GAMBLING COMMISSION

4 January 2018

Customer interaction and anti-money laundering – Compliance assessment activity

The purpose of this letter is to summarise the findings of our recent compliance assessment activity which had a focus on remote casino operators' approach to anti-money laundering and customer interaction. The findings set out in this letter are not comprehensive, but they give a clear indication of actions the Casino sector are required to take with immediate effect.

The compliance assessment focussed on the measures that a remote gambling operator should have in place to address the prevention of money laundering and terrorist financing and, in particular, compliance with the following legislation and licence conditions:

- Licence condition 12.1 Prevention of money laundering and terrorist financing
- The Proceeds of Crime Act 2002 (POCA)
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Regulations).

In carrying out the assessments we also identified action that needs to be taken in respect of social responsibility (SR) code breaches.

Due to the serious nature of the assessment findings, we have already started investigations into 17 remote operators and are keeping under consideration whether it is necessary to commence a licence review of five operators under section 116 of the Gambling Act 2005 (the Act) with a view to exercising our regulatory powers under section 117 of the Act.

For more information on our Enforcement process, please see our *Licensing, Compliance and Enforcement policy statement.*

We have reviewed the findings from the first batch of assessments carried out with remote casino operators. We noted some common themes in the failings, practises and concerns which we set out below. These generally related to operators' approach to:

- Anti-Money Laundering Regulations
- Social Responsibility provisions.

The identified failings have raised significant concerns about the effectiveness of the Casino sector's management and mitigation of risks to the licensing objectives. We set out at the conclusion of this letter what actions you need to take to address our concerns.

Victoria Square House
Victoria Square
Birmingham B2 4BP

T+44 121 230 6666
F+44 121 230 6720
www.gamblingcommission.gov.uk

Summary of compliance assessment findings

1) **Breaches of Licence condition 12.1.1 Anti-money laundering - Prevention of money laundering and terrorist financing/The Regulations**

Risk assessment - Licence condition 12.1.1.1 requires an operator to conduct an assessment of the risks of their business being used for money laundering and terrorist financing. Such risk assessment must be appropriate and must be reviewed as necessary in the light of any changes of circumstances, including the introduction of new products or technology, new methods of payment by customers, changes in the customer demographic, or any other material changes, and in any event reviewed at least annually.

Furthermore, completion of a risk assessment has been a requirement of your licence since October 2016 and there is guidance on risk assessments in *The Prevention of Money Laundering and Combating the Financing of Terrorism - Guidance for remote and non-remote casinos*.

An appropriate money laundering risk assessment is to drive improvements in financial crime risk management through identifying the general and specific money laundering risks an operator is facing, determining how these risks are mitigated by the operators AML programme controls and establishing the residual risk that remains for the MLRO to manage.

Licence condition 12.1.1.3 requires operators implement policies, procedures and controls to mitigate money laundering and terrorist financing risk. Failure to comply with this condition puts the licensing objective of preventing gambling from being a source of crime or disorder, being associated with crime or disorder, or being used to support crime at risk. It is also a breach of Regulation 19 of the Regulations (Policies, controls and procedures).

Customer due diligence (CDD)/enhanced due diligence (EDD) - Casino operators are required to conduct CDD when they establish a business relationship with a customer, suspect money laundering or terrorist financing or doubt the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification.

As operators you must apply enhanced due diligence (EDD) where a customer presents a higher risk of money laundering. You must also apply CDD measures in relation to any transaction that amounts to €2,000 or more, whether the transaction is executed in a single operation, or in several operations which appear to be linked.

In our initial assessments we found a lack of evidence of ongoing monitoring of customer accounts, which is a breach of Regulation 28(11) (Customer due diligence measures) of the Regulations. We are concerned that where ongoing monitoring of customer accounts is not proactively undertaken both money laundering and/or SR issues go unreported.

Training - Casino operators must ensure that employees receive sufficient training. This includes understanding the requirements of the Regulations, the Terrorism Act 2000, the Proceeds of Crime Act 2002 (POCA), and data protection, and apply the operator's policies, procedures and controls, including the requirements for CDD, record keeping and the submission of suspicious activity reports (SARs). Operators must maintain records of training provided to employees. Failure to provide adequate training, and maintain appropriate records of training is a breach of Licence condition 12.1.2 and Regulation 24 (Training) of the Regulations.

During the assessments, whilst Money Laundering Reporting Officers (MLRO) confirmed they had industry experience within payments and fraud, in some case they had no formal AML qualifications. It was of concern that some MLROs were unable to provide suitable explanations as to what constitutes money laundering and had no understanding of the main principles under POCA. There was a general lack of understanding of how criminal spend could affect the business.

SARs/decision making – We found little evidence of effective considerations given to Suspicious Activity Report (SAR) submissions to the National Crime Agency (NCA) or equivalent Financial Intelligence Unit (FIU). The Commission receives reports from the UK FIU and notes that in feedback to operators they often conclude that there was insufficient information provided within the SAR to conduct an in-depth analysis of the money laundering risk. We saw evidence within operators records that they had assumed the FIU had approved the ongoing business relationship, as opposed to operators undertaking further enhanced due diligence and being more curious about that relationship.

MLROs had neither made nor kept any note of specific cases or referrals and there were no documented risk assessments. There was also lack of understanding as to what would constitute 'tipping off' under section 333A of POCA.

2) **Breach of Social responsibility (SR) code provision 3.4.1.1 (e) (i) & 3.4.1.1 (e) (ii) –** Key tools in upholding the licensing objective of protecting children and other vulnerable people from being harmed or exploited by gambling are measures to ensure that operators monitor their customers for signs of problem gambling.

SR code provision **3.4.1.1(e)** which states "*licensees must put into effect policies and procedures for customer interactions where they have concerns that a customer's behaviour may indicate problem gambling".* The policies must include specific provision for making use of all relevant sources of information to ensure effective decision making, and to guide and deliver effective customer interactions, including in particular:

- *provision to identify at risk customers who may not be displaying obvious signs of, or overt behaviour associated with, problem gambling: this should be by reference to indicators such as time or money spent*

- *specific provision in relation to customers designated by the licensee as 'high value', 'VIP' or equivalent.*

We reviewed a large number of customer accounts during the assessments and identified potential signs of problem gambling based on consumers' gambling pattern and spend. In many cases however this behaviour did not trigger a customer interaction.

Customer account records did not show any evidence of customer interactions taking place and operators were of the view that these customers did not raise any concerns. We therefore consider that licensees maybe breaching social responsibility code provision 3.4.1.1(e) (i) customer interaction.

What you need to do now

You need to review your prevention of money laundering and terrorist financing and social responsibility policies and procedures to ensure these meet or exceed the specific requirements contained in the *Licence conditions and codes of practice* and the Regulations. This can be done specifically by:

conducting appropriate assessments of the risks of money laundering and terrorist financing for your businesses, and implement policies, procedures and controls which manage the identified risks effectively
introducing measures for customer due diligence, the ongoing monitoring of customers and enhanced customer due diligence which are sufficiently risk-focused, including better risk profiling of customers
ensuring that you are able to adequately evidence customer interactions
providing your staff with appropriate training to ensure that they are aware of the law relating to money laundering and terrorist financing and how to recognise and deal with transactions, activities or situations which may be related to money laundering or terrorist financing.
ensuring that your policies and procedures make specific provision for making use of all relevant sources of information where you have concerns that a customer's behaviour may indicate problem gambling and putting into effect such policies and procedures.

For guidance on compliance around anti-money laundering see our website.