# Anti Money Laundering briefing for online casino operators

By Niki Stephens and Sam Ruback

Niki Stephens

Sam Ruback

In January 2018 the Gambling Commission of Great Britain announced that it had written to all online casino operators to raise concerns about the sector's approach to anti-money laundering (AML) and social responsibility.

The letter followed months of compliance assessment activity by the Gambling Commission which assessed the casino sector's management and mitigation of risks to the licensing objectives including: preventing gambling from being a source of crime or disorder, being associated with crime or disorder, or being used to support crime.

As a result of the Gambling Commission's concerns it indicated that 17 remote operators were being investigated and that it was keeping under consideration whether 5 of those operators would be the subject of a formal licence review.

The letter indicated that some money laundering reporting officers (MLROs) (also referred to as "nominated officers") were unable to provide suitable explanations as to what constitutes money laundering and had no understanding of the main principles under the Proceeds of Crime Act 2002 (POCA). The Commission also noted, in particular, that there was "little evidence of effective considerations given to Suspicious Activity Reports (SARs) submissions to the National Crime Agency (NCA) or equivalent Financial Intelligence Unit", that the UK FIU often concludes that SARs submitted by casino operators are usually lacking in information and that there was a lack of understanding as to what would constitute the offence of "tipping off".

## The main principles under POCA

POCA establishes a number of money laundering offences including:

- the principal money laundering offences;
- offences of failing to report suspected money laundering; and
- offences of tipping off about a money laundering disclosure, tipping off about a money laundering investigation and prejudicing money laundering investigations.

The principal offences criminalise any involvement in the proceeds of any crime if the person knows or suspects that the property is criminal property.

The offences are broad and can be committed by any person, including, for example, the person appointed by a casino operator as MLRO, and any other persons working for a casino operator, who has knowledge or suspicion that a customer is using the proceeds of crime.

Under section 330 of POCA, a person may commit the offence of "failure to disclose" if they know or suspect, or have reasonable grounds for knowing or suspecting, that another person is engaged in money laundering and they do not make a required disclosure to the MLRO as soon as practicable. For these purposes, the information must have come to the person in the course of a business in the regulated sector and the "regulated sector" includes those "operating a casino under a casino operating licence" (as per the definition provided in s65(2) of the Gambling Act 2005).

Under section 331 of POCA, the MLRO may also commit an offence if they receive an internal disclosure and fail to submit a SAR to the NCA or other or equivalent FIU.

The general purpose of these offences is to reflect the expectation that individuals carrying out activities in the regulated sector should demonstrate a higher level of diligence in handling transactions than those employed in other businesses.

### Internal reports and suspicious activity reports

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Regulations) also apply to online casinos. The Regulations require online casinos to (amongst other things) conduct due diligence on, and ongoing morning of, their customers and to conduct enhanced due diligence and enhanced ongoing monitoring if, taking a risk based approach, they consider the customer to present a higher risk of money laundering.

In the course of conducting CDD, ongoing monitoring, EDD or enhanced ongoing monitoring in accordance with the Regulations, and otherwise, there are various ways in which a person working for a casino may come to know or suspect that a customer is playing with the proceeds of crime. Examples could include a player: making deposits and seeking to withdraw them without any gambling activity taking place; wagering unusually high amounts of money in a short period of time; depositing sums of money that the operator believes may (based on source of funds and source of wealth checks or other sources of information) be beyond their means; or producing fraudulent identification or other documents.

Individuals working for a casino operator have a legal defence if they report to the MLRO where there are grounds for knowledge or suspicion of money laundering or terrorist financing. All persons working for a casino operator must therefore understand the procedure by which reports are to be made to the MLRO and understand the backdrop to, and importance of, making internal reports. On receipt of the internal report, the MLRO must then consider if a disclosure should be made to the NCA.

The preferred way to provide a disclosure to the UK Financial Intelligence Unit within the NCA is in the form of a SAR. SARs can be submitted online, by paper or by encrypted bulk data exchange (usually taken advantage of by high volume reporters). Casino operators should include in each SAR as much information as possible about the customer and their identity (including if a customer has provided debit or credit card details that would identify them), the transaction(s), the relevant activity and the customer's product preferences. The NCA has published a number of guidance notes to assist with preparing SARs and has issued a glossary of appropriate terms.

Once the SAR has been submitted, the MLRO should submit a key event notification to the Gambling Commission as soon as practicable and in any event within five working days from receipt of the unique reference number issued by the NCA. The casino operator will be required to indicate whether the customer relationship has been discontinued at the time the key event is submitted. We are aware of instances where the Gambling Commission has separately asked casino operators to confirm how may SARs it has submitted over a particular period of time - the inference being that the Gambling Commission expects online casinos that are fully and properly discharging their duties to be submitting SARs more regularly than is currently the case.

### Requesting Consent

In making a SAR to the NCA, there is the opportunity to request a defence or, as the mechanism is referred to technically, "appropriate consent." This arises due to the fact that if a casino operator (as someone in the regulated sector for the purposes of POCA) handles the proceeds of crime, they may commit one of the principal money laundering offences. These include: concealing, disguising, converting transferring or removing criminal property under section 327 of POCA; facilitating the acquisition, retention, use of control of criminal property by or on behalf of another person under section 328 of POCA; or acquisition, use or possession of criminal property under section 329 of POCA. Appropriate consent from the NCA will allow a casino operator to permit a suspect transaction to proceed, without the risk of criminal liability on their part. In the case of a casino operator, this could include: paying winnings out to the player, returning deposited funds or using the money locked in the player's account to satisfy chargeback requests. Each case should be considered in relation to its facts to assess if it is appropriate for

consent to be sought (as opposed to the transaction and commercial relationship simply being terminated).

Plainly, if repeated SAR submissions are made in relation to the same customer, it may be difficult for an operator to repeatedly seek a defence (and indeed the Gambling Commission has indicated that the reporting defence is not intended to be used repeatedly in relation to the same customer).

If the casino operator wants to terminate the customer relationship at a time when the suspicion of money laundering remains and there are funds to repatriate, the Commission suggests that the operator considers requesting a defence.

To request a defence, the "consent requested" box should be ticked on the SAR form and requests must be for a specified activity and should not be open ended. Examples might include (without limitation): returning funds to the provider of those funds; under instruction from a competent authority (which would not include a bank), transferring funds to any other party; and under instruction from a bank or other financial institution, transferring funds to any other party.

### Tipping off

Under section 333A of POCA, a person working for an online casino may commit an offence if they reveal that a SAR has been submitted to the NCA and that by sharing such information, they are likely to prejudice any investigation. An offence may also be committed if an individual discloses that an investigation into allegations is being contemplated or carried out, and such disclosure is likely to prejudice the investigation.

After a SAR has been submitted, extreme care should be taken to ensure that a "tipping off" offence is not committed and that any customer enquiries should be conducted in a delicate, and tactful, manner. The Commission has indicated in its guidance to casino operators in relation to the prevention of money laundering and combating the financing of terrorism that "reasonable enquiries of a customer, conducted in a tactful manner, regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity is prudent practice, forms an integral part of CDD measures and should not give rise to tipping off". The Commission's guidance also indicates that if the casino operator wants to terminate the customer relationship, provided this is handles sensitively, there "will be a low risk of tipping off or prejudicing an investigation".

The existence of a SAR must not be revealed to any customer of a casino at any time, whether or not consent has been requested.

### Conclusion

Recent regulatory activity in Great Britain has brought into sharp focus the importance of the MLRO's role, the significant responsibility the office carries, and the importance of thorough and regular training for employees in order to ensure that they understand their responsibilities and the framework underpinning them.

Niki Stephens is a Managing Associate and core member of Mishcon de Reya LLP's Betting & Gaming group. She regularly advises clients in this sector in relation to corporate and commercial matters including acquisitions and intra-group arrangements. Niki also provides gambling licensing, regulatory and compliance advice to regulated gambling clients.

Sam Ruback is an Associate in the Business Crime Group, part of Mishcon de Reya LLP's Fraud and Dispute Resolution team. He specialises in advising individuals and corporate entities in relation to charges of fraud, bribery, money laundering and corruption brought by bodies such as the SFO and CPS. He is also experienced in bringing Private Prosecutions on behalf of victims of such offences.