# 7 - Casino (Non-Remote)

**Table actions:** Turn tags off

| Sector | Previous overall risk rating | Current overall risk rating |
|---|---|---|
| Casino (Non-Remote) | HIGH | HIGH |

## Existing inherent risk rating

There has been an increase in the risk levels for some of the inherent risks for the non-remote casino sector. For further information relating to the inherent risks, including vulnerabilities, consequences and controls, 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 | Undermining of the Money Laundering Reporting Officer (MLRO) role which can intentionally/unintentionally lead to exploitation by money launderers | HIGH | HIGH | HIGH | HIGH | No change |
| 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 | LOW | HIGH | HIGH | HIGH | Increase |
| Operator Control | Lack of adequate and relevant due diligence checks conducted resulting in criminals laundering money | MEDIUM | HIGH | HIGH | HIGH | Increase |
| Licensing & Integrity | Gambling operations being acquired by organised crime to launder criminal proceeds | MEDIUM | HIGH | MEDIUM | HIGH | No change |
| Licensing & Integrity | Ultimate Beneficial Ownership | MEDIUM | HIGH | MEDIUM | HIGH | No change |
| Licensing & Integrity | Employees colluding with criminals | MEDIUM | HIGH | HIGH | HIGH | Increase |
| Licensing & Integrity | Individuals with known criminal records/or suspected criminal activities | HIGH | HIGH | HIGH | HIGH | No change |
| Customer | Customer from high-risk jurisdictions using casino facilities to launder money | MEDIUM | VERY HIGH | MEDIUM | HIGH | Decrease |
| Customer | Customers appearing on international sanctions list laundering corrupt or criminal funds | MEDIUM | VERY HIGH | LOW | HIGH | Decrease |
| Customer | International politically exposed persons (PEPs) using casinos to clean criminal funds | HIGH | VERY HIGH | MEDIUM | HIGH | Decrease |

| 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 |
|---|---|---|---|---|---|---|
| Customer | Domestic PEPs using casinos to clean criminal funds | MEDIUM | MEDIUM | LOW | MEDIUM | Decrease |
| Customer | False/fraudulently obtained or stolen ID docs used to bypass controls | MEDIUM | HIGH | MEDIUM | HIGH | No change |
| Customer | Customers breaking up large amounts of cash into small transactions to minimise suspicion and evade CDD requirements at the threshold (‘smurfing’) | HIGH | HIGH | MEDIUM | HIGH | Decrease |
| Customer | Use of third parties or agents to obscure the source or ownership of money gambled by customers & their identities | HIGH | HIGH | MEDIUM | HIGH | Decrease |
| Means of Payment | Cash Transactions | HIGH | HIGH | HIGH | HIGH | No change |
| Means of Payment | Casinos acting as money service businesses (MSBs) | HIGH | HIGH | HIGH | HIGH | No change |
| Means of Payment | TITO enabled gaming machines used to launder funds when used with ATR machine | HIGH | HIGH | MEDIUM | HIGH | Decrease |
| Product | Electronic roulette - when used with TITO & ATRs | HIGH | HIGH | MEDIUM | HIGH | Decrease |
| Product | Gaming Machines (all) | HIGH | HIGH | HIGH | HIGH | No change |
| Product | Peer to peer gaming (poker) B2C | HIGH | HIGH | HIGH | HIGH | No change |

# Additional inherent risks

## Cashless payments

The use of cashless payments in general has increased in popularity in recent years. This presents a risk where Money Laundering (ML) or Terrorist Financing (TF) could be facilitated using fraudulently obtained and stolen cards. Whilst there are controls in place through closed loop systems, this mitigation is wholly reliant on the operator and its employees' effective application and there is a monetary cap on each transaction, currently £45.

The associated risks with cashless payment include:

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

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

## Emerging risks

### Cryptoasset payments

The Commission has become aware of instances of non-remote casinos accepting cryptoassets as a form of customer payment. Operators are reminded that their Money Laundering (ML) and Terrorist Financing (TF) risk assessment must be reviewed if certain circumstances change, including new methods of payment by customers [14] . This has been rated medium risk as there is no widespread evidence of this specific risk area. For further information on this risk area, see our information on digital technologies and anti-money laundering.

### Bank drafts

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

There is a risk that there could be a shift from cash payments to bank drafts as a form of payment due to the following reasons:

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

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

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

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

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

**Bring your own devices' (BYODs)**

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

These include:

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

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

**Transfer of funds between casino customers**

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

### Unlicensed employees carrying out ID checks

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

### Key person responsible for regulatory compliance

A requirement of the Regulations is for casino operators to appoint, where appropriate with regard to the size and nature of their business, an individual who is either a member of the board of directors (or if there is no board, of its equivalent management body) or of its senior management, as the officer responsible for the operator's compliance with the Regulations. This could be the same person as the nominated officer if the operator considers this a suitable arrangement. [17]

The Commission has received evidence that some casino operators are not complying with this requirement and will view any non-compliance with the Regulations seriously. This has been rated as high risk.

### References

**14** As required under Licence Condition 12.1.1 of the LCCP.

**15** Financial Transactions and Reports Analysis Centre of Canada Operational alert: Laundering the proceeds of crime through a casino-related underground banking scheme (opens in new tab) accessed 25 February 2020, updated December 2019.

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

**17** Regulation 21(1)(a).