gamevy

Anti-Money Laundering

Detecting and Preventing Financial Crime

Training for Gamevy

Introduction

This document is Gamevy's training on anti-money laundering regulations within the context of our operation as a remote casino operator. Having followed the training, we expect employees to:

- Recognise the consequences of financial crime on the individual, firm and society as a whole
- State the details of anti-money laundering and counter-terrorist financing laws and regulations
- Know the money laundering offences and penalties
- Explain the customer identification and verification procedures
- Apply the risk-based approach to due diligence
- Identify suspicious activities and know the process for reporting suspicions
- Know where to go for further information

1 The Consequences of Financial Crime

Money Laundering is defined as the process whereby the proceeds of crime – from drugs, extortion, tax evasion, theft or numerous other crimes – are transformed into ostensibly legitimate money or other assets.

Within the UK, money laundering is defined in section 340 of the Proceeds of Crime Act 2002 and covers wide-ranging circumstances involving any activity concerning the proceeds of crime. This includes:

- Acquiring, possessing, transferring or converting the proceeds of crime
- Handling the benefit of acquisitive crimes such as theft, fraud and tax evasion
- Handling stolen goods
- Being directly involved with any criminal or terrorist property, or entering into an arrangements to facilitate the laundering of criminal or terrorist property
- Criminals investing the proceeds of their crimes in any financial product or using the proceeds to buy goods and services

According to the definition contained in the UN International Convention for the Suppression of the Financing of Terrorism, the primary objective of terrorism is "to intimidate a population or to compel a Government or an international organisation to do or abstain from doing any act". Like any other organisation, a terrorist one requires money to finance its activities – recruitment, training, weapons, bases etc. Terrorist Financing has been extensively linked to organised crime and is the process of diverting legitimate funds and the proceeds of crime to fund terrorist organisations around the world.

The consequences of financial crime for society as a whole are devastating. In 1996, the IMF estimated that 2-5% of the worldwide global economy involved laundered money. It is a necessity for large-scale criminal organisations which cause huge damage to individuals, to property and to governments through their activities, which often include violence, illegal drugs and other dangerous activities.

As defensive measures have been put in place by the financial sector, the criminal have turned their attention to a range of non-financial sectors and businesses to assist in their laundering operations. Law enforcement have identified a number of business sectors where investigations have highlighted money laundering or terrorist financing vulnerabilities. In the gambling industry, for example, betting on high odds was seen as a way to launder money as winnings were declared and losses hidden or casino chips could be bought and then cashed in, with the difference claimed as winnings.

Casinos, including remote casinos, thus now fall within the list of non-financial businesses now subject to anti-money laundering legislation together with other comparable services.

Failure to comply appropriately with the code can lead to Gamevy losing its gambling license or facing other regulatory action.

For individual employees, failing to comply with the regulations or failing to make the appropriate disclosure can be a criminal offence and liable to prosecution. This is especially true of the Nominated Officer, since the decision to report or not to report suspicious activity is the personal responsibility of the nominated officer.

In general, the principles that Gamevy, as well as all remote casinos must follow are:

The Regulations require relevant businesses to:

- put in place procedures to verify the identity of customers on entering into a business relationship or transaction and to carry out ongoing monitoring during the business relationship
- keep records obtained in establishing customers' identities and of business relationships for five years
- train employees in the relevant procedures and law
- appoint a nominated officer whose role includes reporting to SOCA, or its successor, suspicions of money laundering activity

- put in place and maintain policies and procedures to cover the requirements listed above.

2.0 Anti-money laundering and counter-terrorist financing laws and regulations

Remote-Casino Operator

2.1 The Law

The Proceeds of Crime Act 2002 (POCA)2 places a duty on gambling operators to be alert to attempts by customers to gamble money acquired unlawfully, either to obtain 'clean' money in return or simply as a leisure activity. They should report instances of money laundering or attempts by customers to launder money to the Serious Organised Crime Agency (SOCA) and, if circumstances permit, wait for consent to deal with a transaction or arrangement involving the customer and wait until a set period has elapsed before proceeding.

As casinos fall within the 'regulated sector', they have additional legal responsibilities under POCA which could result in criminal charges for failing to comply (for example, the offence of tipping off). Casinos are also required to appoint a nominated officer. The nominated officer is responsible for receiving internal disclosures under POCA, deciding whether these should be reported to SOCA, making such reports to SOCA, and ensuring that appropriate consent is applied for as necessary.

The Proceeds of Crime Act 2002 (References to Financial Investigators) Order 2009 (Statutory Instrument No. 2009/975) gave the Commission the powers of accredited financial investigators under POCA. This means, amongst other things, that (in England and Wales) the Commission can apply for orders and warrants in relation to money laundering, for the purpose of:

- requiring a specified person to produce certain material
- permitting the search and seizure of material from specified premises
- requiring a financial institution to provide customer information relating to a specified person.

2.2 Requirements of Individuals

Employees

Employees must report to their nominated officer any knowledge or suspicion of money laundering whether by customers, guests or other employees.

Employees must follow casino policies and procedures for:

- CDD, including enhanced requirements for high risk customers, which includes politically exposed persons (PEPs);
- reporting suspicious activity to the nominated officer
- where necessary, seeking appropriate consent to allow participation in gaming and to conduct gaming and other business transactions
- record keeping for those who exceed the threshold or who have a business relationship.

The Nominated Officer:

They must have the authority to act independently in carrying out their responsibilities, and have access to sufficient resources to carry out their duties. Casinos must have contingency arrangements in place for circumstances where no nominated officer is in post, for example, if on annual leave, long-term sick leave or if the nominated officer leaves the employ of the casino.

Nominated officers have responsibility for:

- making reports to senior management on anti-money laundering (AML) and countering terrorist financing (CTF) activity
- receiving internal disclosures under Part 7 of the Proceeds of Crime Act 2002 (POCA) and Part III of the Terrorism Act 2000 (the Terrorism Act)
- deciding whether these should be reported to the Serious Organised Crime Agency (SOCA)
- if appropriate, making such external reports.

Senior Management

Senior management must be fully engaged in the processes around an operator's assessment of risks for money laundering and terrorist financing, and must be involved at every level of the decision making to develop the operator's policies and processes to comply with the Regulations. Disregard for the legal requirements, for example, turning a blind eye to customers spending criminal proceeds, may result in criminal or regulatory action.

A member of senior management who consents to, or connives in, the commission of offences under the Regulations, or where the commission of any such offence is attributable to any neglect on his part, will be individually liable for the offence.

Operators must establish and maintain appropriate written risk-sensitive policies and procedures relating to:

- customer due diligence (CDD) measures and ongoing monitoring
- reporting
- record keeping
- internal control
- risk assessment and management
- training

- the monitoring and management of compliance with, and the internal communication of, such policies and procedures.

2.3 Offences

OCA and the Terrorism Act create offences of failing to report suspicious activity. Where a person fails to comply with the obligations to make disclosures to a nominated officer, or the nominated officer to SOCA*, as soon as practicable after the information giving rise to the knowledge or suspicion comes to the employee, they are open to criminal prosecution.

In certain circumstances, a person also commits an offence under POCA or the Terrorism Act if he discloses information that a SAR has been submitted that is likely to prejudice any investigation, or discloses information that an investigation into allegations that an offence under POCA or the Terrorism Act has been committed, that is likely to prejudice the investigation.

A person in the regulated sector also commits an offence if he knows or suspects that an appropriate officer or, in Scotland, a proper person is acting (or proposing to act) in connection with a confiscation investigation, a civil recovery investigation, a detained cash investigation or a money laundering investigation which is being or is about to be conducted, and falsifies, conceals, destroys or disposes of, or causes or permits the falsification, concealment, destruction or disposal of, documents which are relevant to the investigation.

Where the record keeping obligations under the Regulations are not observed, an operator or person is open to prosecution and sanctions, including imprisonment for up to two years and/or a fine, or regulatory censure.

3.0 Customer Due Diligence

3.1 Identifying and Verifying Customers

A key requirement in the Regulations is the requirement to make checks on customers - CDD. Casino operators can use one of two approaches; identifying and verifying the identity of all customers on entry to the casino's licensed premises. In Gamevy's case, this means when setting up an account as a new customer we carry out an identification and verification check including address, date of birth, name, and credit check.

Operators must conduct their CDD on the basis of risk assessment, including simplified due diligence and enhanced due diligence (which includes PEPs). Operators are also required to identify the beneficial owner of a customer and they will also need to have evidence of identity in place for all customers.

Operators should note that CDD is ongoing and may need updating for changes in the customer's circumstances and personal details.

If a customer does not pass the initial CDD, we undertake a manual identification check, to complete within 72 hours. During this time customers are not permitted to withdraw the funds, but may play. If the customer cannot complete the verification within that time, the account will be frozen, pending further investigation. If the customer is under age then all bets are declared null and void and monies returned.

The customer database is run annually against the HM Treasury's Consolidated List of persons subject to financial restrictions.

3.2 Record-keeping

The purpose of the record keeping requirement is to ensure that there is an audit trail that could assist in any financial investigation by a law enforcement body.

The operator's record keeping policy and procedure should cover records in the following areas:

- details of how compliance has been monitored by the nominated officer
- delegation of AML/CTF tasks by the nominated officer
- nominated officer reports to senior management
- information not acted upon by the nominated officer, with reasoning why no further action was taken
- customer identification and verification information
- supporting records in respect of business relationships or occasional transactions
- employee training records
- internal and external suspicious activity reports (SARs)
- contact between the nominated officer and law enforcement or SOCA*, including records connected to appropriate consent.

Gamevy keeps a transaction log of the identity check. Further information required would be held securely.

Any communications with customers, including responses to manual checks, are kept in the CRM.

Information on transaction history and customer details is held for a period of a minimum 5 years.

Gamevy's terms and conditions state that a customer must inform the company if any personal data – such as change of address – is up to date.

Employee training records are held within the Gamevy Employee system – Quickbooks.

4.0 Risk-Based Approach

The risk-based approach involves a number of discrete steps in assessing the most proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the operator. These steps require the operator to:

- identify the money laundering and terrorist financing risks that are relevant to the operator
- design and implement policies and procedures to manage and mitigate these assessed risks
- monitor and improve the effective operation of these controls
- record what has been done, and why.

A risk-based approach tries to strike a balance between over-estimating the threat of money-laundering, being too cautious and thus unnecessarily causing customers annoyance, with under-estimating it and thus permitting money laundering or terrorist financing. It is not a blanket one size fits all approach, and therefore operators have a degree of flexibility in their methods of compliance.

In general, Gamevy operates within a relatively low-risk environment.

Our customers cannot deposit cash into their accounts – only payments from debit cards, pre-approved credit cards and paypal are permitted and a customer is only allowed to deposit using a single type of payment method (unless going through a manual and easily checked procedure). Customers may register more than one payment method on your account, but are only permitted to have one payment method active on the account at any one time. No bank card may be registered to more than one account on the Gamevy platform. Change or updates to a payment method on the account is only permitted when the balance is less than GBP 1.00 (£1.00) or EUR 1.00 (€1.00)).

Customers may only place wagers for the Games through the application. Attempts to place wagers through any other medium, including telephone, fax or post, will not be accepted.

We have no anonymous customers – every customer must go through a verification process in order to create an account. Customers undergo a robust identification and age verification process using a third party supplier. Gamevy only permits UK customers. We do a DEO IP location and only permit customers to register within the UK, our address verification ensures they are a UK citizen and we then permit them to bet within Europe. While this is not perfect or completely fool-proof, the system is robust and it means we are especially unlikely to have any Politically Exposed Persons (PEPs).

We do not, at present, feel the need to distinguish between low and high risk customers in advance of an account being set up. Additional information from the search may produce anomalies – this will flag a customer as being higher risk and therefore subject to additional controls as part of the withdrawal process. Finally,

we use player behaviour to monitor customers and carry out further checks as required.

We have procedures in place to look for unusual betting patterns and we record every single transaction. Gamevy looks for the relationship between the amount deposited, the amount withdrawn and the amount played. For example, anyone depositing and withdrawing large sums without significant play would trigger an investigation.

We have a withdrawal procedure that subjects withdrawals to an audit and we monitor accounts with high withdrawals. All deposited funds must be returned by the method they were originally deposited by (unless the customer follows a manual procedure which is then checked).

We target relatively small sizes of bet and regular play. Thus we would ask a customer wishing to deposit over £10,000 to provide source of funds.

Since our games require a mix of skill and luck, this is rarely appealing to those looking to launder money. We do not have chips or anything which could be used as a secondary currency.

Gamevy reviews this policy and risk assessment at least quarterly as part of our commercial risk.

5.0 Suspicious Activities and Reporting

Employees in casinos are required to make a report in respect of information that comes to them within the course of their business:

- where they know
- where they suspect
- where they have reasonable grounds for knowing or suspecting,

that a person is engaged in money laundering or terrorist financing. Within this guidance, the above obligations are collectively referred to as 'grounds for knowledge or suspicion'.

Under POCA and the Terrorism Act, individual employees face criminal penalties if they are involved in money laundering or terrorist financing. If they do not make an internal report to their nominated officer when necessary they may also face criminal sanctions.

In Gamevy's business, knowledge would only typically arise if a customer made a disclosure of criminal activity. Even seemingly light-hearted references to customer service representatives would be taken seriously and passed to the Nominated Officer.

Suspicion is a subjective judgement call, one which relies on Gamevy's ability to analyse and consider unusual patterns or anomalies in betting, withdrawal and deposits. Our systems are already configured to trigger manual checks at account set up and withdrawal on unusual patterns. As Gamevy develops and our data becomes more robust, these pattern analyses will become more sophisticated.

These cases will be passed to the Nominated Officer who will consider whether to make a report to SOCA. The decision with supporting evidence will be recorded in the CRM system.

If a report is made, the Nominated Officer will do so via SAR Online. https://www.ukciu.gov.uk/saronline.aspx. During this time and for the 7 working days until appropriate consent is given, withdrawals will be blocked from the account although further play and deposits may continue. Gamevy is not permitted to tell the customer that a transaction is delayed due to waiting for consent from SOCA.

6.0 Know where to go for Further Information

Employees are encouraged to read:

- Money laundering: the prevention of money laundering and combating the financing of terrorism Guidance July 2013
- Anti-money laundering: Approach to supervision April 2013
- The threat of money laundering and terrorist financing through the online gambling industry June 2009
  http://www.rga.eu.com/data/files/final__mha_report_june_2009.pdf
- Confidential intelligence line: 0121 230 6655
- Single point of contact for anti-money laundering:
  intelligencereports@gamblingcommission.gov.uk.cjsm.net