9 - Betting (Remote)

Table actions: Turn tags off

Sector rating

Sector	Previous overall risk rating	Current overall risk rating
Betting (Remote)	HIGH	HIGH

Existing inherent risk rating

There has been an increase in the risk levels for some of the inherent risks for the remote betting sector. For further information relating to the inherent risks (including vulnerabilities, consequences and controls), see our previous risk assessments:

- Money laundering and terrorist financing risk assessment within the British gambling industry: 2019 (PDF)
- Money laundering and terrorist financing risk assessment within the British gambling industry: 2018 (PDF)

Vulnerability	Risk	Previous likelihood of event occurring	Previous impact of event occurring	Current likelihood of event occurring	Current impact of event occurring	Change in risk
Operator Control	Operators failing to comply with prevention of money laundering and terrorist financing legislation and guidance	HIGH	HIGH	HIGH	HIGH	No change
Operator Control	Operators staking and winning directly and indirectly on their own products	MEDIUM	MEDIUM	LOW	MEDIUM	Decrease
Operator Control	Lack of competency of key personnel and licence holders which can then be exploited by criminals seeking to launder the proceeds of crime	HIGH	HIGH	HIGH	HIGH	No change
Operator Control	Inadequate/lack of 'know your customer' (KYC) checks resulting in criminals laundering criminal proceeds or risk of this occurring	MEDIUM	HIGH	HIGH	HIGH	Increase
Licensing and integrity	Gambling operations run by organised criminals to launder criminally derived funds	MEDIUM	HIGH	MEDIUM	HIGH	No change
Licensing and integrity	White label providers	HIGH	HIGH	HIGH	HIGH	No change
Customer	Customer not physically present for identification	MEDIUM	HIGH	HIGH	HIGH	Increase
Customer	False or stolen documentation used to bypass controls to launder criminally derived funds	MEDIUM	HIGH	HIGH	HIGH	Increase
Customer	Accessibility to multiple remote accounts	HIGH	HIGH	HIGH	HIGH	No change
Customer	Customers from high risk or non-cooperative jurisdictions using remote facilities to launder criminally derived funds	MEDIUM	VERY HIGH	HIGH	HIGH	Decrease
Customer	Customers who appear on international sanctions lists laundering criminally derived funds	VERY LOW	HIGH	LOW	HIGH	Increase

Vulnerability	Risk	Previous likelihood of event occurring	Previous impact of event occurring	Current likelihood of event occurring	Current impact of event occurring	Change in risk
Means of payment	E-wallets	N/A (no risk rating provided in previous risk assessment)	N/A (no risk rating provided in previous risk assessment)	MEDIUM	MEDIUM	N/A
Means of payment	Cryptoasset transactions	MEDIUM	MEDIUM	MEDIUM	HIGH	Increase
Means of payment	Pre-paid cards	MEDIUM	MEDIUM	HIGH	HIGH	Increase

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

Additional inherent risks

Peer to peer betting

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

‘Closed loop’ system

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

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

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

'High value' customer' schemes

This has been given a high risk rating as previously discussed. See the Casino (Remote) section for further information.

High monetary thresholds

There is substantial evidence that remote betting operators have high customer spending triggers in place before conducting any due diligence checks on customers. This means that for customers that do not hit this threshold, it has been found that only basic checks are being carried out i.e., proof of name, address, and date of birth. Operators are reminded that this is a potential breach of Licence Condition 12.1.1.(1) which requires that licensees must assess the risks of their business being used for Money Laundering (ML) and Terrorist Financing (TF). This is a high risk area.

Emerging risks

Unregulated betting events

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

Customer identity verification

Licence Condition 17 of the LCCP stipulates that online gambling businesses are not permitted to allow a customer to gamble before they have verified the customer's identity [21] . This LCCP change is consistent with our guidance to operators which states that operators need

to give due consideration to ‘whether it is necessary to do KYC or due diligence checks on the customer’ [22] . The Commission has seen evidence in the remote betting sector that licensees are asking for customer ID when a withdrawal request for winnings is submitted by the customer. From a Money Laundering (ML) perspective, this has been given an overall ‘high’ risk rating as it means that insufficient due diligence checks are being carried out early enough in the consumer’s gambling journey.

‘Smurfing’

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

‘Mule’ betting accounts

'Mule' accounts are the creation of online betting accounts via the misuse of personal details belonging to third parties. This can be done both with or without third-parties’ knowledge and their personal data can be used to open both online betting accounts and e-wallet accounts with payment service providers. Large numbers of mule accounts are typically controlled by individuals or groups for the purposes of placing large volumes of bets and or as well as to disguise who is placing the bets and or as well as disguise the sources of funds being gambled.

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

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

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

Mule accounts can be used to:

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

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

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

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

Case example 1:

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

Case example 2:

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

Case example 3:

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

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

1. newly opened accounts with a third party payment set-up
2. first and only bets placed using the accounts on this fixture
3. using total funds deposited to place the bets
4. disguising the main bet by creating an accumulator with short odds selection
5. taking an early cash-out before the settlement and (attempted to) withdraw their funds.

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

Politically exposed persons (PEP)

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

References

19 RUSI: Occasional paper: Play Your Cards Right: Preventing Criminal Abuse of Online Gambling (PDF opens in new tab) (accessed 7th March 2020, updated November 2019). Author: Anton Moiseienko.

20 For a list of high risk third countries see: European Commission: EU policy on high-risk third countries (opens in new tab) (accessed 6th July 2020, updated May 2020).

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

22 Duties and responsibilities under the Proceeds of Crime Act 2002 (updated October 2020, accessed December 2020).

23 FATF Guidance: Politically exposed persons (Recommendations 12 and 22)(PDF opens in new tab) (accessed 11th August 2020, updated June 2013).