Emerging money laundering and terrorist financing risks from April 2020

COVID-19 emerging risks bulletin - April 2020

Our latest emerging risks bulletin looks at the impact of coronavirus, the importance of checking digital identification and increases in online scams and fraud attempts.

Reminder to all licensed operators: impact of the coronavirus pandemic, and heightened money laundering and terrorist financing risks

The Gambling Commission recognises the major impact the current unprecedented coronavirus crisis is having on affected gambling sectors, including the closure of premises, employees furloughed and loss of business. To assist you in managing the risks this presents to your business, customers and employees, we will continue to advise you about emerging risks that we identify. Businesses will need to consider whether their money laundering and terrorist financing risk assessment needs updating as a result.

Operators are reminded to remain vigilant and comply with the LCCP, The Gambling Act 2005 (opens in new tab) and other relevant laws, i.e. the Proceeds of Crime Act 2002 (opens in new tab), the Terrorism Act 2000 (opens in new tab) and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (opens in new tab). The Gambling Commission's guidance to both casino and other operators along with our latest Risk Assessment of The Money Laundering and Terrorist Financing risks within the British Gambling industry (2019 version) will assist licensed operators in mitigating the emerging risks identified below.

Digital ID checks: emerging money laundering and terrorist financing risk

The associated shift to online gambling during the crisis makes it more vital for online gambling businesses to ensure they are carrying out robust digital ID checks upon customer registration. It is therefore even more essential that all operators conduct thorough 'Know Your Customer' checks, and customer due diligence checks in the case of the casino sector, to ensure they are not dealing with illicit funds.

Operators also need to have adequate customer risk profiles in place to ensure all potential money laundering and terrorist financing risks have been considered, and that operators consider making suspicious activity reports to the National Crime Agency in the following cases:

- organised Crime Groups have sought to exploit the current situation through finding new ways to obtain money or monetary equivalents e.g. through the sale of essential healthcare

equipment, the proceeds of which could be used for gambling purposes. Source of fund and 'Know Your Customer' checks (as well as customer due diligence checks for casinos), will be vital in detecting suspicion or knowledge of money laundering or terrorist financing

- there have been reported increases in 'illegal money lending' and fraud, with the risk that problem gamblers could resort to funding their gambling activities through these mechanisms, making affordability and source of funds checks of paramount importance in identifying increased risk of money laundering and terrorist financing.

There is evidence suggesting gambling affiliates are exploiting the coronavirus pandemic to encourage gamblers to spend more money on gambling activities. Operators are reminded:

- to have robust social responsibility provisions in place, as problem gambling and the use of the proceeds of crime (i.e. stolen money) to gamble can in some cases be co-dependent risk factors
- to conduct due diligence checks on any third-party companies being used in reliance on an operator's licence (LCCP Code Provision 1.1.2
- that all marketing must be undertaken in a socially responsible manner and must not encourage customers to spend more than they can afford, and therefore discourage proceeds of crime being spent by customers (LCCP Code Provision 5.1.6).

In addition to customer checks, operators are reminded that it is important to carry out sufficiently robust background checks on employees, referred to as 'Know Your Employee' checks.

Cryptoassets and prepaid cards: emerging money laundering and terrorist financing risk

The coronavirus crisis has seen criminals seeking to exploit the situation with an increase in cyber-attacks, along with the increased use of digital payments (such as cryptoassets and online prepaid cards, also known as vouchers). There are reports of more online scams and fraud targeting vulnerable people. This presents a high money laundering and terrorist financing risk to the gambling industry, as criminals will seek different ways to dispose of and use illicit funds from this fraudulent activity.

The current situation has also seen increased use of digital methods, such as cryptoassets and prepaid cards, as a form of customer payment. Cryptoasset transactions are attractive to criminals as they are fast, convenient and can be carried out anonymously. Evidence shows there is a high risk of 'smurfing' with the use of prepaid cards, and there is evidence that this money has then been used for gambling.

Both methods of payment (cryptoassets and prepaid cards) are viewed as high risk from a money laundering and terrorist financing perspective, and operators are reminded of the need to conduct thorough source of funds and source of wealth checks (where applicable), in order to keep crime out of gambling. Operators are reminded that it is even more vital that they should also submit suspicious activity reports (SARs) where there is knowledge or suspicion of money laundering (including criminal spend) or terrorist financing. When submitting a

SAR, a Key Event should also be made to the Gambling Commission in accordance with Licence Condition 15 of the LCCP.

Operators are reminded of their responsibilities under Licence Condition 12.1.1 (1), which requires licensees to review their money laundering and terrorist financing risk assessments upon the introduction of new products or technology or new methods of customer payment.

Operators are also reminded that it is mandatory to submit a key event to the Commission under Licence Condition 15.2.1(8) where there are any changes to the methods by which, and/or the payment processors through which, the licensee accepts payment from customers using their gambling facilities. When notifying the Commission under Licence Condition 15, we expect the following information to be provided as a minimum:

- the type of payment method
- the provider
- how the payment method was assessed in the operator's money laundering and terrorist financing risk assessment.

If the payment method relates to cryptoassets:

- are cryptoassets being accepted directly or through a third party, if so who?

If cryptoassets are being accepted directly:

- how fluctuations compared to fiat currency will be dealt with (with regards to responsible gambling tools, AML triggers, etc)
- what information has been provided to consumers to ensure they are aware of the risks associated with using cryptoassets as a payment method
- how the funds will be treated in the event of insolvency and how customers will be informed of this.

'Money mules': emerging money laundering and terrorist financing risk

An increase in online scams and fraud targeting vulnerable people has seen illicit funds being transferred through third party bank accounts ('mule' accounts), to break the audit trail of transactions and complicate any investigation. There is evidence that 'mule' accounts have been used for gambling purposes by money mules, with mainly vulnerable individuals targeted.

Operators are reminded to be alert to this. A red flag indicator for this activity is the opening of a gambling account with a minimal deposit initially, which is soon followed by several larger deposits and withdrawn to an increased amount of accounts. This makes it even more vital for operators to conduct thorough source of funds and source of wealth checks (where applicable), as well as customer ID checks upon customer registration, as required under Licence Condition 17 (applicable to remote operators only).

Where appropriate, licensees should consider obtaining their own legal advice regarding the emerging risks discussed here.

For any further assistance please contact us.