6 - Casino (Remote)

Table actions: Turn tags off

Sector rating

Sector	Previous overall risk rating	Current overall risk rating
Remote Casino	HIGH	HIGH

Inherent risks

There has been an increase in the risk levels for the inherent risks for the remote casino sector. For further information relating to the inherent risks, including vulnerabilities, consequences and controls, 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
Licensing and integrity	Gambling operations run by organised criminals to launder funds	MEDIUM	HIGH	LOW	HIGH	Decrease
Licensing and integrity	White label providers	HIGH	HIGH	HIGH	HIGH	No change
Customer	Customer not physically present for identification purposes	HIGH	HIGH	HIGH	HIGH	No change
Customer	False or stolen identity documentation used to bypass controls to facilitate the laundering of criminal funds	MEDIUM	HIGH	HIGH	HIGH	Increase
Customer	Accessibility to multiple remote casinos	HIGH	HIGH	HIGH	HIGH	No change
Customer	Customers from high risk jurisdictions using casino facilities to launder criminal funds	LOW	VERY HIGH	MEDIUM	HIGH	No change
Customer	Customers who appear on sanctions lists laundering criminal funds	LOW	VERY HIGH	LOW	HIGH	Decrease
Customer	International politically exposed persons (PEPs) using casinos to launder illicit or criminal funds	MEDIUM	VERY HIGH	MEDIUM	HIGH	Decrease
Customer	Domestic PEPs using casinos to clean criminal funds identification & verification	MEDIUM	MEDIUM	LOW	MEDIUM	Decrease
Customer	Customers making numerous low-level transactions to minimise suspicion and evade CDD requirements at the threshold (smurfing)	HIGH	HIGH	HIGH	HIGH	No change
Customer	Use of third parties or agents to obscure the source or ownership of money gambled by customers & their identities	HIGH	HIGH	HIGH	HIGH	No change

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	Pre-paid cards	MEDIUM	MEDIUM	HIGH	HIGH	Increase
Means of payment	E-wallets	MEDIUM	MEDIUM	MEDIUM	MEDIUM	No change
Means of payment	Cryptoasset transactions	MEDIUM	MEDIUM	MEDIUM	HIGH	Increase
Product	Peer to Peer gaming (poker)-B2B and B2C	HIGH	HIGH	HIGH	HIGH	No change

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

Additional inherent risks

Organised crime gangs (OCGs)

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

Mule accounts

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

The decrease of international students residing in the UK (due to COVID-19) may have led to reductions in activity through those types of mule accounts, however UK resident [3] students remain vulnerable. There is the risk that OCGs may coerce vulnerable individuals

into becoming money mules, as has been observed in the US. This has been given a high risk rating due to both the likelihood and impact of it occurring within gambling and the high collateral impact upon victims. Linked to this risk area, please see the Betting (remote) section for further information regarding 'mule betting accounts'.

High monetary thresholds

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

'High value' customer schemes

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

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

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

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

interaction with all high value customers).

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

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

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

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

Failure to implement a 'closed loop' system

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

Emerging risks

Payment providers

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

High-stakes gambling/Feature buy-in slots

These are online slot games which allow players to stake significant amounts of money to access a bonus feature without playing the initial stages of the game. There is significant concern about this bonus feature as it appears to encourage higher stake gambling with reports that players can stake £1000+ at a time to directly access bonus features. There was evidence that one game was charging more than £3,000 to enter the bonus feature. As well as appearing to be potential breaches of the Remote Technical Standards (RTS) [12] , it also raises concerns regarding how customer due diligence (CDD) checks (or if needed, EDD checks) are carried out to ensure compliance with the Regulations if customers are permitted to play for high stakes in short periods of time as online games are instantaneous and can encourage fast, addictive play. All high-stakes gambling is susceptible to abuse because it is common for players to gamble with large volumes of cash, the source and ultimate ownership of which may not be readily discernible.

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

References

3 Gambling Commission data.

4 As required under Regulation 33(4) of the Regulations.

5 Gambling Commission data 2020.

6 Applicable to casino operators only.

7 Applicable to all other gambling sectors.

8 Applicable to casino operators only.

9 LCCP 12.1 (requires operators to conduct an assessment of the ML and TF risks posed in their business). Not applicable to gambling software and gaming machine technical licences.

10 Gambling Commission: Customer interaction-formal guidance for remote gambling operators (PDF) (opens in new tab). See section 2.18 and section 4 of the guidance (accessed 23rd June 2020, updated July 2019).

11 Gambling Commission news article: Betway to pay £11.6m for failings linked to 'VIP' customers.

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

13 Games warning for online operators (updated 17th January 2020, accessed 1st March 2020).