

Emerging money laundering and terrorist financing risks from February 2022

10 February 2022

Our latest emerging risks update covers the risks associated with having inadequate money laundering and terrorist financing risk assessments in place (including policies, procedures and controls), insufficient due diligence checks on third party providers and or business relationships, along with the use of Scottish notes and pre-paid cards by customers.

Improvements needed in gambling operators' money laundering and terrorist financing risk assessments (including policies, procedures and controls)

The Gambling Commission expects to see significant improvements by licensees around their money laundering and terrorist financing controls.

Licensees should:

- be aware of the mandatory requirement under [Licence Condition 12.1.1 of the Licence Conditions and Codes of Practice](#) (LCCP) which stipulates that gambling businesses must conduct an assessment of the risks of their business being used for money laundering and terrorist financing and have appropriate policies, procedures and controls in place to mitigate the risk of money laundering and terrorist financing
- be aware of the Commission's guidance for [casinos](#) and [other gambling businesses](#) to assist with compliance, which sets out how to approach implementing a risk-based approach into your gambling business.

There are too many instances being identified where licensees are failing to meet the requirements of the [The Money Laundering, Terrorist Financing and Transfer of Funds \(Information on the Payer\) Regulations 2017 \(opens in new tab\)](#)¹ and the LCCP. We would urge all licensees to review their current controls to ensure that they are fully compliant with Licence condition 12.1.1.

To assist licensees, we have published the [Raising Standards for consumers - Compliance and Enforcement Report 2020 to 2021](#). The Report highlights failings we have identified and includes some examples of good practice to consider.

We will take regulatory action (which can include suspension and revocation of licences) where we identify significant failings by licensees. Further information about the action we have taken can be found on the Commission's [regulatory actions](#) page.

¹ applicable to casinos only

Due diligence checks on third party business relationships and business investors

The Commission has become aware of instances of gambling operators failing to conduct sufficient due diligence measures in their third-party business relationships (including where licensees have received third party investment or entered into white label partnerships).

White label partnerships have been noted as high risk specifically for anti-money laundering failures in the Commission's [current money laundering and terrorist financing risk assessment of Britain's gambling industry](#).

Gambling operators are required to take account of such publications under Licence Condition 12.1.1(3) of the [LCCP](#). Further information on white label partnerships can be found in the Commission's publication '[Reminder to licensees regarding white label gambling websites](#)'.

The Commission's guidance for both [casino](#) and [other gambling operators](#) notes the following:

'Operators should also give due consideration to the money laundering risks posed by their business-to-business relationships, including any third parties they contract with. The assessment of these risks are based, among other things, on the risks posed to the operator by the jurisdictional location of their third-party and any relevant domestic anti-money laundering legislation they must comply with, transactions and arrangements with business associates and third-party suppliers such as payment providers and processors, including their beneficial ownership and source of funds. Effective management of third-party relationships should assure operators that the relationship is a legitimate one, and that they can evidence why their confidence is justified'.

In one case study a gambling operator failed to conduct sufficient checks on the source of funds from an investment that had originated from cryptoassets (which was then converted to Sterling when it was invested into the gambling business). This case study highlights failings with the licensed business, including: failure to establish the source of funds for the originating cryptoassets; transactional risks of asset exchange and jurisdictional risks due to the sources of funds originating from a high risk jurisdiction.

There have been repeated examples of gambling operators failing to consider jurisdictional risk in relation to these business relationships. The Commission's guidance for both casino and other gambling operators highlights the importance of considering jurisdictional risk. These risks are heightened where gambling operators are conducting business or customer relationships with sanctioned jurisdictions as this is a breach of the [Sanctions and Anti-Money Laundering Act 2018 \(SAMLA\)](#) [\(opens in new tab\)](#) (for example) and international law. Further information can be found on the [GOV.UK](#) [\(opens in new tab\)](#) website.

Please see the April and July 2020 e-bulletins for more information on the risks associated with cryptoasset payments and the importance of operators conducting robust due diligence measures in their third-party business relationships.

By failing to consider the risks associated with such relationships, operators run the risk of breaching the following:

- Licence Condition 12.1.1(1) of the LCCP which requires that operators ‘must conduct an assessment of the risks of their business being used for money laundering and terrorist financing’
- Licence Condition 12.1.1(3) which requires that operators ‘take into account any applicable learning or guidelines published by the Gambling Commission from time to time’
- Part 7 of the [Proceeds of Crime Act 2002 \(opens in new tab\)](#) and Part 3 of the [Terrorism Act 2000 \(opens in new tab\)](#) which requires that a suspicious activity report (SAR) must be submitted to the UK Financial Intelligence Unit wherever there is knowledge or suspicion of money laundering or terrorist financing. Please refer to the May 2021 e-bulletin below which provides advice on how to submit quality SARs.

Scottish notes and pre-paid cards

The significant, potential money laundering risks associated with the use of Scottish notes and pre-paid cards have been highlighted separately in the Commission’s current money laundering and terrorist financing risk assessment of Britain's gambling industry. However, there is now also an increased risk of Scottish notes being used to top up pre-paid cards.

Operators should remain curious as to the source of customer funds and conduct ongoing customer monitoring to ensure that customer spending levels align with your knowledge of their affordability to gamble. The Commission’s [Raising Standards for consumers - Compliance and Enforcement report 2019 to 2020](#) shows the ‘good practice’ techniques gambling operators should be conducting in order to ensure compliance with their legal responsibilities.