight key areas of risk within the GB gambling industry by sector.

2.3 In transposing the EU 4th Money Laundering Directive (the Directive), HM Government decided to utilise powers provided to member states to exempt gambling sectors which are lower risk in comparison to the wider financial system, for example retail banking, with the exception of non-remote and remote casinos, which could not be exempted.

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

2.5 The Government recognises that the risk levels attributed to a particular gambling sector are not static and will vary over time. As a result, where a gambling sector can no longer be deemed low risk (including where the sector fails to effectively manage the ML/TF risks), then it will likely lead to their inclusion within the provisions of the Regulations, subjecting that sector to its requirements.

3 Regulatory framework

3.1 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[1]. The National Lottery Act requires that that the National Lottery is run and every lottery that forms part of it, is promoted with all due propriety, and that the interests of every participant in a lottery that forms part of the National Lottery are protected. ML/TF are criminal activities in GB.

3.2 The Proceeds of Crime Act 2002 (POCA) places a further obligation on 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.

3.3 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.

[1] Section 1(a) of the Act.

3.4 The Commission has based its framework for this and the previous assessment on FATF's risk assessment methodology. For the next iteration of the assessment, the Commission will continue to use FATF's framework and also develop bespoke methodologies specific to gambling, to provide additional information on sector specific risks and threats to operators, consumers and Government.

3.5 The Regulations came into effect on 26 June 2017. These replaced the Money Laundering Regulations 2007. The Regulations require remote and non-remote casinos to, for example, undertake ML/TF risk assessments, conduct due diligence checks, establish policies, procedures and controls, and provide employee training to mitigate the risks of ML/TF. The Regulations designate the Commission as the supervisory authority for casinos in GB. While, under the Regulations, HM Revenue and Customs (HMRC) is the supervisory authority for Money Service Businesses (MSB) activities, the Commission and HMRC have agreed, under regulation 7(2) of the Regulations, which the Commission acts as the supervisory authority for MSB activities carried on by casinos.

3.6 The risk of crime, however, affects all gambling operators, including those in the non-regulated sector, and they are required to have regard to POCA and TACT, and adopt a risk-based approach consistent with the Commission's Licence Conditions and Codes of Practice (LCCP), guidance and advice.

3.7 Licence condition 12.1.1 requires all operating licensees (with the exception of gaming machines technical and gambling software licensees) to conduct an assessment of the risks of their businesses being used for ML/TF. Licensees must also ensure they have appropriate policies, procedures and controls to prevent ML/TF having regard for 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 take into account any applicable learning or guidelines published by the Commission from time to time.

4 Money laundering and terrorist financing threat

4.1 The ML/TF threats that the gambling industry face are varied, complex and evolving rapidly. ML/TF threatens the UK's national security, economic prosperity and international standing. If left unimpeded, it damages communities and undermines the integrity of both public and private sector organisations. On an international level, ML/TF threatens security and stability, as well as harming the UK's ability to conduct business around the world.

4.2 The best available estimate of the amount of money laundering globally is equivalent to 2.7% of global GDP or US$1.6 trillion (in 2009).[2] The National Crime Agency (the NCA) says, in their 2017 National Strategic Assessment, that previous domestic estimates of *"GBP of 36 billion to GBP 90 billion for all money laundering impacting on the UK are a significant underestimate".* The Home Office has estimated the domestic social and economic cost of organised crime in the UK to be at least £24 billion per year.[3] It is clear from these estimates that the risk of ML/TF to the UK economy, GB gambling market and UK consumers are significant.

4.3 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, domestically and abroad. There is evidence of terrorist financing in the UK financial sector and of terrorist financing posing a significant threat to the UK's national security.[4]

[2] 'Estimating illicit financial flows resulting from drug trafficking and other transnational organised crimes: Research report', UNODC, October 2011.
[3] 'Understanding organised crime: estimating the scale and the social and economic costs', Home Office, October 2013
[4] 'UK national risk assessment of ML/TF', HM Treasury and Home Office, October 2017.

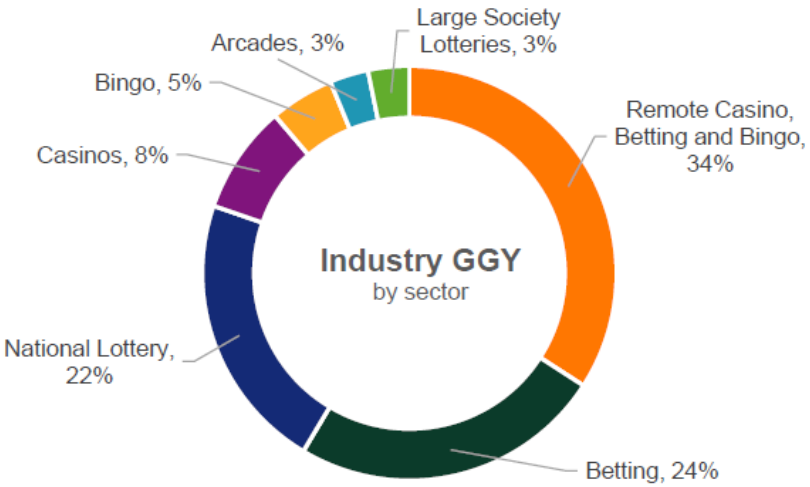
ML/TF in gambling

4.4 The gambling industry is not immune to ML/TF. It is highly segmented, with a wide range of operators based both domestically and overseas, offering diverse products, in different environments, to different types of customers, with various payment methods. Criminals are increasingly looking for alternative ways to launder criminal proceeds, and the gambling industry needs to be alert to this. Furthermore, it is accepted that a significant proportion of the ML/TF that takes place within the gambling industry is by criminals spending the proceeds of their crimes as a leisure activity and predominantly using cash, as advised by the Treasury in their recent NRA publication (for example, for gambling purposes rather than the traditional 'washing' of criminal funds).

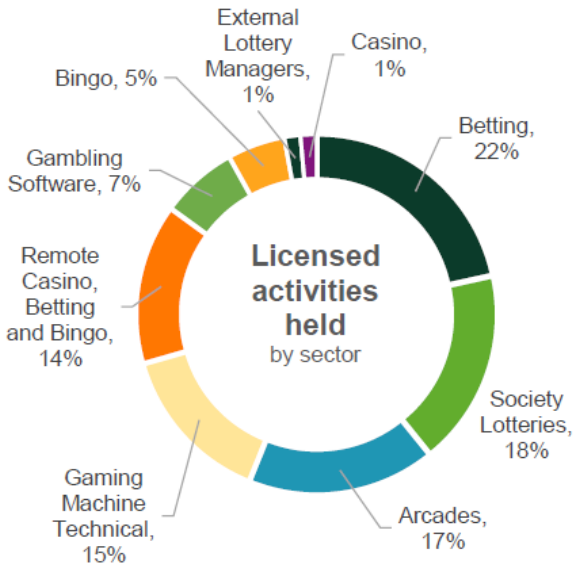
5 Industry overview

5.1 The Commission publishes industry statistics which provide an overview and analysis of the GB gambling industry. The summary below covers the period up to March 2017.

5.2 Between April 2016 and March 2017, the regulated GB gambling industry generated a gross gambling yield (GGY) or equivalent of £13.8bn, an increase of 2% on the previous year. The breakdown by sector was:



5.3 On 31 March 2017, there were a total of 2,788 operators licenced by the Commission, 357 of which operate across more than one sector. Those operators held licences that entitled them to conduct 3,685 activities, a 1.4% decrease on the previous period. The breakdown by sector was:



Arcades

Vulnerabilities	Controls
Arcade operators failing to comply with the Act, POCA, TACT, licence conditions and ordinary codes of practice preventing ML/TF This vulnerability relates to arcade operators failing to apply controls to mitigate the risk of ML/TF It is important to also recognise the following control risk which has emerged in the arcade sector[5] and until further assessment of the control risk it has been rated medium risk: Privacy booth is a concept being introduced to premises where gaming machines are available for play. Its concept is to afford the player additional privacy by way of screens or pods, this however, may cause a reduction in supervision by employees of the customers, as they are clearly being afforded additional privacy. Licence condition 9.1 states '*Facilities for gambling must only be offered in a manner which provides for appropriate supervision of those facilities by staff at all times'.* Affording additional privacy to customers may reduce the supervision by employees in respect of preventing money laundering and criminal lifestyle spending. A further update regarding this risk will be provided in the next published assessment	• The limited size of stakes, goes some way to mitigate the risk of 'traditional' money laundering within the sector, such as 'washing' criminally derived funds. This sector is more likely to be vulnerable to criminal lifestyle spending and 'smurfing'[6] • Controls within the sector largely rely on staff supervision and face-to-face interactions with customers • Loyalty schemes have the potential to increase operators knowledge about their customers and assist in the detection of money laundering • CCTV and automated system triggers assist in the identification and reporting of suspicious behaviour by customers enabling operators to report to law enforcement • Implementation of the Act, POCA, TACT and LCCP policies, procedures and controls are designed to mitigate the risk of money laundering and employees are trained to report incidents to their employer • Facial recognition software assists in capturing information that could assist law enforcement in their investigations

Consequences

- Arcade operators fail to comply with the Act, POCA, TACT and the LCCP through poor policies, poor risk assessment procedures, monitoring, training, embedding published learning and risk assessment, resulting in non-compliance
- Where weak controls exist, customer, product and means of payment vulnerabilities are all interlinked and exploited by a launderer
- There is continued evidence of laundering by criminal lifestyle spending due to the anonymised business model used by the sector
- Poor controls provide opportunities for money laundering of small stakes through this sector to occur, mainly criminal spend and / or 'smurfing'
- Controls within the sector are largely reactive, with limited real time data to trigger employee intervention

Risk rating

Arcade operators failing to comply with the Act, POCA, TACT, LCCP requirements and guidance: **Medium**

[5] This emerging control risk is applicable to non-remote betting, bingo and casino
[6] Customers' breaking up large amounts of cash into smaller transactions in order to minimise suspicion and evade threshold reporting requirements

Licensing and integrity vulnerabilities in the arcade sector

Vulnerabilities	Controls
Arcade operators acquired by criminals as a means to launder funds	• The Commission's suitability assessment reviews new and current licensees on a range of factors to ensure the activities are carried out in a way that minimises the risks to the licensing objectives • The Commission independently assures itself that its controls are robust • The Commission receives and shares intelligence with law enforcement agencies which has the potential to identify individuals associated with criminal activity
Consequences	
• Limited evidence of this vulnerability being realised • The Commission has robust controls and any attempts to date have been successfully prevented • There is no evidence to suggest arcades are being run as ML/TF vehicles by organised crime	
Risk rating	
Arcade operators acquired by criminals as a means to launder funds: **Medium**	

Customer vulnerabilities in the arcade sector

Vulnerabilities	Controls
Anonymous customers laundering or spending the proceeds of crime	• Arcades must comply with the Act, POCA and TACT and should take into account the Commission's advice on POCA, as required under section 2.1 of the LCCP • Licence condition 12.1.1 places obligations on operators to assess ML/TF risks to their business and implement suitable policies and procedures to mitigate any risks • Automated systems allow operators to flag suspicious activity and patterns of play • Alerts, triggers and similar technologies have the potential to mitigate the risk through machine products, effective staff intervention to act on and determine whether an alert is valid or not can prevent money laundering • Due to a regular customer base, inland AGCs provide an increased ability for staff to intervene and carry out know your customer (KYC) checks • Motorway service station premises are, at times, able to provide significant information to assist law enforcement due to the number of reactive controls available. For example, the use of TITO vouchers in conjunction with CCTV, or triggers and alerts to suspicious gaming patterns of play • All major service station operators use automatic number plate recognition systems, which adds to their ability to follow up on criminal activity and provide valuable intelligence to law enforcement • In FECs the low value of deposits as well as the different types of returns are a control (e.g. Low value prizes rather than money)
Consequences	
• Use of controls within the AGC sector are largely reactive in nature • It is internationally recognised that anonymity is a key enabler of money laundering, and the arcades sector has an anonymised business model • Growing availability of ATR machines within the sector has the potential to change the risk rating attributed to this vulnerability in future, due to an increased level of anonymity being provided by a reduction in face to face interaction with employees	
Risk rating	
Arcade operators acquired by criminals as a means to launder funds: **Medium** No evidence is available for FECs and limited evidence is available for AGC premises being used to launder criminal monies or used for terrorist financing. Based on this, a medium level of impact and likelihood has been allocated to the arcades sector for this threat. Individually assessed FECs receive a rating of **lower** based on the size and nature of the sector.	

Product vulnerabilities in the arcade sector

Vulnerabilities	Controls
Gaming machines, category B3[7] being used to launder criminally derived funds (excluding FECs)[8] Automated ticket redemption (ATR) machines used to facilitate the laundering of criminally derived funds (excluding FECs)[9]	• Arcade operators must comply with POCA and TACT assess and have in place suitable policies and procedures to manage ML/TF risk as prescribed under LC12.1.1 risk assessment • Number plate recognition systems, the use of CCTV and TITO tickets providing the ability to follow up on criminal activity and assist law enforcement • Automated systems can allow for successful flagging of suspicious activity and, when used in conjunction with CCTV, can be used to identify customers suspected of money laundering • TITO offers the opportunity to identify suspicious activity (including insertion of large amounts of money with little or no play, and subsequent presentation and redemption of the ticket value over the counter) using data derived from game play, in conjunction with CCTV, may assist in identification of suspicious behaviour • Some machines will reject dye stained notes, as well as fraudulent notes and coins.
Consequences	
• In the absence of human intervention, the controls have the potential to be exploited by a money launderer • Inconsistent use of standards for machine triggers and flags within the sector offer opportunities to money launderers	
Risk rating	
Gaming machines, category B3[10] being used to launder criminally derived funds: **Medium.** There is evidence of gaming machines in the AGC sector being used to spend criminally derived funds. Also, there is evidence that ATR machines have been used to facilitate the laundering of criminally derived funds: **Medium** Individually assessed FECs receive a rating of **lower** based on the size and nature of the sector.	

Means of payment vulnerabilities in the arcade sector

Vulnerabilities	Controls
• TITO used in conjunction with ATR machines (excluding FECs) • Cash transactions	• Licence condition 5.1.1 – cash handling places AML obligations on operators for the use of cash and cash equivalents by customers designed to minimise the risk of crimes such as money laundering • Some machines within the sector will reject dye stained notes, and fraudulent notes and coins • Controls are largely in relation to machine triggers and alerts to possible suspicious activity prompting staff intervention • Inland AGCs provide a greater ability for staff to intervene and carry out KYC • Motorway service stations are, at times, able to provide significant information to assist law enforcement due to the number of reactive controls available. For example, the use of TITO vouchers in conjunction with CCTV or triggers and alerts to suspicious gaming patterns of play • In FECs the low value of deposits as well as the different types of returns are controls (e.g. low value prizes rather than money).

[7] A gaming machine with a maximum stake of £2 and a maximum price of £500
[8] This vulnerability is compounded by TITO technology and when used in conjunction with Automated Ticket Redemption (ATR) machines
[9] This vulnerability largely applies to motorway service station AGCs
[10] A gaming machine with a maximum stake of £2 and a maximum price of £500

Consequences	
• There is evidence that vulnerabilities relating to TITO and ATR machines are being exploited within the sector • Anonymity of customers compounds these vulnerabilities as there is an incomplete audit trail, which reduces the risk to criminals	
Risk rating	
TITO used in conjunction with ATR machines (excluding FECs): **Medium** Cash transactions: **Medium** This is based on the medium impact and likelihood of the vulnerabilities being exploited in the sector with the evidence and intelligence known about TITO and ATR machines.	

Betting

Betting (non-remote)	Overall rating
	Higher

Off-course	Higher
On-course	Lower

Control vulnerabilities in the non-remote betting sector

Vulnerabilities	Controls
Betting operators failing to comply with the Act, POCA, TACT, LCCP and guidance This vulnerability relates to betting operators failing to apply controls to mitigate the risk of ML/TF	• The limited size of stakes goes some way to mitigating the risk of 'traditional' money laundering within the sector, such as 'washing' criminally derived funds • Controls within the sector largely rely on staff supervision and face-to-face interactions with customers • Loyalty schemes have the potential to increase operators' knowledge of their customers and assist in the detection and prevention of money laundering • CCTV and automated triggers assist in identification and reporting of suspicious behaviour by operators to law enforcement • The Act, POCA, TACT and LCCP policies, procedures and controls are designed to mitigate the risk of ML/TF, and employees are trained to report suspicions to their employer.

Consequences

- Non-remote betting operators fail to comply with the Act, POCA, TACT, and LCCP through poor policies, procedures and controls, monitoring, training, failure to embed published learning and ineffective risk assessment, resulting in non-compliance. The Commission will take action where it identifies non-compliance, this may range from action plans through to the review and/or revocation of personal and/or operating licences. Failure to follow good practice, as advised by the Commission in published guidance under ordinary code 2.1.2, will be a material factor in any action we take when considering the review and/or revocation of personal and/or operating licences

- Stake size is usually centrally controlled by operators for commercial reasons. Evidence held shows decisions to accept bets are made so as to control the operators' liabilities, but there is a lack of knowledge of the customers' source of funds and wealth

- Continued evidence of money laundering through criminal lifestyle spending prevails in non-remote betting, due to the anonymised business model used by the sector

- Failure by employees to follow their employers' policies and procedures intended to mitigate money laundering has resulted in criminal lifestyle spending continuing in the sector

- Decline in the use of loyalty schemes increases the anonymity of customers in the sector, which provides opportunities for criminals to spend their criminal funds

- Reporting of suspicious behaviour triggered by automated systems and/or observed behaviour is delayed, either due to limited employee knowledge of the customer or by employees being too intimidated to report suspicions about local criminals

- Senior management decision makers with oversight of data and suspicion are not effectively identifying criminal lifestyle spending within their estate.

Risk rating

The Commission has evidence of the continued laundering of criminally derived monies in this sector, however, it has no evidence of terrorist financing. Non-remote betting operators are failing to comply with the Act, POCA, TACT and LCCP requirements: **Higher**

Licensing and integrity vulnerabilities in the betting sector

Vulnerabilities	Controls
• Betting operators acquired by criminals as a means to launder criminal funds • Betting employees colluding with criminals to launder criminal funds	• The Commission assesses the suitability of new and current licensees against a range of factors to ensure the activities they are likely to carry out are done so in a way that minimises the risks to the licensing objectives • The Commission independently assures itself that its controls for the licensing of entities and individuals are robust • The Commission receives and shares intelligence with law enforcement agencies which provides the potential to identify individuals associated with criminal activity • The Commission has a role in licensing individuals in qualifying positions, which involves fit and proper checks • In instances where there are concerns about staff integrity (for non-licensed employees), a betting operator will take action where appropriate • Monitoring of customers and their transactions by operators goes some way to mitigating some of the risks associated with this vulnerability • Licensed individuals are subject to both general and individual licence conditions under sections 75 and 77 of the Act (monitoring ongoing suitability). Should concerns about staff integrity arise, the Commission will take proportionate action, up to and including reviewing and revoking personal licences.
Consequences	
• The vulnerability of non-remote betting operations being run by organised criminals has materialised, to the extent that attempts appear to have been made by organised criminals to acquire gambling businesses • The Commission has robust controls and any attempts by criminals to obtain licences have been successfully prevented to date • There is no current evidence that non-remote betting operators are being run as a ML/TF vehicles by organised criminal gangs • Integrity of both licensed and non-licensed staff employed within this sector has, at times, been called into question. Properly applied controls by operators can mitigate the risk of collusion by employees.	
Risk rating	
Non-remote betting operators acquired by criminals as a means to launder funds: **Medium-to-higher** Betting employees colluding with criminals to launder criminally derived funds: **Medium-to-higher**	

Customer vulnerabilities in the betting sector

Vulnerabilities	Controls
• Anonymous customers laundering or spending the proceeds of crime • Accessibility of multiple premises/operators (off-course only) • False or stolen identity documentation used to bypass controls in order to launder criminally derived funds • Access to online wallets over the counter for the deposit or withdrawal of funds	• Betting operators must comply with the Act, POCA, TACT and LCCP, and should take into account the Commission's advice on POCA as prescribed under section 2.1 of the codes of practice. • Licence condition 12.1.1 places obligations on operators to assess ML/TF risks to their business and implement appropriate policies and procedures to mitigate the identified risks • Loyalty schemes can remove elements of the anonymity of the customer and potentially mitigate vulnerabilities for the operator • Automated systems allow operators to flag suspicious activity and patterns of play, and provide information to law enforcement • Alerts, triggers and similar methods have the potential to mitigate risks associated with machine products, it relies upon effective staff intervention to act on and determine whether an alert is valid or not and report it to their employer for further investigation • CCTV and TITO, when used in conjunction, can provide a reactive control to assist law enforcement investigations by providing an audit trail • The risks associated with multiple card use across estates is mitigated by implementing effective policies, procedures and controls involving a 'closed loop' system • Auditing and the management of suspicion and triggers by senior members of the operator's staff can identify human error, trends, intelligence patterns and failures in policies and procedures • Customers accessing online wallets in retail premises required to provide proof of identity and passwords to withdraw or deposit into account

Consequences

- Removal of loyalty schemes has the potential to increase customer anonymity and, therefore, the likelihood of money laundering and criminal spending occurring in the sector
- Failures in controls relating to staff intervention using automated systems means customer information is lost and can no longer assist law enforcement
- There is evidence of customers spending the proceeds of crime in betting premises, particularly where the ability to remain anonymous has benefited the individual committing the crime
- Evidence of anonymity being exploited is increasing at present and would seem to support the view that it is recognised by criminals internationally as a key enabler of money laundering
- Staff fail to effectively implement policies and procedures for the 'closed loop' system, resulting in criminals being able to exploit the use of fraudulent or stolen debit cards across multiple premises of the same operator for betting with monies derived from a criminal lifestyle. There is also evidence that they use their own legitimate debit cards for this purpose
- Audit and management employees fail to identify or act upon triggers, incidents or errors resulting in criminal lifestyle spending occurring and continuing unchallenged in the sector
- Staff fail to request proof of identification or passwords for online wallets when customers deposit or withdraw from accounts whilst gambling in retail premises. Senior management fail to monitor activity effectively, thereby allowing criminally derived funds to be moved through online wallets and eventually legitimised through retail banking systems

Risk rating
• Anonymous customers laundering or spending the proceeds of crime: **Higher** • Accessibility to multiple premises assists those customers laundering monies by providing the means for them to spend larger amounts of cash with high levels of anonymity: **Higher** • Successful use of fraudulent or stolen debit cards increases due to employees failing to follow policies and procedures and 'closing the loop'. Poor oversight and monitoring by management fails to identify instances where 'closing the loop' has not occurred : **Higher**

Product vulnerabilities in the betting sector

Vulnerabilities	Controls
• Gaming machines, category B2 (also known as FOBTs) being used to launder criminally derived funds[11] • Self-service betting terminals (SSBTs) being used to launder criminal funds • It is important to also recognise the product risk of Bring Your Own Device (BYOD) which has emerged in both the on- and off-course non-remote betting sectors and, until further assessment of the product and its vulnerabilities occurs, it will be given a likelihood and impact rating of medium. • BYOD is an evolution of SSBTs, where consumers use their own device to place bets through non-account based play either in off-course or at on-course premises • Anonymity is a potential risk with BYOD, as a customer could place bets without needing an account or interacting with employees of the operator. There are further risks with customers potentially using multiple premises without this being identified by the operator, due to the lack of interaction; which is further compounded by a lack of staff knowledge and awareness, due to customer interaction not being required. While the technology exposes the non-remote on and off-course betting sector to ML/TF risks, robust management by operators should mitigate some of the risks identified, if employees are appropriately trained. Robust transactional monitoring in real time should be adopted by operators when using this innovation, which will allow swift and decisive identification of suspicious transactions or behaviour.	• Non-remote betting operators must comply with the Act, POCA, TACT and LCCP to assess and have in place suitable policies, procedures and controls to manage ML/TF risk, as required under LC12.1.1 risk assessment • Regulations imposing controls on B2 gaming machines to limit spins over statutory monetary limits • The use of CCTV and TITO receipts provide operators with the ability to follow up on criminal activity, and thereby assist law enforcement • Automated systems can allow for successful flagging of suspicious activity and, when used in conjunction with CCTV, can be used to identify customers suspected of money laundering and offer law enforcement an audit trail[12] • TITO receipts offer the opportunity to identify suspicious activity (including the insertion of large amounts of money with little or no play, and subsequent presentation and redemption of the ticket value over the counter), using data derived from play • Operators continue to develop tracking software for game play, assisting in the identification of customers • Some machines are designed to reject dye stained notes, as well as fraudulent notes and coins • Operators' policies, procedures and controls for SSBTs are implemented consistently and effectively in the sector in order to minimise opportunities for money laundering.

[11] This vulnerability is compounded by TITO technology and when used in conjunction with Automated Ticket Redemption (ATR) machines

[12] These are not, however, widespread across the sector

• eSports is a term used to describe the playing of computer games competitively. At present, betting operators offer a relatively limited range of betting on eSports, however, the Commission has published a position paper on eSports (along with virtual currencies and social gaming), following an engagement exercise and discussion paper in 2016. • AML risks for eSports primarily concern the use of companies who are not licenced by the Commission, potential issues in relation to betting integrity and the prevalence of bets wagered from higher-risk foreign jurisdictions.	

Consequences

- In the absence of human intervention or tracking software, the controls have the potential to be exploited by criminals seeking to launder criminally derived funds
- The sector will need to improve and further agree standards for machine triggers and flags so as to further develop opportunities for intervention
- Failure to implement regulations for limiting B2 spins over the statutory monetary limit will facilitate the use of gaming machines in betting premises to spend larger amounts of criminally derived funds
- Customers are able to redeem SSBT tickets across outlets, facilitating anonymity and the spending of criminally derived monies
- TITO redemption not tracked effectively and staff allow TITO vouchers to be redeemed across retail premises and between online and offline accounts through wallet account based play, thereby failing to 'close the loop'

Risk rating

- Gaming machines, category B2, being used to launder criminally derived funds: **Higher**
- SSBT machines used to facilitate the laundering of criminally derived funds: **Higher**

Means of payment vulnerabilities in the betting sector

Vulnerabilities	Controls
• Cash transactions • Cash or cash equivalents are widely recognised, including by FATF, as being attractive for money launderers and terrorist financers because of their anonymity, difficulties in tracing their origin, and because they can be forged and are easily transferrable. HMT and the Home Office's NRA highlights the use of cash as being high risk.	• All operators must comply with the Act, POCA, TACT and LCCP to mitigate risks associated with ML/TF • Ordinary code provision 2.1 anti-money laundering, licence condition 5.1.1 – cash handling, and licence condition 12.1.1 risk assessment place obligations on operators in relation to the use of cash and cash equivalents by customers. It is designed to minimise the risk of crimes such as money laundering and the spending of criminally derived funds • Some machines within the sector will reject dyed stained and fraudulent notes and coins • Controls in respect of gaming machines include triggers and alerts to possible suspicious activity, which then prompts staff intervention • Betting operators will monitor commercially high risk customers by flagging activity under their name or assigning them a nom de plume where the customer's name is unknown. The use of CCTV and interaction with staff helps operators to build profiles of such customers • Small and independent betting operators largely rely on staff awareness of their customers (due to a lack of technology) and the nature of their business (smaller customer base, reduced risk for liability margin and limited size of bets placed) limits the level of risk of money laundering • Betting premises' staff provide a presence to be able to intervene and carry out identity checks

The vulnerabilities associated with cash transactions include criminal lifestyle spending, foreign currency, Scottish and Irish notes, and fraudulent notes and coins.	• The betting sector is, at times, able to provide information to assist law enforcement due to the use of TITO vouchers, which provide an audit trail, and CCTV or triggers and alerts to detect suspicious game play • Much of the risk with cash transactions in on-course betting is mitigated, as the risk appetite of many on-course operators limits the size of bets placed. In addition, the transient nature of customers attending on-course events mitigates repeated, ongoing criminal spending, and the limited number of on-course betting events taking place on any given day mitigates opportunity and value.

Consequences

- There is evidence of cash as a vulnerability being exploited to launder criminally derived monies within the off-course betting sector
- Employees failing to log or incorrectly allocating cash spent by monitored customers to their nom de plume resulting in false or under-reported triggers, trends in criminal lifestyle spending or money laundering will obscure criminal spending, and thereby potentially undermine investigations
- Employees intimidated due to them residing in the same geographic area as customers suspected to be spending criminally derived cash, resulting in under-reporting, or none-reporting of suspicious activity
- Regarding anonymity, there is frequently an audit trail that cannot be linked to a criminal, thereby reducing the risk of detection of criminality in a law enforcement investigation.

Risk rating

TITO used in conjunction with ATR machines: **Higher**
Cash transactions: **Higher**

Bingo (non-remote)

Bingo (non-remote)	Overall rating
	Medium

Control vulnerabilities in the bingo sector

Vulnerabilities	Controls
Bingo operators failing to comply with the Act, POCA, TACT and LCCP requirements and taking into account Commission guidance under ordinary code 2.1.2 • This vulnerability relates to bingo operators failing to apply controls to mitigate the risk of ML/TFML/TF It is important to also recognise the following control risk which may begin to emerge in the non-remote bingo sector: • It is expected, by a significant operator in this sector, that membership schemes will be removed (with the exception of EBT play). This alteration to the business model of the non-remote bingo sector may lead to a decline in information known about customers using their gambling facilities (inclusive of gaming machines on the premises). Furthermore, it could result in a decline of interaction with customers gambling on the premises. Both of these factors, would increase the anonymity of customers on licensed premises, largely in a cash rich environment, thereby increasing ML/TF risks in the sector • The Commission understands that it may also be the intention of the sector to request local licensing authorities to remove a default licence condition which currently prevents the playing of bingo between 00:00 and 09:00 hours. If this request is successful, it may lead to an increase in customers playing bingo during these hours (as well as gaming machines which are not currently prohibited during these hours). Taken in conjunction with the risk of increased anonymous gambling due to a potential decline in membership, it may pose a higher risk as it is traditionally a time that the business is minimally staffed. This may potentially result in a time of day/evening where an even greater risk of weak controls exists, which could lead to exploitation by criminals.	• The size of stakes, although higher than some other non-regulated sectors, goes some way to mitigating the risk of 'traditional' money laundering within the sector, such as 'washing' criminally derived funds • Controls within the sector largely rely on staff supervision and face-to-face interactions with customers • Membership schemes have the potential to increase operators' knowledge about their customers and assist in the detection of money laundering • CCTV and automated triggers assist in identifying and reporting suspicious behaviour by customers to law enforcement, however, this is unlikely to be in real time • Effective implementation of the Act, POCA, TACT and LCCP policies, procedures and controls are designed to mitigate the risk of money laundering and employees are trained to report incidents to their employer.

Consequences

- Non-remote bingo operator fails to comply with the Act, POCA, TACT, LCCP through poor policies, procedures and controls, monitoring, training, limited embedding of published learning and poor risk assessment, resulting in non-compliance. The Commission will take action where it identifies non-compliance. This may range from action plans through to the review and/or revocation of personal and/or operating licences. Failure to follow good practice provided by the Commission in guidance published under ordinary code 2.1.2 or published learning will be a material factor in considering any action, including reviewing and/or revoking personal and/or operating licences

- Stake size is controlled with paper-based bingo as it is self-monitored due to the skill of playing more than six individual tickets simultaneously. Electronic bingo is also controlled by the individual operators' risk appetites, which limits the profitability and opportunity for traditional money laundering. Gaming machine and table top bingo play are a significant proportion of the bingo industry's profit stream, with minimal knowledge of the source of such funds that customers are using. However, limited controls are in place to monitor or assess the funding of gaming by customers. This provides an enabler for 'smurfing' which, in this context, could comprise low level stakes being placed by an organised group of individuals within the same premises whilst playing bingo or participating in gaming to avoid detection of large amounts being staked by an individual. This aspect is also relevant to all other non-regulated sectors in gambling, where 'smurfing' can occur

- Failure by employees to follow their employer's policies and procedures intended to mitigate money laundering, has resulted in criminal lifestyle spending continuing in the sector
- Decline in the use of membership schemes increases the anonymity of customers in the sector, which is an enabler for criminal spending
- Real time reporting of suspicious behaviour triggered by automated systems and/or observed behaviour is delayed, either due to technological limitations, limited employee knowledge or limited staffing levels, or a decreasing level of employees knowledge of regular customers due to the decline of membership
- Senior management decision makers with oversight of data and incidents are not effectively identifying criminal lifestyle spending within their estate through ineffective analysis and minimal customer knowledge.

Risk rating

The majority of money laundering through this sector is criminal lifestyle spend. There is evidence of money laundering within the sector enabled by the increasingly anonymised business model. At present, the amount being laundered is similar to that in some other medium risk sectors and is currently limited. The Commission has no evidence of terrorist financing occurring within the bingo sector.

Bingo operators failing to comply with the Act, POCA, TACT and LCCP requirements: **Medium**

Licensing and integrity vulnerabilities in the bingo sector

Vulnerabilities	Controls
• Bingo operations acquired by criminals as a means to launder criminal funds • Bingo employees colluding with criminals to launder criminal funds	• The Commission assesses new and current licensees against a range of factors to ensure that the activities are carried out in a way that minimises the risks to the licensing objectives • The Commission independently assures itself, through external audit processes, that its controls are robust • The Commission receives and shares intelligence with law enforcement agencies, which has the potential to assist in identifying individuals associated with criminal activity • The Commission has sole responsibility for licensing individuals in qualifying positions which require fit and proper tests • Instances where there are concerns of staff integrity, bingo operators will act appropriately and take action where appropriate • Training, and the monitoring of customers and transactions mitigates some of the risks associated with this vulnerability • Licensed individuals are subject to both general and individual licence conditions under sections 75 and 77 of the Act which ensures ongoing suitability, including conditions for reviewing and revoking individual licences.

Consequences

- There is limited evidence of bingo operators being acquired by criminals
- The Commission has robust controls in place to prevent criminals acquiring bingo operators
- There is nothing to suggest bingo operators are being run as a ML/TF vehicles by organised criminals
- There has been some evidence of possible collusion, which raises questions regarding integrity, however, the number of incidents reported to the Commission are very low

Risk rating

Bingo operators acquired by criminals as a means to launder criminal funds: **Medium**
Bingo employees colluding with criminals to launder criminal funds: **Medium**

Customer vulnerabilities in the bingo sector

Vulnerabilities	Controls
Anonymous customers laundering or spending the proceeds of crime	• Bingo operators must comply with the Act, POCA, TACT and LCCP. They should take into account the Commission's advice on POCA, as required under section 2.1 of the LCCP • Licence condition 12.1.1 places obligations on operators to assess ML/TF risks to their business and implement suitable policies, procedures and controls to mitigate those risks • Membership schemes can remove an aspect of the anonymity of customers, however, membership is currently in decline • Automated systems allow operators to flag suspicious activity and patterns of play • Whilst it is recognised that alerts, triggers and similar techniques have the potential to mitigate the risks associated with machine products, effective staff intervention to determine whether an alert is valid or not remains critical • CCTV and TITO, when used in conjunction, can provide a reactive control to assist law enforcement investigations.
Consequences	
• Removal of membership schemes has the potential to increase the likelihood of money laundering occurring in the sector due to increased anonymity • Additionally failures in controls relating to staff intervention means customer information may go unreported or inappropriately acted upon • There is evidence of customers spending the proceeds of crime in bingo premises, where the ability to remain anonymous has benefited the individual perpetrating the crime • Although the evidence of this vulnerability being exploited is limited at present, anonymity is internationally recognised as a key enabler for money laundering.	
Risk rating	
Anonymous customers laundering or spending the proceeds of crime: **Medium**	

Product vulnerabilities in the bingo sector

Vulnerabilities	Controls
• Category D, C, B4, and B3 machines being used to launder[13] criminally derived funds • Electronic bingo terminals (EBTs) with gaming machine content being used to launder[14] criminal funds	• Bingo operators must comply with the Act, POCA, TACT and LCCP. They must assess the risks to their business and have in place suitable policies, procedures and controls to manage the identified ML/TF risks, as required byLC12.1.1 risk assessment • Automated systems can allow for the flagging of suspicious activity and, when used in conjunction with CCTV, it could be used to identify customers suspected of money laundering[15] • TITO offers the opportunity to identify suspicious activity (including the insertion of large amounts of money with little or no play, and subsequent presentation and redemption of the ticket) using data derived from game play • Some machines will reject dye stained notes, especially those heavily dyed as well as fraudulent notes and coins • Effectiveness of controls largely relies on scrutiny of customers and their gambling activity by staff

[13] Particularly criminal spend
[14] Particularly criminal spend
[15] These are not, however, widespread across the sector

• Cash table top gaming being used to launder criminal funds • Gaming machines played on EBTs being used to increase anonymity and launder criminal funds	• EBTs set the maximum purchase amount to play bingo and gaming machine levels are controlled by applicable gaming machine regulations • EBTs are rented for a session of bingo through interaction with operators' employees, providing face-to-face interaction • EBTs rented ensures any gaming occurring through gaming machines, via an EBT device, are traceable transactions • Pricing structures for bingo stakes limit the vulnerabilities afforded to criminals laundering or spending criminal lifestyle cash • Limited stake size and length of play for this type of gaming mitigates traditional laundering of monies through table top gaming

Consequences

- There is evidence of money laundering occurring through the use of gaming machines within the sector, although this is currently limited
- In the absence of machine supervision, the controls have the potential to be exploited by a criminal either disposing of lifestyle spend or laundering
- Ineffective levels set for machine alerts and triggers, with the threshold being too high to efficiently detect criminal lifestyle laundering of monies
- Traditional paper-based bingo significantly reduces staking levels by virtue of the human capability to play multiple games within the pace of the game. EBTs significantly increase staking levels, which provides additional routes for laundering or spending lifestyle cash derived from criminality in a relatively anonymous environment. Additionally, customers are afforded the opportunity to play gaming machines through EBT units, providing a further route to spend monies in a reasonably anonymous environment
- Frequency and variety of stakes for table top gaming affords the opportunity for the spending of criminal lifestyle monies.

Risk rating

Gaming machines, category B3[16] being used to launder[17] criminal funds: **Medium**
Electronic bingo terminals (EBTs) with gaming machine features being used to launder[18] criminal funds: **Medium**
Table top gaming being used for criminal lifestyle spending: **Medium**

Means of payment vulnerabilities in the bingo sector

Vulnerabilities	Controls
• Cash transactions • TITO used in conjunction with ATR machines	• Licence condition 5.1.1 – cash handling places obligations on operators for the use of cash and cash equivalents by customers, designed to minimise the risk of crimes such as money laundering • Some machines within the sector will reject dyed notes, and fraudulent notes and coins • Controls are largely machine triggers and alerts to possible suspicious activity, prompting staff intervention • Although TITO is recognised as a vulnerability, it can also be considered a control when used in conjunction with CCTV. However, this is reactive in nature • Gaming machine areas where TITO and ATR machines are located have employees working in such areas for customer service purposes, and any suspicious behaviour can be reported for investigation. Gaming machine content can be used on EBT units which is usually purchased from an employee • EBT units are usually rented from the operator for the duration of the gaming session, which facilitates interaction with the customer in areas monitored by CCTV.

[16] A gaming machine with a maximum stake of £2 and a maximum price of £500
[17] Particularly criminal spend
[18] Particularly criminal spend

Consequences

- Cash is recognised by FATF as a key money laundering vulnerability. This sector mainly receives cash payments from customers and makes payments in cash to customers, making this sector attractive for criminal lifestyle spending and 'smurfing' of low amounts of criminal money

- Controls which focus on the use of customer information could be further improved within the sector. With membership schemes in decline, the quality and reliability of customer information may be jeopardised

- Cash transactions by anonymous customers in the bingo sector account for most of the non-remote bingo transactions. Declining membership increases the risk of the sector being exposed to further money laundering activities

- EBTs offer the facility to increase the amount of staking in traditional bingo from the usual six tickets to upwards of 72 tickets. EBTs also offer gaming machine content to customers, which can be played away from the traditional gaming area. A combination of increased staking levels, gaming machine content, table top gaming (table top content can be played via the EBT unit, or table top or both by the customer) and reduced supervision by the operator (as the customer can play table top bingo, traditional bingo games and gaming machine content at their table as opposed to a security monitored area of the premises) increases the risk of low level criminal lifestyle and 'smurfing' within the sector

- Employees located in areas where TITO and ATRs are situated, may be moved to other areas of the business, leaving these areas understaffed or poorly supervised. This results in customers being able to use TITO and ATRs in unsupervised areas, which allows customers to have minimal staff interaction or avoid staff interaction

- There is evidence of these vulnerabilities being exploited within the bingo sector

Risk rating

Cash transactions: **Medium**
TITO used in conjunction with ATR machines and EBT units: **Medium**

Casino (non-remote)

Casinos (non-remote)	Overall rating
	Higher

Control vulnerabilities in the non-remote casino sector

Vulnerabilities	Controls
• Non-remote casino operators failing to comply with the Act, POCA, TACT, the Regulations (inclusive of MSB activities) and LCCP requirements • This vulnerability relates to non-remote casino operators failing to apply controls to mitigate the risk of ML/TF.	• Casinos are part of the regulated sector and must comply with the Act, POCA, TACT, the Regulations and LCCP requirements • Senior management must appoint a nominated officer and must comply with requirements in the Regulations to minimise the risk of ML/TF occurring. The role of the nominated officer includes: reporting suspected or known ML/TF activity via SARs, providing adequate training to employees, and reporting annually on the business's AML activities to their senior management and board • CDD checks, including the verification of customer identities and source of funds, which should limit the risk of exposure to money laundering • PEP monitoring should minimise corruption and the risk of money laundering occurring • Staff supervision, CCTV and automated triggers derived from transactional data assist in identifying and reporting suspicious behaviour by customers to law enforcement • Policies, procedures and controls implemented effectively should minimise the risk of ML/TF through effective risk assessments, monitoring, training and revision of risk assessments • Fit and proper persons in key positions are licensed to undertake specified roles to mitigate the risk of ML/TF occurring • In instances where there are concerns about staff integrity, operators will take action where appropriate. If the staff are also licensed by the Commission, we may consider revocation of their personal licences • Adequate supervision of table gaming and gaming machines minimise the risk of money laundering, criminal lifestyle spend, cheating and collusion • The risks associated with product or means of payment innovations are assessed for any impact upon money laundering requirements, and controls are implemented to effectively mitigate any risks posed • Formal tronc system established by casino operators to discourage collusion between employees and customers, which mitigates corruption and money laundering • Section 81 of the Act prohibits credit in casinos. With effectively implemented policies and procedures, this limits the risk of illegal money lending (which is also subject to an ordinary code provision in LCCP 3.8.1) • Casinos must comply with the Regulations in respect of Money Business Services for foreign currency exchange to minimise the risk of ML/TF • Membership schemes increase the operators' ability to know their customers, confirm their details and verify their identity, ascertain their source of funds and wealth, and check their PEP and sanctions list status. This decreases the risk of money laundering and terrorist funding in the sector • Operators ensure effective monitoring of sanction lists, both country and individual specific, taking note of the restrictions and acting accordingly to mitigate the risk of criminally derived cash infiltrating the UK financial and associated sectors.

Consequences

- Non-remote casino operator fails to comply with the Act, POCA, TACT, the Regulations (inclusive of MSB activities) and LCCP by having poor policies, procedures, controls, monitoring and training; failing to embed applicable learning published by the Commission; and conducting an inadequate assessment of the risk and failing to review and adjust it in the light of new and emerging threats, which results in non-compliance. The Commission will take affirmative action where it identifies non-compliance, which may range from action plans through to the review and/or revocation of personal and/or operating licences. Failure to follow good practice as advised by the Commission, through ordinary code provision 2.1.1, will be a material factor in considering any action we take to review and/or revoke personal and/or operating licences

- Continued evidence of money laundering through collusion, cheating and criminal lifestyle spending, due to policies, procedures and controls not being effectively implemented, monitored or revised by senior licensed employees

- Failure by senior management and nominated officers to identify areas of ineffective or negligent staff training, which results in poor compliance by staff, including: not following policies, procedures and controls; and not identifying that senior licensed staff are failing to monitor the effectiveness of employees' performance and their ability to follow policies, procedures and controls. Senior management's failure to identify and rectify failures by employees in the above areas remains a concern in the sector

- Nominated officers' failing to submit SARs when knowledge or suspicion has been identified by them, or procedures are not sufficiently effective for the nominated officer to assess whether knowledge and suspicion has been identified, remains an area of concern in this sector

- Failure by licensed employees to follow policies, procedures and controls intended to mitigate ML/TF has resulted in criminal lifestyle spending continuing in the sector

- Decline in the use of full membership schemes and threshold or hybrid CDD schemes increases the opportunity for customers in the sector to spend criminally derived funds for a period of time before reaching the monetary threshold and triggering full CDD procedures

- Real time reporting of suspicious behaviour triggered by employee intervention, automated systems and/or observed behaviour is delayed due to the use of threshold and or hybrid CDD models, limiting the level of information known about customers

- Senior management decision makers with oversight of data and suspicion are not effectively identifying criminal lifestyle spending within their estate and reporting it to law enforcement

- Licensed employees colluding with customers for personal gain remains evident in the sector. Cheating is a criminal offence under the Act and any personal gain from cheating is the proceeds of crime

- Employer's resource to effectively monitor table and gaming machine play being reduced to save on costs, increases the likelihood of criminal lifestyle spending occurring in the sector. Monetary threshold limits apply separately to both table play and gaming machine play in this sector, as applicable by the Regulations. Due to resource pressures and cost saving requirements, this may lead to inconsistently monitored areas of gaming, capturing of customer behaviour / spend and under reporting of suspicion or knowledge

- New products and means of payments being introduced to increase consumer service and operator profits are not considered against a risk framework for ML/TF prior to implementation. Compliance considerations are overlooked or dismissed leading to increased likelihood of ML/TF occurring within the sector

- MSB activities, such as foreign currency exchange, not implemented correctly or effectively may result in overseas criminally derived funds infiltrating the UK's financial system and the potential for committing criminal offences by circumventing other jurisdictions' money laundering legislation and controls

- Failing to monitor the sanctions list, for either country or individual restrictions, resulting in illicit funds being used in the sector and ultimately infiltrating the UK's financial system

- Failing to identify PEPs prior to gaming increases the likelihood of monies derived from corruption being laundered through the casino and ultimately infiltrating the UK's financial system

- Failure by the sector to implement an effective tronc system, as required by licence condition 10.1, will increase the likelihood of employees accepting undeclared tips from players. This could result in increased instances of collusion and cheating in the sector, with personal gains from these activities being regarded as the proceeds of crime

- Failure by the sector to prevent credit being provided to customers through facilities offered by the operator, resulting in customers extending credit to other customers for profit, which is a criminal offence under section 81 of the Act. Operators' failure to prevent this increases the likelihood of money laundering occurring through their businesses

- Automated triggers and CCTV footage providing data on suspicious table or machine gaming, or in relation to the behaviour of customers. The failure to act upon this, either through poor staff knowledge or negligence, will increase the likelihood of money laundering and criminal lifestyle spending occurring and going unreported to senior decision makers in the business, and to law enforcement

- Failure by the nominated officer to identify and act upon any of the above circumstances increases the likelihood of money laundering, including criminal lifestyle spending, occurring in the sector and could result in the nominated officer committing criminal offences under POCA

- Risks not detected or acted upon by the nominated officer result in an inadequate money laundering report being submitted to the operators' senior management and Board. Corporate negligence through ineffective monitoring and revision of policies, procedures and controls designed to minimise ML/TF, which may result in criminal offences under POCA being committed.

Risk rating

The Commission has evidence of non-remote casino operators failing to comply with requirements: **Higher**

Based on the likelihood and impact of these vulnerabilities being exploited in the non-remote casino sector, it receives a rating of **higher**

Licensing and integrity vulnerabilities in the casino sector

Vulnerabilities	Controls
The two highest impact licensing and integrity vulnerabilities in the non-remote casino sector are: • attempts by organised criminal gangs to acquire casino operations as a means to launder criminal funds • casino employees acting in collusion with criminals to launder criminal funds FATF recognise both vulnerabilities in their most recent gaming sector review. The vulnerability of casino operations being run by organised criminal gangs is also identified within Treasury's National Risk Assessment of ML/TF. Both vulnerabilities receive a rating of **medium-to-higher.** It is important to also recognise the following licensing and integrity risk which has emerged in this sector and could emerge in other gambling sector in the future. The risk rating provided for this licensing and integrity risk is medium likelihood and impact until further assessment: • Ultimate Beneficial Ownership (UBO) It has emerged that, when businesses apply to be licensed, or those already licensed apply for a Change of Corporate Control (CoCC), companies listed on stock exchanges in certain jurisdictions (for example, Hong Kong) permit the shares to be held by brokers or custodians who have no obligation to reveal who are the	The Commission effectively mitigates the risk of gambling operations being run by organised crime. • The Commission assesses new licence applications (including personal licence applications) and current licensees against a range of factors to ensure that the licensee is suitable and the activities they carry out are conducted in a way which minimises the risks to the licensing objectives. The Commission has robust and independently assured controls in place to mitigate this vulnerability from being exploited • Although the Commission licenses individuals in qualifying positions, it is the primary responsibility of operators to limit any risks of employee collusion. Compliance with the LCCP, in particular social responsibility code 7.1.1 – Gambling staff – casinos, SR code 4.2.5 – supervision of games and 5.1.1 – cash handling, further mitigate this risk • In instances where there are concerns about the integrity of a staff member, it is expected that casino operators will act appropriately to investigate and take

ultimate beneficiaries of the shares. In the absence of such information, and if share options are offered by the group to raise funds are taken up by the unknown ultimate beneficiaries, the risk is that the source of funds and source of wealth of the unknown beneficiary will not be identifiable to the Commission. This emerging risk has been revealed in the non-remote casino sector, but could equally occur in other gambling sectors licensed by the Commission. Sufficiently robust controls implemented by the Commission have so far prevented any applications or CoCC being granted under these circumstances. The Commission will keep this emerging risk under scrutiny and report in the next iteration of this assessment.	action where necessary. Additionally, licensed individuals are subject to both general and individual licence conditions under sections 75 and 77 of the Act, which address ongoing suitability (this includes conditions in relation to reviewing and revoking individual licences).

Consequences

- Vulnerabilities relating to casino operations being run by organised criminals have materialised to the extent that attempts appear to have been made by organised criminal gangs to acquire gambling businesses as a means to launder criminal proceeds. However, the Commission's controls have been sufficiently robust and these attempts appear to have been prevented to date

- Vulnerability of casino operations run by organised criminal gangs as a means to launder criminal funds receives a rating of medium-to-higher, as the Commission recognises the high impact but medium likelihood of occurrence. This vulnerability is also recognised by FATF and is discussed in Treasury's NRA

- Vulnerability relating to casino employees acting in collusion with criminals to launder criminal funds has materialised in this sector. The Commission has evidence of employees colluding with customers to launder criminal proceeds. Staff employed in qualifying and functional positions within the casino industry have demonstrated dishonesty, and collusion with customers and between employees, resulting in criminal convictions. Serious cases have resulted in licence reviews and subsequent revocation of personal licences by the Commission. Properly applied controls by operators can mitigate the risk of collusion by employees.

Risk rating

Operator being owned by organised criminal gang: **Medium-higher**

Casino employees acting in collusion with organised criminal gangs to launder criminal funds: **Higher**

Customer vulnerabilities in the casino sector

Vulnerabilities	Controls
The Commission has identified six customer vulnerabilities in the non-remote casino sector: • Customers' breaking up large amounts of cash into smaller transactions in order to minimise suspicion and evade threshold reporting requirements, commonly referred to as 'smurfing' • False and stolen documentation used to bypass controls for the identification and verification of individuals in order to launder criminal funds	• In addition to POCA, the casino sector must comply with the Regulations. They are required to undertake measures regarding customer due diligence (CDD) including ongoing monitoring, simple due diligence (SDD) and enhanced customer due diligence (EDD), record-keeping, policies, procedures and controls, and training • The senior management of operators have the responsibility to: appoint a nominated officer; provide sufficient employee training in relation to ML/TF; and to establish, maintain and update risk-sensitive policies and procedures • In threshold casinos[20], full verification is required either at the point a business relationship is established or until the customer reaches or approaches the €2000 threshold for either table gaming or gaming machine play or both. Some of the controls available to mitigate the vulnerability of exploiting the CDD threshold arise from requirements contained within the LCCP relating to table supervision, CCTV and effective employee training, so as to ensure that employees recognise possible indicators of ML/TF

[20] Under the Gambling Act 2005 membership is not required and the threshold approach can be applied, whereby customer identification is only required if the financial threshold of €2000 is reached.

• Use of third parties or agents to obscure the source and ownership of money gambled by overseas customers and the customers' identities • Customers from high risk jurisdictions using casino facilities to launder criminal funds, deposit large amounts of cash on account or withdraw large amounts of cash (which is either held on deposit or involves sham transactions), thereby circumventing AML controls • Customers who appear on sanctions lists being permitted, either intentionally or through negligence, to launder criminal funds • PEPs using casinos to clean criminal funds.[19]	• Measures to reduce criminals using false or stolen identification in the casino sector begins with registration and initial screening, authentication and verification processes. Operators use a range of software which enhances the ability to validate a customer's identity and prevent criminals using others or false identities to money launder. More sophisticated software which risk scores a customer on the basis of their historical play and transactions is further used to prevent fraudulent activity • Casinos are required to have effective controls to manage high-risk customers. Many operators compare new and existing customers against PEPs databases and sanctions lists. Parts of the industry have developed and maintain awareness of those countries which are considered to present a higher risk of corruption • Third parties or agents visits to casinos are usually known in advance, and casinos must comply with licence condition 3.1.3 to minimise the risk of money laundering and cheating. Casinos will use this advance notice to conduct a risk assessment of the relevant third parties and any visitors, including: PEP screening, sanctions list review, depositing of foreign currency, cheque cashing facilities, money transfer facilities, identification and verification processes in relation to the agent and any customers they introduce to the casino.

Consequences

- Effective implementation of policies, procedures and controls, and having assurance that the controls in place are robust through effective monitoring are the broad areas of weakness demonstrated to the Commission through our compliance activity and casework over the past four years. Public statements issued by the Commission demonstrate serious failings within this sector in relation to CDD, EDD, ongoing monitoring, staff training, the implementation of policies, procedures and controls, and record keeping

- Due to continuing failings in the sector, the Commission has taken steps to engage the relevant trade association and operators to improve compliance

- FATF recognises that structuring or smurfing[21] occurs within the casino sector, the extreme of which is where customers (particularly vulnerable persons are asylum seekers, students and those that have been trafficked) are being used as 'mules' to launder money below the monetary threshold in casinos with threshold access models. The Commission holds some intelligence and evidence of this vulnerability materialising, however, this is limited. Customers' smurfing in order to minimise suspicion and evade threshold CDD requirements, receives a risk rating of medium-to-higher, as a result of it being identified as having a medium-to-higher impact and being likely to occur in the casino sector by comparison to other gambling sectors. Evidence suggests that there are opportunities for casinos to improve their controls to mitigate this vulnerability and to improve their monitoring processes to more frequently detect its occurrence and inform authorities timeously

- FATF and the European Commission recognise identity theft as an increasing trend in money laundering. Customers using false or stolen identity documentation to disguise their true identity, thus avoiding money laundering activity being traceable to them within the gambling industry, does occur. It is challenging to detect customers who use false or stolen documentation, given the number of sophisticated techniques criminals now employ and the broad range of nationalities the GB casino sector attracts. The vulnerabilities relating to customers who attempt to open accounts or verify their age by using forged or stolen identities affects all gambling sectors.
- The use of third parties and agents primarily applies to the London high-end casino sector. It receives a

[19] It is important to note that domestic PEPs and foreign PEPs are subject to the Regulations which came into force in June 2017. The Commission will be assessing the sector's compliance with the new legal requirement in the future and will provide further comment on this risk in the next published assessment.

[21] Structuring or smurfing is the breaking up of large amounts into smaller amounts for the purposes of money laundering. This is often accompanied by the use of third party 'mules' to undertake transactions with the structured funds. Funds exchanged for casino value instruments are often 'cashed up'.

rating of medium-to-higher, recognising the high impact relative to other sectors of the gambling industry and some evidence that money laundering legislation in other jurisdictions has been incorrectly applied, and UK legislation does not have direct applicability in those jurisdictions. Steps are being taken by the industry and the Commission to ensure that the use of third parties and agents is prevented from being used as a way to facilitate money laundering and cheating in the GB non-remote casino sector

- The Commission does not have significant evidence that PEPs, customers from high risk jurisdictions or customers appearing on sanctions lists are laundering illicit funds through the non-remote casino sector. The Commission currently has limited information on the number of PEPs frequenting GB non-remote casinos. The Regulations now include domestic PEPs, however, many casinos previously adopted measures similar to that for international PEPs for domestic holders of public office and VIPs, so this control measure should be adopted swiftly in the sector.

Risk rating

Customers breaking up large amounts of cash into smaller transactions in order to minimise suspicion and evade threshold CDD requirements, the use of false or stolen identity documentation and the use of third parties or agents to introduce criminal funds receives a risk rating of **medium-to-higher**. These three vulnerabilities are also identified by FATF for the non-remote casino sector.

The remaining three vulnerabilities received a rating of **medium**.

Smurfing: **Medium-Higher**
False or stolen identity documentation: Medium-Higher
Agents: Medium-Higher
MSB activities: Medium
Sanctions: Medium
PEPs: Medium

Product vulnerabilities in the casino sector

Vulnerabilities	Controls
The product vulnerabilities within the sector are: • electronic roulette[22] • peer-to-peer gaming (poker) B2C • gaming machines The vulnerabilities in relation to electronic roulette are compounded where customers play individually at terminals rather than at a live table with staff supervision, due to the use of TITO facilities to cash out monies won without staff intervention. This risk applies to threshold and hybrid[23] casinos where a customer plays below the €2000 CDD threshold. The vulnerability of peer-to-peer gaming (poker) is associated with the ability for customers to collude and deliberately 'transfer' funds to one another. The Commission considers peer-to-	The casino sector must comply with the Act, POCA, TACT, and the Regulations and should act in accordance with the Commission's guidance on anti-money laundering under LCCP[24] ordinary code provision 2.1.1. Casino operators are therefore required to apply a risk-based approach to manage and mitigate the ML/TFML/TF risks they face • LCCP Social Responsibility code provision 4.2.5 applies to non-remote casinos. They must put in place effective policies and procedures concerning supervision of table gaming • LCCP Social Responsibility code provision 9.1.3.2 applies to non-remote casinos (with the exception of 2005 Act premises) and requires appropriate supervision by staff of gambling facilities offered at all times. Gaming machines on offer on the premises must be adequately supervised by staff at all times to mitigate the risk of money laundering and prevent breaches of the Regulations monetary threshold. Adequate supervision allows for prompt and effective detection of customers attempting to launder monies through gaming machines, and assists with the reporting of suspicious activity by the nominated officer to law enforcement • licence condition 5.1.1 – cash and cash equivalents requires

[22] This is compounded by the use of ticket in, ticket out (TITO) technology and automated ticket redemption machines (ATRs).
[23] This is where a casino uses a combination of the membership and threshold approaches.
[24] A new version of the licensing conditions and codes of practice (LCCP) came into effect on the 31 October 2016. The new LCCP amends and adds some requirements for operators in respect of crime including anti-money laundering.

peer gaming (poker) and electronic roulette to be two of the highest risk products offered by the casino sector, and they receive a rating of higher. Casinos also offer a variety of gaming machines, up to and including B1 class. Risks associated with gaming machines are explained in depth in the gaming machines section and also apply in this sector. The additional vulnerability that casinos have in this regard is their ability to meet the CDD requirements in the Regulations. Inconsistent staffing levels impacting on the ability to adequately monitor customers approaching the mandatory threshold for CDD is evidenced by Commission compliance activity. Those casinos that adopt an approach where customers are only identified when they reach the CDD threshold potentially provide customers with additional anonymity whilst playing on gaming machines, which is compounded by inadequate staffing levels in gaming machine areas.	operators to put into effect policies and procedures designed to minimise the risk of crimes such as money laundering and the offering of credit. It also requires operators to implement such policies and procedures effectively, keep them under review and ensure that they remain effective • Licence condition 12.1.2 requires operators to conduct a risk assessment of their business being used for ML/TFML/TF. It is to be reviewed if changes occur to the business (e.g. new products), and in any event at least annually. Policies, procedures and controls produced as a result of the risk assessment must be implemented effectively, and reviewed regularly to ensure policies, procedures and controls remain effective. • Controls to mitigate product risks within the non-remote casino sector include table and gaming machine supervision, awareness by staff, the use of CCTV, transaction monitoring, and automated alerts and triggers on gaming terminals • As far as gaming machines are concerned, effectiveness in identifying activities which may raise suspicion of ML/TF varies from operator to operator. Operators have set up alerts and triggers to identify suspicious patterns of play and to comply with the €2000 CDD threshold.
Consequences	
• The Commission is not satisfied that the casino industry is applying their control requirements to the rigour set out in the Regulations or the Act. This is demonstrated through Commission investigations and compliance activity over the past 18 months, which have demonstrated consistent failings in this sector • The Commission considers electronic roulette to be a higher risk product. There is evidence that the vulnerabilities with this product has materialised in the sector and that the relevant controls can be improved • Evidence of the product vulnerability of electronic roulette terminals being exploited is largely where there is an absence of customer interaction through staff supervision • Electronic roulette is rated higher due to the continued occurrence of money laundering by criminals using this product • Peer-to-peer gaming (poker) is also rated as higher as it is assessed as having high impact and likelihood due to operators failing to implement effective controls to mitigate this vulnerability and it subsequently being exploited by criminals.	
Risk rating	
The Commission considers peer-to-peer gaming (poker), electronic roulette and gaming machines to be three of the highest risk products offered by the casino sector, and receive a rating of **higher**.	

Means of payment vulnerabilities in the casino sector

Vulnerabilities	Controls
The greatest means of payment vulnerabilities within the casino sector are: • cash or cash equivalents transactions (this includes the exchange of foreign currency, cheque cashing facilities and money transfer) • ticket in, ticket out (TITO) in a threshold and hybrid casino[25] Cash is internationally recognised as being attractive to money launderers and terrorist financers because it facilitates anonymity, is difficult to trace and is easily transferrable. Treasury's NRA highlights the use of cash and MSB activities within the regulated sector as high risk. The vulnerabilities associated with cash transactions includes cash equivalents (TITO), stained and fraudulent notes/coins, and MSB activities. Although TITO can be considered a control for cash in the right circumstances, it is also considered a vulnerability particularly when used in conjunction with ATRs. It is also important to recognise the following means of payment vulnerability which is emerging across the sector. The risk rating provided for this payment method is medium likelihood and impact until further assessment: • Contactless payments This payment method is currently emerging in the non-remote casino sector. It is unclear currently what risk of ML/TF this technology poses. This issue will be further considered in the next iteration of the risk assessment.	• The casino sector must comply with the Act, POCA, TACT, the Regulations (inclusive of MSB activities), LCCP[26] and should act in accordance with the Commission's AML guidance. In regard to foreign currency and large cash transactions, LCCP Social Responsibility Code provision 5.1.1 requires all casino operators to have effective policies and procedures for the handling of cash and cash equivalents (banker's drafts, script cheques, foreign currency and debit cards), designed to minimise the risk of crimes such as money laundering • Controls must be implemented to mitigate money laundering risks associated with the use of cash in the casino sector. Vulnerabilities within the sector vary depending on which membership model the casino[27] adopts. However, it is standard practice that, if a customer wishes to use a foreign exchange facility, they will be required to have an account or be a casino member, therefore customer due diligence will have been carried out on at least one occasion. Additionally, cashiers who operate the foreign exchange service within the casino will be personal licence holders and undergo training in relation to AML, POCA, TACT and the Regulations • TITO controls primarily involve staff supervision, automatic triggers/alerts for machine- based play and the use of CCTV. Customer due diligence is carried out when: a business relationship is established with the customer; when the €2000 CDD threshold is approached and when enhanced customer due diligence for those customers considered higher risk is required. Many machines within the sector will reject dye stained notes. The sector has an opportunity to work with machine manufacturers to further improve the effectiveness of alerts and triggers.

Consequences

- FATF is one of many international bodies that identify the reliance by criminals and terrorists on cash. By using cash, money launderers are able to stay close to their money without having to place those funds into the financial sector (which leaves an audit trail).[28] The Commission concurs with FATF's view. We have found strong evidence of the vulnerability of cash transactions being exploited within the sector

- The use of script cheques permits large amounts of money to be deposited into the casino accounting system for the customer to draw down and settle against. This type of arrangement is widespread in

[25] This vulnerability is compounded when considered in conjunction with electronic roulette and in situations where the casino operates an ATR machine. There is evidence of the use of TITO in threshold casinos to enable the use of large amounts of cash beneath the CDD threshold and in the absence of human interaction.
[26] A new version of the licensing conditions and codes of practice (LCCP) came into effect on the 31 October 2016. The new LCCP amends and adds requirements for operators in respect of crime prevention, including anti-money laundering and counter terrorist financing.
[27] Membership casinos require a customer to provide full ID before being allowed entry into the casino.
[28] FATF: Vulnerabilities of Casinos and Gaming Sector – March 2009

casinos and is particularly prominent in high-end London casinos. This arrangement falls outside the traditional banking system (which has controls to minimise money laundering opportunities inherent in the banking system). Script cheque facilities are predominantly used by overseas customers, and jurisdictional and corruption risk are inherently higher in these circumstances. Failure to verify source of funds/wealth, along with ineffective enhanced due diligence (EDD) measures, could result in the movement and cleaning of criminal monies, across jurisdictions. As this activity occurs outside of traditional banking system, it could obscure the audit trail to assist in law enforcement and enforcement activity

- MSB facilities offered within the casino sector have inherent risks in relation to the movement of foreign currency across jurisdictions, particularly where the customers are from overseas. Failing to apply robust anti-money laundering and counter terrorist financing procedures may result in casinos permitting the movement of cash (in foreign currency) from high risk jurisdictions, jurisdictions that register highly on the corruption perception index, or from individuals who carry a high risk of money laundering, such as PEPs. This effectively facilitates money laundering

- Failure to effectively train employees and senior management in policies and procedures for MSB activities, PEPs and cheque cashing facilities, including ongoing monitoring, record keeping, and to update such training. This leaves casino operators vulnerable to criminal monies being laundered through the sector

- Failure to monitor TITO transactions in electronic gaming or gaming machine winnings could allow criminals to launder criminal monies through the casino. Employees' failure to conduct customer due diligence checks could result in criminal spend through TITO facilities. This inherent risk is further compounded when the cashing out of winnings from TITO is permitted through ATR machines. The removal of customer interaction at both the play and cash out stages of gaming may result in operators missing requirements in the Regulations for EDD in relation to high risk customers, CDD for those customers it has formed a business relationship with, and those customers approaching the monetary CDD threshold, which may result in criminally derived funds being laundered through the sector

- There is evidence which suggests that criminals have exploited this vulnerability to launder the proceeds of crime. Where the means of payment vulnerability of TITO in a threshold casino has been exploited, it largely relates to there being an absence of human intervention, or AML controls not being effectively implemented across the casino.

Risk rating

Due to the continued frequency of cash and cash equivalent transactions (TITO, MSB facilities and script cheques) being used to launder criminally derived funds this area receives a rating of higher.

The vulnerabilities received a rating of **higher** due to the high likelihood of occurrence and high impact of the risk materialising.

Gaming machine technical and gambling software

Manufacturers and suppliers	Overall rating
	Low

Control vulnerabilities of manufacturers and suppliers

Vulnerabilities	Controls
Manufacturers and suppliers failing to comply with the Act, POCA, TACT and LCCP requirements This vulnerability relates to manufacturers or suppliers failing to apply controls to mitigate the risk of ML/TF.	• Employees are trained to understand and recognise ML/TF risks to the business • New product development includes the consideration of compliance requirements, ML/TF risks and impact, prior to placement of the product in the market • Business-to-business entities have robust commercial contracts in place that ensure that the risks and impact of ML/TF are equally considered when conducting business • Businesses that supply and provide back office support are capable of identifying and reporting unusual data patterns, trends or incidents to business-to-customer business partners, which enables them to conduct an assessment of the data and discharge any duties to report any suspicions to regulators or law enforcement • A senior manager is identified as having responsibility for the completion of any risk or impact assessment of ML/TF for the business and report accordingly to regulators and law enforcement of any suspicions.

Consequences

- Manufacturer, supplier, gambling software licensees fail to comply with the Act, POCA, TACT and LCCP through poor policies, procedures and controls, monitoring, training, embedding published learning and risk assessments, resulting in non-compliance. The Commission will take action where it identifies non-compliance. This may range from action plans through to review and/or revocation of personal and/or operating licences. Failure to follow good practice as required by ordinary code 2.1.2 will be a material factor considered in any decision regarding review and/or revocation of personal and/or operating licences

- Business-to-business operators fail to train employees in anti-money laundering and counter terrorist financing as they regard it as irrelevant to their business because they have no direct interaction with the public. This leads to unusual data patterns not being reported to their customer facing business partner (B2C) including suspicious data not being reported to law enforcement and the Commission. It may also result in poorly constructed software which does not minimise risks to the licensing objectives

- Software and new products developed by business-to-business operators fails to take into account the risks of ML/TF, as they introduce the software and new products to the market. Software and new products may be introduced to the gambling market which provides opportunities to customers to launder monies from criminal activity and fund terrorist activity in the UK

- Business-to-business and business-to-customer operators fail to have sufficiently clear commercial contracts which set out responsibilities in relation to compliance with the Act, and the prevention of ML/TF, which results in adverse risks and impacts not being sufficiently mitigated in the marketplace

- Business-to-business data producing anonymous but unusual transactional patterns or trends and failing to report this to business-to-customer partners, regulators or law enforcement.. Unusual transactional data and trends may be difficult to link to individual customers, however, vital information is being overlooked which may have assisted operators, regulators and law enforcement

- Failing to have sufficient senior management oversight in business-to-business activities for the prevention of ML/TF, leading to ineffective and unmonitored policies, procedures and controls being relied upon.

Risk rating

Manufacturers or suppliers failing to comply with the Act, POCA, TACT, LCCP and technical standards receives a rating of **low**.
This is based on the low likelihood and low impact in the manufacturers and suppliers sector.

Licensing and integrity vulnerabilities of manufacturers or suppliers

There are no licensing and integrity vulnerabilities for manufacturers and suppliers which could have a significant impact on the gambling industry or are likely to occur. There is no evidence to suggest that gaming machine manufacturers have been acquired by organised crime for the purpose of laundering criminal funds. Furthermore, there are no known cases involving staff employed by gaming machine manufacturers manipulating machines, although there are isolated cases involving gaming machines being targeted by criminals while in transit, in order to manipulate the machine hardware/software for personal gain, and isolated cases of software developers ignoring impact and compliance considerations when developing new software and introducing it to the market with potentially adverse effects.

Customer vulnerabilities in manufacturers or suppliers

Manufactures and suppliers of gaming machines or software do not have direct interaction with the end users of their products. They are business-to-business providers and, consequently, are not exposed to the same customer risks as gambling operators.

However, a customer using a gaming machine to defraud the gambling business is a matter which affects gaming machine manufacturers and the Commission has seen minor cases where malicious software has been used to commit fraud.

In cases where customers have attempted to defraud the gambling business using gaming machines, the operator and the manufacturer work together to ensure that any instances are investigated and the risks are removed or reduced to an acceptable level. Operators and manufacturers will take active steps to do this, given the commercial impact should they fail to do so.

Product vulnerabilities in manufacturers or suppliers

Vulnerabilities	Controls
• Gaming machines used to launder the proceeds of crime, including criminal spend • self-service betting terminals (SSBTs) used to launder the proceeds of crime, including criminal spend • TITO and ATR facilities being used to launder the proceeds of crime, including criminal spend • Failing to consider compliance risks in relation to ML/TF in the development of new products prior to placement in the marketplace.	• Gaming machine manufacturers must comply with the gaming machine technical standards (GMTS), which provide some protection against money laundering vulnerabilities • Automatic alerts and/or triggers (for example, redemption and churn level limits on TITO/ATR/SSBT enabled machines) • TITO/ATR/SSBTs can act in part as a control if effectively monitored (although they are also considered as vulnerabilities) • Some gaming machines will reject dyed notes, as well as fraudulent notes and coins • New software is subject to rigorous gateway development processes, that includes compliance scrutiny, and identifying the risks and impact of ML/TF associated with the new product.
Consequences	
• Manufacturers and suppliers would not necessarily be in a position to detect 'reasonable grounds for knowing or suspecting' ML/TF linked to an identifiable customer, recognising that they do not have access to all the information available (including customers details). However, they are in a position to identify unusual data or patterns and alert their business-to-customer partners, regulators and law enforcement • TITO-enabled gaming machines are not currently monitored in real time, making it difficult to detect money laundering as it takes place and increasing the risk of it proliferating across other gambling operators and sectors	

- There is opportunity for manufacturers, suppliers and operators to work together to develop a standardised approach to alerts and triggers and to report any information promptly to regulators and law enforcement

- New software development should include compliance oversight to assist with thorough identification of opportunities inadvertently created for ML/TFML/TF to occur in the marketplace, taking corrective steps before release.

Risk rating

Gaming machines, TITO and ATRs used to launder the proceeds of crime, including criminal spend: **Low**
Self-service betting terminals (SSBTs) used to launder the proceeds of crime, including criminal spend: **Low**
Software development creating opportunities to launder the proceeds of crime and for terrorist financing in the gambling market**: Low**
This is based on the low likelihood and impact in the manufacturers and suppliers sector as B2Bs, while being mindful that it will affect their B2C partners.

Means of payment vulnerabilities in manufacturers or suppliers

Vulnerabilities	Controls
• TITO used in conjunction with ATR machines • SSBTs used to launder the proceeds of crime, including criminal spend • It provides opportunity for manufacturers, suppliers and retailers to work together to better develop robust controls (although this is a machine operator risk).	• Gaming machine manufacturers must comply with the GMTS which provide some protection against money laundering vulnerabilities • Automatic alerts and/or triggers, for example, those in relation to redemption and churn level limits on TITO/SSBT/ATR enabled machines. This data can used to minimise risks by identifying unusual spikes in play or markets • Whilst it is recognised that alerts, triggers and similar technologies have the potential to mitigate the risk associated with machine products, effective staff intervention to determine whether an alert is valid or not is essential.

Consequences

- Money laundering is unlikely to be identified by a gaming machine manufacturer in isolation. Gaming machine manufacturers are not necessarily in a position to identify 'reasonable grounds for knowing or suspecting' where money laundering is concerned, but could identify unusual data or patterns of play

- The information available (i.e. machine transaction data) does not identify the customer and/or any behavioural factors which may inform 'reasonable grounds for knowing or suspecting' taking place in the physical environment, therefore staff interaction on premises is an essential element in mitigating the risks associated with machines

- TITO-enabled gaming machines or ATR machines are not currently monitored in real time, making it difficult to detect ML/TF as it takes place

- There is opportunity for manufacturers, suppliers and operators to work together to develop a standardised approach to alerts and triggers, and how to report incidents when identified.

Risk rating

TITO used in conjunction with ATR machines: **Low**
SSBT used in conjunction with ATR machines: **Low**
This is based on the low likelihood and impact in the manufacturers and suppliers sector being a B2B, however, it will affect their B2C partners.

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

Lotteries (remote and non-remote) incl National Lottery	Overall rating
	Low

Control vulnerabilities in the lottery sector

Vulnerabilities	Controls
• Lottery operators failing to comply with the Act, POCA, TACT, LCCP and not implementing good practice as required by ordinary code 2.1.1 • This vulnerability relates to lottery operators failing to apply controls to mitigate the risk of ML/TFML/TF	• Stakes to participate in lotteries remain low, and statutory limits prevent larger stakes being introduced by operators • Staff are trained to identify ML/TFML/TF risks in gambling • Instances of money laundering are likely to be criminal spend in low monetary transactions, due to the stakes offered and statutory monetary controls.

Consequences

- Non-remote and remote lottery operator fails to comply with the Act, POCA, TACT and LCCP through poor policies, procedures and controls, monitoring and training; and failing to embed published learning and risk assessments, resulting in non-compliance. The Commission will take action where it identifies non-compliance. This may range from action plans, through to review and/or revocation of personal and/or operating licences. Failure to follow good practice as issued by the Commission under ordinary code 2.1.2 will be a material factor in any decision regarding the action taken regarding the review and/or revocation of personal and/or operating licences
- The nature of the sector, including the low stakes and frequency, largely controls the risk of ML/TFML/TF in the sector
- Although there is only minor evidence of criminal spend in this sector, lottery operators should continue to acknowledge and better understand the risk of ML/TFML/TF in the sector
- There Commission is unaware of any instances of 'traditional' money laundering through the licensed GB lottery sector, including through the National Lottery.

Risk rating

Lottery operators failing to comply with the POCA, TACT, LCCP and Commission guidance : **Low**

Licensing and integrity vulnerabilities in the lottery sector

Vulnerabilities	Controls
• Lottery operators acquired by criminals as a means to launder criminal funds • There is no evidence to suggest that applicants for a lottery licence are fronted by criminal enterprises. The vulnerability is relevant to the National Lottery, where a retailer who offers National Lottery products potentially allows the products to be exploited for criminal purposes. This risk assessment does not consider the risk of the National Lottery being taken over by criminals.[29]	• The Commission's suitability process assesses prospective and current licensees against a range of factors to ensure that the activities are carried out in a way that minimises the risks to the licensing objectives • The Commission independently assures itself that controls are robust • The National Lottery operator takes steps to prevent fraud, for example, the establishment of a dedicated security team who monitor transactions, staff vetting and the implementation of security standards • Small society lotteries must register with their local authority and meet a range of requirements set out by the local authority to minimise risk • The Act sets out requirements relating to stake, prize limits and proceeds for society lotteries, which minimises risks.

[29] More information on National Lottery licensing

Consequences
• There are a small number of isolated cases where a licensed lottery has been run unlawfully and the proceeds of the lottery have been misused • Controls (both direct and indirect) appear to be effective in mitigating the licensing and integrity vulnerability from being exploited • There is nothing to suggest lotteries are being run as ML/TF vehicles by organised crime.
Risk rating
Lottery operators acquired by criminals as a means to launder criminal funds Based on the impact and likelihood of this vulnerability occurring, it receives a rating of **low**.

Customer vulnerabilities in the lottery sector

Vulnerabilities	Controls
• Anonymous customers laundering the proceeds of crime (non-remote lotteries only) • False or stolen identity documentation • Customers not physically present (remote lotteries only)	• Licence condition 12.1.1 places an obligation on lottery operators to complete a ML/TFML/TF risk assessment at least annually • LCCP ordinary code 5.1.5[30] places obligations on non-commercial society lotteries and external lottery managers (ELMs) to minimise fraud • The Act sets out requirements relating to stakes, prize limits and proceeds for small society lotteries, which can be a mitigating factor • Customer identity is verified in most cases where lottery prizes of significant value are claimed • The National Lottery takes steps to prevent fraud, for example, a security team who monitor transactions, online controls, staff vetting a the implementation of security standards • The nature of the sector, including the low stakes and frequency of play, largely mitigate the risk of ML/TFML/TF in the sector.
Consequences	
• There is limited evidence of anonymous customers spending the proceeds of crime in the lottery sector • Fraudulent or stolen identities being used when claiming significant prizes, which may lead to criminal spending in this sector • The impact on the National Lottery, particularly in relation to good causes and reputation, would be significantly higher compared to other types of lotteries, should criminal spending be identified in this sector.	
Risk rating	
Low overall	
Society lotteries Anonymous customers (non-remote only): **Low** False or stolen identity documentation: **Low** Customers not physically present (remote only): **Low**	
National Lottery Anonymous customers (non-remote only): **Medium** False or stolen identity documentation: **Low** Customers not physically present (remote only): **Medium** These ratings reflect the greater reputational impact of the National Lottery, based on the medium likelihood and impact of occurrence.	

[30] Ordinary code provision 5.1.5 Mailing of lottery tickets, All lottery licences
1) With a view to minimising the risk of fraud, licensees who are non-commercial societies or external lottery managers should adopt one or more of the following measures:
a) prohibit the unsolicited mailing of tickets to non-members of the promoting society
b) limit the value of tickets sent to any one address which is not that of a member of the promoting society to £20
c) maintain records of tickets distributed and not returned.

Product vulnerabilities in the lottery sector

Vulnerabilities	Controls
• Scratch cards, interactive instant win and draw-based games used to spend the proceeds of crime	• Licence condition 12.1.1 places an obligation on lottery operators to conduct a risk assessment in respect of ML/TF • The Act sets out requirements relating to stakes, prize limits and proceeds for small society lotteries, which can be a mitigating factor • The nature of the sector, including the low stakes and frequency largely mitigate the risk of ML/TF in the sector • With National Lottery products, winners of the highest prizes are identified and verified[31] • In the remote sector, customers need to register and provide their details, which are then verified by the operator • For draw based games, the low stakes and prizes, the time lag between wagering a stake and the result, lower odds and customers' primary motivation for purchasing lottery products (i.e. contributing to charitable causes), are factors which further mitigate the risk.
Consequences	
• There is minimal evidence of this vulnerability being exploited in relation to criminal spend • Scratch cards and interactive instant win games, while posing a greater risk than draw-based games, do not present significant risks due to limited evidence of money laundering in the sector.	
Risk rating	
Risk rating: **Low** Scratch cards/interactive win games/draw based games Based on the likelihood and impact of this vulnerability occurring, it receives a rating of low.	

Means of payment (transaction) vulnerabilities in the lottery sector

Vulnerabilities	Controls
Cash transactions (non-remote only)	• The lotteries sector must comply with the Act, POCA, TACT, LCCP and the Commission's AML advice under ordinary code 2.1 • Limits on prizes and proceeds of society lotteries and low stakes are factors that mitigate the risk of money laundering • Many lotteries require customers who win the largest prizes to have their identity fully verified • The National Lottery takes steps to identify and verify the identity of winners of the top prizes.
Consequences	
• There is minimal evidence of criminals using criminal proceeds to purchase lottery products • Current stakes and prizes, coupled with the controls available in the sector, are mitigating factors to prevent ML/TF.	
Risk rating	
Risk rating: **Low**	

[31] For National Lottery prizes, customers can claim up to £500 in cash from some retailers. Prizes over £500, up to and including £50,000, must be claimed from designated post offices, at a National Lottery regional centre, or by post, where the customer's identity is verified.

Remote: Casinos

Remote casino sector	Overall rating
	Higher

Control vulnerabilities in the remote casino sector

Vulnerabilities	Controls
Remote casino operators failing to comply with the Act, POCA, TACT, the Regulations (inclusive of MSB activities if offered) and LCCP requirements This vulnerability relates to casino operators failing to apply controls to mitigate the risk of ML/TF	• As part of the regulated sector, remote casinos must comply with the Act, POCA, TACT, the Regulations and LCCP • Senior management must appoint a nominated officer, comply with requirements in the Regulations to prevent ML/TF, comply with requirements under POCA including reporting known or suspected ML/TF activity via SARs, provide adequate training to employees, conduct risk assessments of ML/TF and report to their board annually on the businesses' AML performance • Remote casino operators must also appoint a board member (or equivalent if no board exists) with responsibility for oversight of AML policies and procedures within the business, in compliance with the requirements of the Regulations • CDD and EDD checks and monetary limits must be complied with, including the verification of customers' identities and source of funds and wealth checks, which should limit exposure to ML/TF • Adequate PEP monitoring should minimise exposure to corrupt funds and jurisdictional risk • Automated system triggers assist in identifying and reporting suspicious transactions involving customers • Effectively implemented policies, procedures and controls, as well as effective risk assessments (and revision thereof), monitoring and training should minimise the risk of money laundering • Persons in key positions who undertake specified roles to mitigate the risk of money laundering are fit and proper • Where there are instances of concerns about staff integrity, operators will take appropriate action. Where the staff are licensed by the Commission, we may consider the revocation or suspension of personal licences • The risks associated with innovation in products or payment methods are assessed for any impact on the AML requirements and controls are put in place to effectively mitigate any risks posed by such innovation • Casinos must comply with the Regulations, including in relation to MSB activities such as foreign currency exchange and the transfer of monies, to minimise the risk of ML/TF • Account-based play enhances the operators' ability to conduct CDD, which decreases the risk of ML/TF in the sector • Operators effectively monitor the sanction lists and act to mitigate risk of sanctioned monies entering the UK financial sector.

Consequences

- Having recently conducted thematic compliance assessments of the remote casino sector, the Commission is not assured by the remote casino sector's compliance with the Act, POCA, TACT, the Regulations, LCCP and Commission guidance. The evidence gathered during the assessments demonstrated frequent and systemic failures in complying with the legal requirements. This non-compliance significantly increases the likelihood of vulnerabilities being exploited in the sector

- Remote casino operators fail to comply with the Act, POCA, TACT, the Regulations (inclusive of MSB activities, if offered) and LCCP through poor policies, procedures and controls, monitoring and training, and failing to embed published learning and relevant risk assessments, resulting in non-compliance.
- The Commission will take action where it identifies non-compliance. This may range from action plans through to formal review and / or revocation of personal and /or operating licences. Failure to follow good practice as advised by the Commission through guidance under ordinary code 2.1.1 will be a material factor in any action we take in relation to the review and / or revocation of personal and/or operating licences.

Risk rating

Risk rating: **Higher**

- Remote casino operators failing to comply with the Act, the Regulations, POCA, TACT, LCCP and guidance issued by the Commission

Licensing and integrity vulnerabilities in the remote casino sector

Vulnerabilities	Controls
• Operators acquired by criminals as a means to launder criminal funds • Employees colluding with criminals to launder criminal funds	Licensed individuals are subject to both general and individual licence conditions under sections 75 and 77 of the Act (monitoring ongoing suitability), including conditions relevant to the review and revocation of individual licences: • The Commission assesses new licence applications (including personal licence applications), and current licence holders against a range of factors to ensure that the licensees are suitable and the activities they carry out are conducted in a way which minimises the risks to the licensing objectives. The Commission has robust and independently assured controls to mitigate risks identified through the licensing process and the likelihood of it being exploited • The Commission licenses individuals in qualifying positions, and it is the responsibility of the operators to limit any risks of employee collusion. Compliance with licence condition (LCCP) 5.1.1 and 5.1.2 – cash handling further mitigates the risk of employees colluding with others (either employees or customers) within remote gambling. The exception to this risk is peer-to-peer gaming, where a lack of appropriate controls fails to prevent customer-to-customer collusion • Where there are concerns about the integrity of a staff member, it is expected that remote operators will act appropriately to investigate and take action where necessary so as to minimise the risks to the licensing objectives.

Consequences

- Vulnerabilities relating to the risk of organised criminals infiltrating and taking over remote businesses have materialised, to the extent that attempts appear to have been made by organised crime to acquire gambling businesses as a means to launder criminal proceeds. However, the Commission's controls have been robust and any attempt by organised criminals to do so have been prevented. This vulnerability is recognised by FATF and is also discussed in the UK NRA, so constant vigilance must be maintained

- Vulnerabilities relating to remote employees in key positions acting in collusion with criminals to launder criminal funds have materialised. The Commission has evidence of employees colluding with customers to launder criminal proceeds. Serious cases have resulted in licence reviews and subsequent revocation of the licences of employees in qualifying positions and of operating licences. Properly applied controls by operators can mitigate the risk of employee collusion.

Risk rating

Risk rating: **medium-to-higher**

- Operators acquired by criminals as a means to launder criminal funds: medium-to-higher
- Employees colluding with criminals to launder criminal funds: medium-to-higher

Customer vulnerabilities in the remote casino sector

Vulnerabilities	Controls
• Customers breaking up large amounts of cash into smaller transactions in order to minimise suspicion and avoid CDD, registering multiple accounts. Also used for online bonus abuse • Customers not physically present for identification purposes • False or stolen identity documentation used to bypass controls in order to launder criminal funds • Easy accessibility to multiple remote casinos • Customers from high risk jurisdictions using casino facilities to launder criminal funds • Customers who appear on international sanctions lists laundering illicit funds • PEPs using casinos to clean corrupt funds The Regulations identify instances where the customer is not physically present for identification purposes as high risk, except where adequate safeguards are in place. Furthermore, the use of false and stolen identity documentation is seen by FATF and the European Commission as an increasing trend. The ease of accessibility to a large number of remote operators is seen as another advantage to money launderers or terrorist financers. The first four vulnerabilities receive a risk rating of higher. The remaining three vulnerabilities receive a rating of medium-to-higher. It is important to also recognise the following customer vulnerability which has emerged in the sector following the implementation of the Regulations: • Domestic PEPs Enhanced customer due diligence and enhanced ongoing monitoring of domestic PEPs became a requirement with the enactment of the Regulations in June 2017. The Commission will be assessing the sector's compliance with this requirement and will provide further comment on this risk in the next version of this assessment.	• All remote casino operators must comply with the Act, POCA, TACT, the Regulations, and LCCP, and should follow Commission guidance[32] • The Regulations require operators to take specific and adequate measures to compensate for the higher risk where a customer is not physically present for identification purposes, except where adequate safeguards are in place. Measures to identify and verify customers begin with the registration process and initial screening measures, authentication and verification. Remote operators use a range of software which enhances their ability to verify a customer's identity. More sophisticated software which risk scores a customer on the basis of their historical play, transactions and payment methods are further used to prevent the risk of ML/TF activity. Remote customers must have a gambling account and operators have measures in place to prevent duplicate accounts being opened. Controls concerning customers' accessibility to multiple remote gambling operators/platforms are largely dependent on each individual operator • Remote casinos have effective controls to manage high risk customers. The approach to PEPs, customers from high risk jurisdictions and customers who appear on international sanctions lists varies from operator to operator. Some remote operators develop and maintain awareness of countries which are considered to have a high risk of corruption and will check customers against databases as part of the CDD process. However, this is not widespread across the remote casino industry.

Consequences
• The Commission is not assured by the remote casino sector's compliance with the Regulations (inclusive of MSB activities), the Act, POCA, TACT, LCCP or Commission guidance, having recently conducted compliance assessments that evidence frequent and systemic failures in the sector. This, therefore, significantly increases the likelihood of vulnerabilities being exploited by money launderers and terrorist financers. Account-based play means remote operators can have access to significantly more player data, for example, a full audit of transactions and details of IP addresses used. If used effectively, this data can reduce the ML/TF risks.

[32] A new version of the licensing conditions and codes of practice (LCCP) came into effect on the 31 October 2016. The new LCCP amended and added some requirements for operators in respect of crime, including anti-money laundering measures. For example, licence condition 5.1 – cash and cash equivalents, payment methods and services, new licence condition 12 - anti-money laundering and new ordinary code provision 7 – gambling licensees' staff. These conditions have further assisted in mitigating the risk of money laundering in gambling.

However, the Commission has evidence that some operators are better than others in identifying and mitigating these risks. The Commission also has evidence of money laundering through the remote casino sector

- Identity theft is a risk. It is possible for criminals to use false or stolen identity documentation to disguise their true identity, and thereby avoid being identified as high risk customers. It is becoming increasingly difficult to detect customers who use false or stolen identity documentation, due to the number of sophisticated techniques criminals employ and the broad range of nationalities the GB gambling market now attracts. An area of further development required by remote operators is where the name on the account is unrelated to the name on the payment method(s) used to fund it. There is evidence of money laundering through the remote sector using false or stolen identity documentation

- The Commission does not have significant evidence that PEPs, customers from high risk jurisdictions or customers on sanctions lists are laundering illicit funds through the remote sector. Nevertheless, the absence of robust controls within the sector more generally, and the internationally recognised higher risk associated with these vulnerabilities, means that issues are not being detected by the remote sector, thereby limiting their ability to identify and mitigate the vulnerabilities.

Risk rating

Risk rating: **Higher**

- Customer not physically present for identification purposes: **higher**
- False or stolen identity documentation used to bypass controls in order to launder criminal funds: **medium**
- Easy accessibility to multiple remote casinos: **higher**
- Customers from high risk jurisdictions using casino facilities to launder criminal funds: **medium**
- Customers who appear on sanctions lists laundering illicit funds: **medium**
- PEPs using casinos to launder corrupt funds: **medium**

Customers not present for identification purposes and their accessibility to multiple remote operators and accounts receives a rating of higher, as they are very likely to occur and have higher impact

Customers from high risk jurisdictions using casino facilities to launder criminal funds, customers who appear on international sanctions lists laundering illicit funds, customers using false and stolen identity documentation and PEPs using remote casinos receive a rating of medium as they have medium impact with medium likelihood.

Product vulnerabilities in the remote casino sector

Vulnerabilities	Controls
• Electronic roulette[33] • Peer-to-peer gaming (poker) B2C The vulnerability of peer-to-peer gaming (poker) is associated with the ability for customers to collude and deliberately 'transfer' funds to one another, sometimes referred to as 'chip dumping'. The Commission considers peer-to-peer gaming (poker) offered by remote casinos a higher risk product.	• Remote casino operators comply with the Act, POCA, TACT, the Regulations and licence conditions, and should act in accordance with the Commission's guidance on anti-money laundering under LCCP[34] ordinary code provision 2.1.1. Remote casino operators apply a risk-based approach to manage and mitigate ML/TF risks identified within their business • Remote casino operators comply with licence conditions 3.1.1, 3.1.2 and 3.1.3 where they provide facilities for peer-to-peer gaming but do not contract directly with all of the players using those facilities ('network operators') • Remote operators take steps to deter, prevent and detect collusion, as required by Technical Standard 11

[33] Compounded by ticket in, ticket out (TITO) technology and the use of automated ticket redemption machines (ATRs)
[34] A new version of the licensing conditions and codes of practice (LCCP) came into effect on the 31 October 2016. The new LCCP amends and adds some requirements for operators in respect of crime including anti-money laundering.

B2B and B2C gaming operators providing facilities for peer-to-peer gaming (poker) receives a rating of higher Electronic roulette facilities in non-remote casinos are licensed as remote gaming. The specific vulnerabilities associated with this product, including the use of TITO/ATR technology, are explained fully in the non-remote casino section of this report.	• When the customer is not physically present for identification purposes, operators must take specific measures to compensate for the higher risk, as required by the Regulations[35] (except where appropriate safeguards are in place) • Remote gambling requires a customer to have a gambling account. Registration processes, initial screening, authentication and verification of identity allows information obtained to be used to minimise risk • Remote casino operators use a range of software to enhance their ability to prevent fraudulent and duplicate accounts. Software which automatically monitors customer transactions and historical play helps prevent collusion between customers.

Consequences

- The Commission is not assured by the remote casino sector's compliance with the Act, Regulations (inclusive of MSB activities if offered), POCA, TACT, LCCP or Commission guidance, having recently conducted compliance assessments that evidence frequent and systemic failures. This, therefore, significantly increases the likelihood of vulnerabilities being exploited across the sector by money launderers and terrorist financers

- Some gambling operators licensed by the Commission are located in geographical areas outside of the UK that are characterised by poor anti-money laundering regulations, high levels of corruption, high levels of poverty, political instability or with significant crime or terrorist threats[36], although the numbers of operators licensed by the Commission who are located in these areas is relatively low

- FATF and Treasury identify criminal attempts at gaining control of gambling businesses as a vulnerability. The Commission's robust licensing process effectively mitigates the risk of operators being run by organised crime

- Vulnerabilities relating to the risk of remote casino operations being run by organised criminals have materialised to the extent that attempts appear to have been made by organised crime to acquire gambling businesses as a means to launder criminal proceeds. The Commission's controls have been robust and attempts by organised criminals to do so have been prevented to date

- The Commission is not convinced that the remote casino sector is applying the requirements to the rigour set out in the Act, Regulations, POCA, TACT, LCCP and specific guidance. Compliance evidence held by the Commission indicates widespread risks and issues of breaches of the AML requirements

- Product vulnerabilities have materialised in the sector and the relevant controls require improvements in effectiveness

- B2B and B2C peer-to-peer remote gaming (poker) lack effective controls to mitigate vulnerabilities being exploited for ML/TF purposes. With B2B poker, no one operator has full visibility of player data and gambling activity to enable the effective identification and investigation of suspicious activity.

Risk rating

Risk rating: **Higher**

- Peer-to-peer gaming (poker) B2C

Both B2B and B2C peer-to-peer gaming (poker) are rated as **higher** as they are assessed as having a high level of impact and likelihood, due to the absence of effective controls to mitigate the vulnerability being exploited.

[35] For example:
(a) ensuring that the customer's identity is established by additional documents, data or information;
(b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution which is subject to the money laundering directive;
(c) ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution

[36] The Commission will need to be alert to new methods of financing gambling businesses such as crowdfunding. New, novel and contentious forms of funding present new risks, for instance not being able to identify the ultimate beneficial owner.
Similarly, the casino sector is finding novel ways to attract high value customers through the use of third parties, which raises concerns about the effectiveness of relevant AML controls.

Means of payment vulnerabilities in the remote casino sector

Vulnerabilities	Controls
The highest rated vulnerabilities relating to means of payment within the remote casino sector are: • E-wallets • Pre-paid cards These vulnerabilities create difficulties in identifying where funds for gambling originate. It is important to identify the following means of payment vulnerability which could emerge in the sector: • Digital/cryptocurrencies Alternative currencies are recognised as an emerging means of payment vulnerability, however, the use of digital currencies has only recently begun to emerge within the remote sector. The Commission, however, recognises the higher risk of impact associated with digital currencies should their use become more prevalent in remote gambling. • Decentralised platforms, crowdfunding, blockchain and FinTech These are new technological solutions providing faster, more efficient financial transactions, capital raising methods or which provide additional privacy for customers' information along the transaction pathway. The Commission will assess what, if any, ML/TF risks these new technologies create, and will provide further commentary in the next version of this assessment.	• Operators must comply with the Act, Regulations, POCA, TACT and licence conditions, and should take into account the Commission's advice on POCA under ordinary code provision 2.1.1 [37]. Effective policies, procedures and controls must be in place to manage and mitigate the risk of ML/TF. Additionally, LCCP licence condition 5.1.2 places further obligations on remote operators in relation to the payment services they use • When the customer is not physically present for identification purposes, a remote casino should take measures to compensate for the higher risk (except where appropriate safeguards are in place). For example: (a) ensuring that the customer's identity is established by additional documents or information; (b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution which is subject to the money laundering directive; and (c) ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution • Ongoing monitoring of business relationships, including scrutinising transactions throughout the course of the relationship including, where necessary, the source of funds or wealth • Access to player data and assessment of customers on the basis of their historical play and transactions, which may include source of funds checks.

Consequences

- The Commission is not assured by the remote casino sector's compliance with the Act, Regulations (inclusive of MSB activities), POCA, TACT, LCCP and Commission guidance, having recently conducted compliance assessments that evidence frequent and systemic failure in the sector. This significantly increases the likelihood of vulnerabilities being exploited across the sector by money launderers and terrorist financers

- The remote casino sector, and the associated vulnerabilities of e-wallets, being used as a means to introduce criminal funds into the gambling industry have so far been realised in a limited way (evidenced in the data analysed), although FATF recognise the ML/TF risk associated with using remote accounts in conjunction with land based premises and e-wallets to move cash. It remains a risk in the GB gambling market. The use of such payment methods makes it difficult for the operator to identify the source of funds of the customer. The use of e-wallets and pre-paid cards to launder money through gambling receives a rating of medium due to their current use within the industry

- The potential use of digital or crypto currencies as a means to launder criminal funds is relevant to this vulnerability. This risk is not currently prevalent, due to the volatility of digital or cryptocurrencies' value. The need to hack the computer file containing the digital currencies makes this unattractive to organised crime. However, this assessment highlights the potential for abuse within the GB gambling industry in the light of increased anonymity and difficulty in traceability for law enforcement investigations.

[37] A new version of the licensing conditions and codes of practice (LCCP) came into effect on the 31 October 2016. The new LCCP amends and adds some requirements for operators in respect of crime including anti-money laundering.

Risk rating
Risk rating: **Medium** E-wallets: Medium Pre-paid cards: Medium Digital/crypto currencies: Medium

Remote: Betting and bingo sectors

Remote betting and bingo sector	Overall rating
	Higher

Control vulnerabilities in the remote betting and bingo sector

Vulnerabilities	Controls
Remote betting and bingo operators failing to comply with the Act, POCA, TACT, LCCP and to follow Commission guidance under ordinary code provision 2.1.2 • This vulnerability relates to remote betting and bingo operators failing to apply controls to mitigate the risk of ML/TF. It is important to recognise the following control risk which has recently emerged in the remote betting sector: • Operators gambling directly and indirectly on their own products, in this case remote pool betting The Commission has evidence that an operator was playing directly and indirectly into their own pool to such an extent that they were wagering the most into the pool, winning the most from the pool and receiving a rebate on their wages from the company for monies staked, so that they broke even or made a profit. In order to guarantee the prizes in the pool and pay the rebates, the operator required continual investment by way of loans from the owners. This business model poses a risk to the remote pool betting control framework aimed at preventing ML/TF.	• The remote betting and bingo sectors are not part of the regulated sector, but must nonetheless comply with the Act, POCA, TACT, LCCP and should follow Commission advice under ordinary code provision 2.1.2 • Key positions, such as compliance functions, are licensed by the Commission and they must comply with requirements in POCA and TACT to minimise the risk of ML/TF. These requirements include reporting suspected or known suspicious activity by means of SARs, adequate training for employees, risk assessment of money laundering to the business and planning effective mitigation • Compliance with the Commission's technical requirements, such as KYC procedures (social responsibility code 3.9), EDD checks and monetary threshold limits, must be complied with. This is aimed at limiting the risk of exposure to money laundering by verifying identification and source of funds or wealth • Automated system triggers assist in identifying and reporting suspicious transactional behaviour of customers to operators • Implemented policies and procedures by operators should minimise the risk of money laundering through effective assessment, monitoring, training and revision of risk assessment • Instances where there are concerns of staff integrity, operators should act appropriately and take action where they see fit (social responsibility code 8.1.2) or, if licensed by the Commission, we may consider review or revocation of personal licences • Product or means of payment innovation risk is assessed for any impact upon money laundering requirements and implemented controls put in place to effectively mitigate any risks posed • Account based play increases the operators' ability to know their customer, confirm their details and verify their identification. By using an account based system this decreases the risk of ML/TF in the sector • LCCP requires contracts with 3rd party business relationships, for example social responsibility codes 1.1.2 and 1.1.3, to ensure standards are kept high by B2B partnerships in ensuring mitigation of money laundering risks.
Consequences	
• Remote betting and bingo operator fails to comply with the Act, POCA, TACT and LCCP through poor policies, procedures and controls, monitoring and training, also failing to embed published learning and risk assessment, resulting in non-compliance. The Commission will take action where it identifies non-compliance. This may range from action plans through to review and /or revocation of personal and /or operating licenses. Failure to follow good practice issued in guidance under code 2.1.2 will be a material factor in considering review and / or revocation of personal and/or operating licences.	
Risk rating	
Remote betting and bingo operators failing to comply with the AML & CTF requirements: **Higher**.	

Licensing and integrity vulnerabilities to remote betting and bingo operators

<table>
<tr><th>Vulnerabilities</th><th>Controls</th></tr>
<tr><td>The licensing and integrity vulnerability concerning the remote betting and bingo sector is as follows:

• Gambling operations run by organised criminals as a means to launder criminally derived funds.

This vulnerability received a rating of medium-to-higher.

It is important to recognise the following licensing and integrity risk which has emerged in the remote betting sector:

• Ultimate Beneficial Ownership (UBO) and seeding arrangements

When businesses apply to be licensed, or those already licensed, apply for a Change of Corporate Control (CoCC), it has emerged that companies incorporated in overseas jurisdictions with overseas UBOs are then attracting new shareholders who are expected to place liquidity (through a seeding arrangement) into the betting exchange. In the absence of information regarding the secondary shareholders adding liquidity to the betting exchange, the Commission will not be sufficiently assured regarding the source of wealth and funds. This potentially exposes the GB gambling market and consumers to the risk of ML/TF. This emerging risk has been revealed in the remote betting sector, however, sufficiently robust controls implemented by the Commission have so far prevented any applications or CoCC being granted under these circumstances. The Commission will keep this emerging risk under observation and report further in the next iteration of this risk assessment.</td><td>The Commission assesses new licence applications (including for personal licences), and current licensees, on a range of factors to ensure the licensee is suitable and the activities they carry out are conducted in a way which minimises the risks to the licensing objectives. The Commission has robust and independently assured controls to mitigate this vulnerability being exploited.[38]</td></tr>
<tr><th colspan="2">Consequences</th></tr>
<tr><td colspan="2">• The amendment to the Act in 2014 has exposed the Commission to a greater degree of risk in this area recognising that some gambling operators are located in geographical areas outside the UK, some of which could be characterised by poor governance, political instability or with significant criminal or terrorist threats.[39] This is supported by the number of remote betting applications where the Commission has questioned the integrity, ownership and provenance of funding into the business. At present there are low numbers of operators licensed by the Commission who are located in areas characterised by the this

• The number of remote betting applications where the Commission has reason to question the integrity, ownership and provenance of funding for businesses is increasing, and this has been linked to the requirement for overseas operators to be licensed by the Commission

• Attempts have been made by organised crime to acquire online gambling businesses, potentially as a means to launder criminal proceeds or finance terrorist activity. The risk rating applied is higher, recognising the high impact. The Commission's controls relating to this risk are robust. A number of unsuitable applicants have been identified and declined for licence applications. On occasions adverse information has been identified at a later stage and licences revoked accordingly

• Integrity of both controllers and staff employed within this sector have, at times, been compromised leading to dismissal and revocation of Personal Management Licences issued by the Commission.</td></tr>
<tr><th colspan="2">Risk rating</th></tr>
<tr><td colspan="2">Risk rating: organised crime being licensed medium-to-higher</td></tr>
</table>

[38] A new version of the licensing conditions and codes of practice (LCCP) came into effect on the 31 October 2016. The new LCCP amends and adds some requirements for operators in respect of crime including anti-money laundering.
[39] The Commission will need to be alert to new methods of financing gambling businesses such as Crowdfunding. New, novel and contentious forms of funding present new risks, for instance not being able to identify the ultimate beneficial owner.
Similarly, the casino sector is finding novel ways of attracting high value customers through the use of third parties (sometimes referred to as junkets). The Commission will need to satisfy itself that current controls filter down to these third parties in order to meet the required level of protection for consumers.

Customer vulnerabilities in the remote betting and bingo sector

Vulnerabilities	Controls
The customer vulnerabilities concerning the remote betting and bingo sector are the following: • Customer not physically present for identification purposes • False or stolen identity documentation used to bypass controls in order to launder criminal funds • Accessibility to multiple operators • Customers from high risk or non-cooperative jurisdictions using remote facilities to launder criminal funds • Customers who appear on international sanctions lists laundering illicit funds • Customers who are citizens or residents of, or associated with, countries with a high score in Transparency International's Corruption Perceptions Index Where the customer is not physically present for identification purposes, it makes it more difficult for remote operators to know their customers, identify them and verify their identities. Furthermore, as indicated in the remote casino section, the use of false identity documentation is seen by FATF and the European Commission as an increasing trend in ML/TF. The ease of access to multiple remote operators can also provide an advantage to money launderers trying to avoid detection. These three vulnerabilities receive a rating of higher, and the remaining three receive a rating of medium-to-higher.	• All operators must comply with the Act, POCA, TACT and the LCCP[40], and take into account the Commission's advice on POCA under ordinary code provision 2.1.2 • Remote gambling requires customers to have a gambling account. Measures to identify customers require initial registration, screening, authentication and verification • Age verification checks are a further control. Acceptable forms of identity documents include: any identification carrying the PASS logo (for example Citizencard or Validate), a driving licence (including provisional licence) with photocard or a passport • Software which enhances the ability to validate a customer's identity and prevent identity fraud is used by many remote operators. Additionally, software which risk scores a customer on the basis of their historical play and transactions is used to help identify suspicious activity by customers • Remote gambling requires a customer to have a gambling account, and operators have controls in place to prevent duplicate accounts being opened by customers. • Parts of the industry maintain awareness of countries which are considered to have a high risk of money laundering or corruption and check customers from those countries against relevant databases to mitigate risk and comply with legislative obligations

Consequences

- There is evidence that controls within the remote betting and bingo sector are not effective in mitigating the risk of money laundering. Account-based play gives remote betting and bingo operators access to significantly more player data, for example, a full audit trail of transactions and details of the IP addresses of customers. It is apparent that some operators are better than others at identifying and mitigating risks and analysing data in order to identify money laundering activity

- FATF and the European Commission recognise identity theft as an increasing trend in ML/TF. It is possible for customers to use false or stolen identity documentation to disguise their true identities so as to avoid being identified as high risk customers. It is becoming increasingly difficult to detect customers who use false identity documentation due to the increasing sophistication of the documents being produced

- An area of further development for remote operators is where the name on the account is unrelated to the name used on the payment method(s) to fund the account. This increases the risk of ML/TF. There is evidence of money laundering through the remote betting and bingo sector facilitated by the use of false and stolen identity documentation

[40] A new version of the licensing conditions and codes of practice (LCCP) came into effect on the 31 October 2016. The new LCCP amends and adds some requirements for operators in respect of crime including anti-money laundering.

- There is currently no known significant evidence in the GB remote gambling market of customers from high risk or non-cooperative jurisdictions using remote facilities to launder criminal funds. There is also no know evidence of remote customers who appear on sanctions lists or customers who are citizens or residents of (or associated with) countries with a high score in Transparency International's Corruption Perceptions Index laundering illicit funds. Nevertheless, the absence of robust controls within the sector must be taken into account when assessing the likelihood of occurrence of this risk.

Risk rating

- Customer not physically present for identification purposes – **Higher**
- False or stolen identity documentation used to bypass controls in order to facilitate the laundering of criminal funds – **Higher**
- Access to multiple operators – **Higher**
- Customers from high risk or non-cooperative jurisdictions using remote facilities to launder criminal funds - **Medium-to-Higher**
- Customers who appear on international sanctions lists using illicit funds to gamble - **Medium-to-Higher**
- **Customers who are citizens or residents of (or associated with) countries with a high score in Transparency International's Corruption Perceptions Index - Medium-to-Higher**

Customers not present for identification purposes, false or stolen identity documentation and the accessibility of multiple remote operators receive a rating of higher due to being assessed as being very likely to occur and having a high impact. The remaining three vulnerabilities receive a rating of medium-to-higher due to being assessed as having a high impact, but a medium likelihood of occurring.

Product vulnerabilities in the remote betting and bingo sector

Vulnerabilities	Controls
• Bring your own device The product risk of Bring Your Own Device (BYOD) is identified in the non-remote betting sector of this assessment. However, customers using their own mobile devices to place bets on licensed premises is being used in remote gambling. This has emerged in both the on- and off-course non-remote betting sectors and, until further assessment of the product and its vulnerabilities, will be given a likelihood and impact rating of medium. BYOD is an evolution of SSBTs where consumers use their own device to place bets through non-account based play, either in off-course or at on-course premises Anonymity is a potential risk with BYOD, as a customer could place bets without needing an account or interacting with employees of the operator. The product could expose the remote betting operator accepting wagers to ML/TF risks. Robust transactional monitoring in real time should be adopted by operators when using this this innovation, which will allow swift and decisive identification of suspicious transactions or behaviour.	• Remote betting and bingo operators must comply with the Act, POCA, TACT, licence conditions, and should act in accordance with the Commission's guidance on anti-money laundering under LCCP[41] ordinary code provision 2.1.2. Remote betting and bingo operators apply a risk-based approach to manage and mitigate ML/TF risks identified within their business • Remote betting and bingo operators comply with licence conditions 3.1.2 and 3.1.3 where they provide facilities for gambling but do not contract directly with all of the players using those facilities ('network operators') • Remote betting and bingo operators must comply with licence conditions 5.1.1 cash and cash equivalents and 5.1.2 payment method services • Licence condition 3.9.1 requires a customer to have a gambling account. Registration processes, initial screening, authentication and verification of identity allows information obtained to be acted upon to minimise risk • Remote operators use a range of software to enhance their ability to prevent fraudulent and duplicate accounts. Software which automatically monitors customer transactions and historical play helps prevent collusion between customers.

Consequences	
• In the absence of human intervention or tracking software, the controls have the potential to be exploited by criminals seeking to launder criminally derived funds • Product vulnerabilities have materialised in the sector and the relevant controls require improvement • B2B and B2C remote gaming via 'network operators' can be vulnerable to a lack of effective controls to mitigate vulnerabilities being exploited for ML/TF purposes. It is incumbent upon the licensed operator to ensure they are complying with the Act, POCA, TACT, licence conditions and codes of practice.	
Risk rating	
Risk rating: **Higher** • B2B to B2C remote gaming via 'network operators' • BYOD (rated in non-remote betting) Both B2B and B2C gaming are rated as **higher** as they are assessed as having a high level of impact and likelihood, due to the higher likelihood of an absence of effective controls to mitigate the vulnerability being exploited through 3rd party providers.	

Means of payment vulnerabilities in the non-regulated remote betting and bingo sector

Within the remote betting and bingo sectors there is no clear product vulnerability which is exploited more than others, due to the nature of the industry, especially the use of account-based play. However, the Commission recognises the risk associated with remote business models and products where users are not known to one another and, additionally, there could be an absence of effective controls. However, non-anonymous peer-to-peer betting and mitigating controls are yet to be fully realised, however, it appears there is minimal evidence of abuse.

Vulnerabilities	Controls
The highest rated vulnerabilities relating to means of payment within the remote betting and bingo sector are: • E-wallets • Pre-paid cards These vulnerabilities create difficulties in identifying where the funds for gambling are coming from. It is also important to recognise the following means of payment vulnerability which could emerge in the sector: • Digital / crypto currencies Digital and crypto currencies are recognised as an emerging means of payment vulnerability, however, use of such currencies has not widely emerged within the sector and is graded as medium. The Commission however recognises the higher risk associated with these currencies if they were to be widely used within the sector, future iterations of the risk assessment will assess them in greater detail.	• All operators must comply with The Act, POCA, TACT, LCCP and should specifically take into account the Commission's advice on POCA as prescribed by LCCP ordinary code provision 2.1.2[42] Operators have suitable policies, procedures and controls in place to manage and mitigate the risk of ML/TF • LCCP licence condition 5.1.2 places further controls on remote operators around payment services • Most remote gambling requires an account, this gives the ability to access more player data and assess customers on the basis of their historical play and transactions, which can be used to prevent ML/TF • Method of payment used by customers will on a risk-sensitive basis require the assessment of the source of wealth and source of funds.

[42] A new version of the licensing conditions and codes of practice (LCCP) came into effect on the 31 October 2016. The new LCCP amends and adds some requirements for operators in respect of crime including anti-money laundering. For example, licence condition 5.1 – cash and cash equivalents, payment methods and services, new licence condition 12 - anti-money laundering and new ordinary code provision 7 – gambling licensees' staff. These conditions will further assist in mitigating the risk of money laundering in gambling.

Consequences

- Vulnerabilities of e-wallets being used as a means to place laundered funds into the gambling industry have not yet been realised, however, FATF recognises the ML/TF risk associated with this payment type. This payment methods makes it difficult for the operator to identify the source of funds. The use of e-wallets and pre-paid cards to launder money through gambling has received a rating of **medium** due to their current use within the industry and the theoretical risk that is evident.
- The potential use of digital or crypto currencies as a means to launder criminally derived funds is relevant to payment type vulnerabilities. Although latent at present, the prior use of such currencies by organised crime highlights the potential for abuse within the GB gambling industry. The vulnerability received a rating of **medium** at present, however, as previously stated, the Commission recognises higher risk associated with digital currencies if they were to be used within the sector. No evidence as yet is revealed that an operator can demonstrate they can effectively manage risk to do with the direct use of digital currencies.

Risk rating

Risk rating: **Higher**

- peer-to-peer betting

Both B2B and B2C peer-to-peer betting was rated as **higher** as they are assessed as having a high level of impact and likelihood due to the absence of effective controls to mitigate the vulnerability being exploited.

14 Methodology

14.1 We continue to adopt the same methodology as the previous version of the risk assessment. Our methodology defines risk to be the potential that an event, action, or series of events or actions will have an adverse effect on the Regulations, POCA, TACT, the Act's strategic objectives or the LCCP.

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

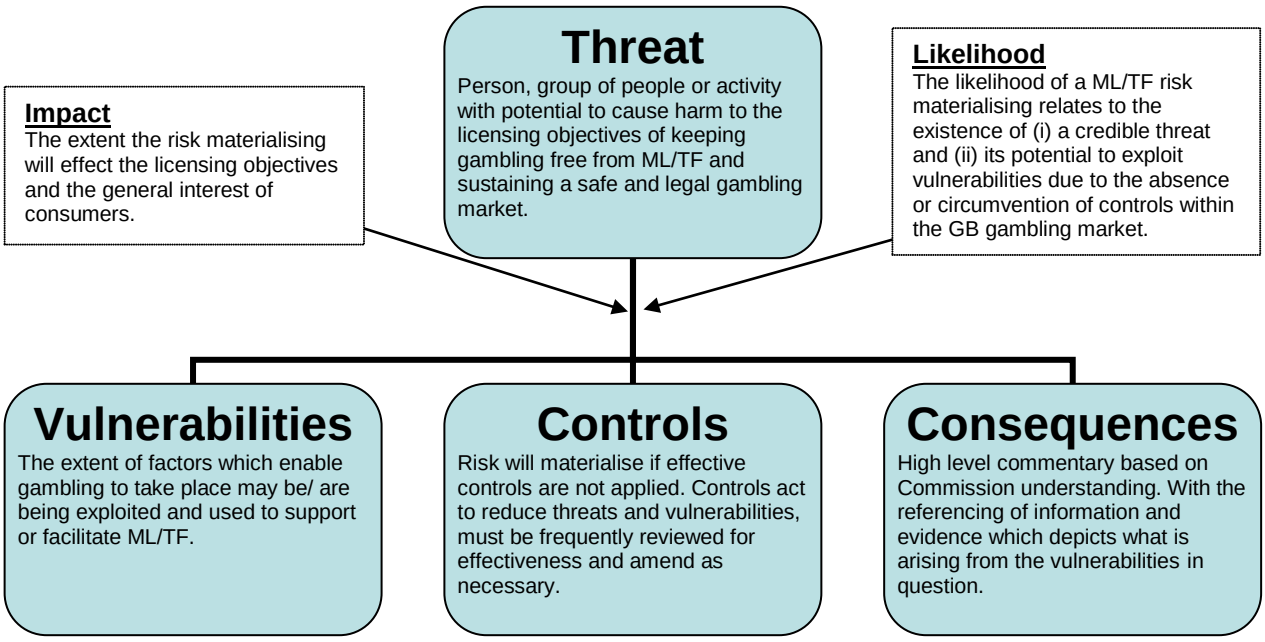
14.3 The Commission recognises the methodology used by the Financial Action Task Force (FATF) which sets the global standard for anti-money laundering and counter-terrorist financing and adopts a similar framework upon which to base our analysis.

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

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

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

The Commission's risk assessment methodology:



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

Application of approach:

<table>
<tr>
<td>Threats:

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

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

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

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

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

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

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

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

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

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

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