Emerging money laundering and terrorist financing risks from May 2021

28 May 2021

Our latest emerging risks bulletin looks at innovations in cryptoassets, the quality of suspicious activity report (SAR) submissions, insufficient due diligence checks, the threat of organised crime and the latest podcast from the UK's Financial Intelligence Unit.

Innovations in the cryptoasset market

The Commission is reiterating the importance of operators' responsibilities under Licence Condition 12.1.1 (1) of The LCCP which requires licensees to conduct an assessment of the risks their businesses face from money laundering and terrorist financing upon the introduction of new products or technology or new methods of customer payment.

The cryptoasset market is constantly evolving due to increasing popularity and product innovations e.g., 'non-fungible tokens' ‡ . Licence Condition 12.1.1.(3) requires operators to take account of any applicable learning or guidelines published by the Commission on this subject. Cryptoasset payments have been rated high risk in our current publication of the money laundering and terrorist financing risks within Great Britain's gambling industry (2020 version). Operators are also required to submit a Key Event to the Commission under Licence Condition 15.2.1(8) wherever there are changes in payment methods.

The UK's Crown Prosecution Service (CPS) (opens in new tab) expects to see an increase in the number of Bitcoin and cryptoasset related scams in the coming years and the Commission encourages operators to remain vigilant to such changes and update their money laundering and terrorist financing risk assessments accordingly.

Also, to assist with implementing a risk-based approach, the Financial Action Task Force (FATF), the inter-governmental watchdog that establishes standards for anti-money laundering and know-your-customer requirements, has published both new standards for implementation of a risk-based approach (opens in new tab) and new draft guidance (opens in new tab) for decentralised platforms. Operators must familiarise themselves with FATF's guidance to help combat money laundering and terrorist financing and implement such learning into their business.

Quality of suspicious activity report (SAR) submissions

The National Crime Agency (NCA) has published guidance (opens in new tab) providing information on submitting quality SARs. The guidance acts as a useful checklist for what information should be included in a SAR to ensure the maximum impact from the information provided. During the COVID-19 pandemic, the NCA has seen an increase in SAR submissions and it is vital that operators submit a SAR to the United Kingdom's Financial Intelligence Unit (UKFIU) whenever there is knowledge or suspicion of money

laundering or terrorist financing (as required under The Proceeds of Crime Act 2002 (opens in new tab) ('PoCA') and The Terrorism Act 2000 (opens in new tab) ('TACT')). Failure to do so can result in committing a criminal offence.

Furthermore, operators are also reminded of the need to submit quality SARs as this will aid the UKFIU if further investigations need to be carried out i.e., with other law enforcement agencies. Operators are also reminded that failure to submit a Defence Against Money Laundering (DAML) SAR to the UKFIU (when needing to commit a prohibited act) could be a criminal offence under PoCA and TACT. Examples of prohibited acts include:

- transferring customer balances when a suspicion has been formed
- retaining customer's account balance once a suspicion has been formed
- moving a customer's account balance within your business to a different account, once a suspicion has been formed.

Operators are also reminded that a corresponding SAR Key Event which includes the SAR's unique reference number (URN) must also be submitted under Licence Condition 15 of The LCCP.

Insufficient due diligence measures, the threat of organised crime and customers from high risk third jurisdictions

The Commission has come across various examples of operators failing to sufficiently scrutinise the source of customer funds. It is becoming increasingly important for operators to carry out sufficient due diligence checks as the threat of serious and organised crime increases globally. Failure to conduct sufficient due diligence checks becomes even more problematic (for example) as:

- the threat from organised crime infiltrating businesses remains significant.This year's EU Serious Organized Crime Threat Assessment 2021 (opens in new tab) states that trade in illegal drugs continues to 'dominate' the world of organised crime in the EU accounting for a large portion of criminal profits, money laundering and violence linked to organised crime
- if a customer is from a high-risk third country.

The UK government has added Pakistan to the list of undesirable 21 high-risk countries with unsatisfactory money laundering and terrorist financing controls. This list of 21 countries replicates the list of countries named by FATF as high-risk or under increased monitoring.

The full list of high-risk third countries under Schedule 3ZA of The Money Laundering and Terrorist Financing (Amendment) (High-Risk Countries) Regulations 2021 (opens in new tab) ('MLTFR 2021') includes (in order):

- Albania
- Barbados
- Botswana
- Burkina Faso

- Cambodia
- Cayman Islands
- Democratic People's Republic of Korea
- Ghana
- Iran
- Jamaica
- Mauritius
- Morocco
- Myanmar
- Nicaragua
- Pakistan
- Panama
- Senegal
- Syria
- Uganda
- Yemen
- Zimbabwe.

According to the UK government, the nations in this category pose a threat because of weak tax controls and lack of check and balance on terrorism financing and money laundering.

The MLTFR 2021 came into force on March 26th, 2021 after the definition of a high-risk third country identified in a new Schedule 3ZA and updates The Money Laundering Regulations 2017.

All operators are required to take a risk-based approach in order to mitigate the risk of money laundering and terrorist financing. Both our casino guidance and guidance for non-casino operators makes clear that, 'higher risk customers should be subjected to a frequency and depth of scrutiny greater than may be appropriate for lower risk customers'.

Casino businesses are also required under The Money Laundering Regulations 2017 (opens in new tab) to carry out enhanced customer due diligence measures (ECDD) wherever there is a higher risk of money laundering or terrorist financing. Please refer to our comprehensive casino guidance for further information on the circumstances in which ECDD measures **must** be applied.

† The risks associated with cryptoasset payments have been previously discussed in the Commission's April 2020 emerging risks ebulletin. Please refer to this further below for more information.