Duties and responsibilities under the Proceeds of Crime Act 2002

This advice explains how operators can make sure they and their employees comply with their obligations under The Proceeds of Crime Act 2002 (POCA).

Published: 13 November 2020

Last updated: 18 February 2021

This version was printed or saved on: 5 July 2022

Online version: https://www.gamblingcommission.gov.uk/guidance/duties-and-responsibilities-under-the-proceeds-of-crime-act-2002

Introduction and summary of the advice

Purpose of the advice

All gambling operators have a responsibility to keep financial crime out of gambling. The Proceeds of Crime Act 2002 (POCA) (link opens in a new window) places an obligation on gambling operators to be alert to attempts by customers to gamble money acquired unlawfully, either to obtain legitimate or 'clean' money in return (and, in doing so, attempting to disguise the criminal source of the funds) or simply using criminal proceeds to fund gambling. Both modes of operation are described as money laundering.

This advice document explains how operators can make sure they and their employees comply with their obligations under POCA. It sets out a number of matters operators need to be aware of and explains their duties and responsibilities under POCA.

While the advice focuses primarily on the relationship between operators and their customers, and the money laundering risks presented by transactions with customers, 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. (See code provision 1.1.2)

Who is this intended for?

This advice is directed at all holders of operating licences issued by the Gambling Commission (the Commission), excluding non-remote and remote casino operating licence holders who are provided with separate guidance in relation to anti-money laundering (AML) and counter terrorist financing.

The advice is detailed and aimed primarily at operators with a number of employees, either full time or part time. Operators with few or no employees may find the quick guide published separately on the Commission’s website helpful, although it remains the operator’s responsibility to understand and comply with the requirements of POCA.

The role of gambling operators

Operators have a responsibility to uphold the three licensing objectives set out in the Gambling Act 2005 (the Act)(opens in a new tab). The first of those licensing objectives is to prevent gambling from being a source of crime or disorder, being associated with crime and disorder, or being used to support crime.

As described in Purpose of the advice, money laundering in the gambling sector takes two main forms:

- exchanging money, assets, goods and property that were acquired criminally for money or assets that appear to be legitimate or 'clean' (so called classic money laundering). This is frequently achieved by transferring or passing the funds through some form of legitimate business transaction or structure
- the use of criminal proceeds to fund gambling as a leisure activity (so called criminal or 'lifestyle' spend).

In order to avoid committing offences under POCA, operators should report instances of known or suspected money laundering by customers to the National Crime Agency (the NCA) and, where a defence (appropriate consent) is requested, wait for such defence (consent) to deal with a transaction or an arrangement involving the customer, or wait until a set period has elapsed before proceeding.

Operators should be aware that there is no minimum financial threshold for the management and reporting of known or suspected money laundering activity.

The role of the Gambling Commission

The Commission requires operators to prevent gambling being a source of crime or disorder, being associated with crime and disorder, or being used to support crime. This advice document is an important frame of reference to help operators meet that objective. Whilst potential breaches of POCA will normally be reported to the NCA and fall to the police to investigate, the Commission, in its role as the gambling regulator, seeks assurance that risks to the licensing objectives posed by money laundering activity are effectively managed, and this advice will assist operators to meet their obligations under POCA, where appropriate.

The Commission adopts a risk-based approach to its role. We focus our attention on circumstances where the processing of criminal funds or criminal spend indicates serious failures in an operator’s arrangements for the management of risk and compliance with POCA, or makes a reasonably significant contribution to the financial performance of the business, particularly concerning their continued suitability to hold a licence. See the public statements.

Where an operator fails to uphold the licensing objectives, for example by being ineffective in applying AML controls or ignoring their responsibilities under POCA, or breaches an applicable licence condition, the Commission will consider reviewing the operating licence under section 116 (opens in a new tab) of the Act. This could result in the suspension or revocation of the operator’s licence under sections 118 (opens in a new tab) and 119 (opens in a new tab) of the Act. The Commission may also consider imposing a financial penalty where a licence condition has been breached, in accordance with section 121 (opens in a new tab) of the Act.

The Commission and other agencies or authorities that have the appropriate authorisation under POCA in England and Wales (see The Proceeds of Crime Act 2002 (References to Financial Investigators) (England and Wales) Order 2015) (opens in a new tab) can, in certain circumstances, apply for orders and warrants in relation to money laundering, for the purpose of, for example:

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

Licence conditions and codes of practice

Operators are required to comply with the applicable Licence Conditions and Codes of Practice and should read this advice in conjunction with the conditions and codes. Should operators breach the licence conditions or not follow the code provisions, the Commission may consider reviewing the operating licence in accordance with section 116 (opens in a new tab) of the Act.

This could result in the suspension or revocation of the operator's licence under sections 118 (opens in a new tab) and 119 (opens in a new tab) of the Act. The Commission may also consider imposing a financial penalty where we think that a licence condition has been breached, in accordance with section 121 (opens in a new tab) of the Act.

Operators should take note of the following licence conditions and codes of practice, in particular:

Licence condition 12.1.1, which requires operators to:

- Conduct an assessment of the risks of their business being used for money laundering and terrorist financing.
- Have appropriate policies, procedures and controls to prevent money laundering and terrorist financing.
- Ensure that such policies, procedures and controls are implemented effectively, kept under review, revised appropriately to ensure that they remain effective, and take into account any applicable learning or guidelines published by the Gambling Commission from time to time.
- Licence condition 15.2.1 (4c), which requires operators to report the appointment of a person to a position where the holder of which has overall responsibility for the licensee's AML/CTF compliance and/or for the reporting of known or suspected money laundering or terrorist financing activity.
- Licence condition 15.2.2 (1d), which requires operators to report any actual or potential breaches by the licensee of the requirements imposed by or under Parts 7 (link opens in a new window) or 8 (opens in a new tab) of the Proceeds of Crime Act 2002, or Part III (opens in a new tab) of the Terrorism Act 2000.
- Ordinary code 2.1.1, which requires operators to act in accordance with the Commission's advice on POCA.

The Proceeds of Crime Act 2002

POCA defines criminal property as property which constitutes a person's benefit from criminal conduct or represents such a benefit, in whole or in part, whether directly or indirectly, and the alleged offender knows or suspects it constitutes or represents such a benefit.

Criminal conduct is defined as conduct which constitutes an offence in any part of the United Kingdom or would constitute an offence in any part of the United Kingdom if it occurred there.

A person benefits from criminal conduct if they obtain property as a result of or in connection with the conduct. If a person benefits from criminal conduct, their benefit is the property obtained as a result of, or in connection with, the conduct. Property is gained by a person if they obtain an interest in it.

POCA creates several principal offences that apply to everyone and criminalise any involvement in the proceeds of any crime if the person knows or suspects that the property is criminal property (Section 327 (opens in a new tab), 328 (opens in a new tab) and 329 (opens in a new tab) of POCA).

These offences relate to the concealing, disguising, converting, transferring, acquisition, use and possession of criminal property, as well as an arrangement which facilitates the acquisition, retention, use or control of criminal property. For example, in the gambling industry, this may involve the taking of cash, cheque, or card payments, based on funds which are the proceeds of crime, in the form of a bet or wager, or holding money on account for a customer for the purposes of gambling.

POCA and the offences under POCA are discussed in The Proceeds of Crime Act 2002 and Offences under the Proceeds of Crime Act 2002 of this advice.

Risk-based approach

A risk-based approach focuses effort where it is most needed and will have most impact. It requires the full commitment and support of senior management, and the active co- operation of all employees.

A risk-based approach involves a number of steps to assess the most proportionate way to manage and mitigate the risks faced by the operator:

- identifying the money laundering risks relevant to the operator
- designing and implementing policies, procedures and controls to manage and mitigate the risks
- monitoring and improving the effective operation of these controls
- recording what has been done, and why.

The possibility of gambling being used by criminals to assist in money laundering poses many risks for operators. These include criminal and regulatory sanctions for operators and their employees (including the potential loss of licences), civil action against the operator, damage to the reputation of the operator leading to a loss of business, and inflated or false business performance.

Operators need to continually identify, assess and prevent these risks, just like any other business risk. Operators should assess the level of risk in the context of how their business is structured and operated, and the controls in place to minimise the risks posed to their business by money launderers, including those engaged in criminal spend.

The risk-based approach is discussed in Risk-based approach of this advice.

Customer relationships

Operators should be mindful that some risk indicators (for example, a pattern of increasing spend, spend inconsistent with apparent source of income or unusual patterns of play) could be indicative of money laundering, but also equally of problem gambling, or both (or, possibly, neither).

Given that operators have the responsibility to prevent gambling from being associated with crime and disorder and protecting vulnerable people from being harmed by gambling, they should carry out appropriate enquiries and assessments which help them in fulfilling that role. It is important that the operator is able to continually access and understand information relating to gambling activity by the same customer in different parts of the business so that the operator has a fuller picture of the risks to which they are exposed.

Customer relationships consist of the following three aspects:

- the establishment of the business relationship with the customer
- the monitoring of customer activity, including account deposits and withdrawals
- the termination of the business relationship with the customer.

In all instances of the relationship it is necessary to consider whether the customer is engaging in money laundering, including criminal spend, and to report suspicious activity and seek a defence (appropriate consent) where appropriate, as well as considering any risk to the licensing objectives.

Customer relationships are discussed in Customer relationships of this advice.

Duties under the Proceeds of Crime Act 2002

POCA imposes duties on all operators to:

- disclose instances where operators know or suspect that another person is engaged in money laundering
- make disclosures in the prescribed form and manner
- obtain a defence (appropriate consent) to do a prohibited act, where appropriate.

If a person carries out any action contemplated under the principal money laundering offences, the person can potentially commit one or more of the principal offences, except if an authorised disclosure is made prior to carrying out the action. The principal offences can be committed by any employee of the operator, except if a report is made to the NCA and, where applicable, a defence (appropriate consent) is obtained from the NCA. Therefore, in all instances where customers' funds are known or suspected to have criminal origins, a report must be made to the NCA at the earliest opportunity.

Nominated officer

Whilst it is only incumbent upon those companies in the regulated sector (which, in the gambling industry, currently includes non-remote and remote casinos) to appoint nominated officers, the Commission recommends that operators in the non-regulated sector also consider appointing a nominated officer, as this will help them meet their obligations under POCA more effectively.

Where a nominated officer is appointed, they will normally be responsible for ensuring that, when appropriate, information or any other matter leading to knowledge or suspicion of money laundering is properly disclosed to the NCA. The decision to report or not to report suspicious activity is the responsibility of the nominated officer.

The nominated officer will:

- receive internal disclosures under Part 7 of POCA (opens in a new tab)
- decide whether these disclosures should be reported to the NCA
- if appropriate, make such external reports to the NCA
- ensure that a defence (appropriate consent) is applied for, as necessary.

The nominated officer should record all decisions made in this regard.

Suspicious activity reporting

All operators 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

that a person is engaged in money laundering, including criminal spend.

In order to provide a framework within which suspicious activity reports (SARs) may be raised and considered:

- each operator should ensure that employees make reports to the operator’s nominated officer, or an employee in a managerial capacity, where they know or suspect that a person is engaged in money laundering

- the nominated officer, or the manager, should consider each report, and determine whether it warrants the submission of a SAR
- operators should ensure that employees are appropriately trained.

Knowledge means actual knowledge. Having knowledge means actually knowing something to be true. In a criminal court, it must be proved that the individual in fact knew that a person was engaged in money laundering.

Whether you hold suspicion or not is a subjective test. Being suspicious of a transaction does not require knowledge of the exact nature of the criminal offence or that the funds are definitely those arising from the crime.

In order for a disclosure to the NCA to be made, it is not necessary to know or to establish the exact nature of any underlying criminal offence, or that the particular funds or property were definitely those arising from a crime. Furthermore, it is not necessary to await conviction of a customer for money laundering or other criminal offences in order to generate suspicion that money laundering has taken place.

If operators handle any proceeds of crime, they may commit a principal money laundering offence. However, if the operator submits a SAR to the NCA, this may provide a defence. There is a statutory mechanism which allows the NCA either to grant or refuse the 'prohibited act' going ahead. This statutory mechanism is called 'appropriate consent' and is referred to by the NCA as 'requesting a defence from the NCA under POCA and TACT'.

A defence (appropriate consent) is granted by the NCA's United Kingdom Financial Intelligence Unit (UKFIU) Consent Desk, who carry out the necessary internal enquiries, and will contact the appropriate law enforcement agency, where necessary, for a defence (consent) recommendation. Once the NCA’s decision has been reached, the disclosing operator will be informed of the decision by telephone, and be given a reference number, which should be recorded, along with the operator’s record of decisions made.

Operators duties under POCA, the status and role of the nominated officer, suspicious activity and reporting, and requesting a defence (appropriate consent) are discussed in Duties under the Proceeds of Crime Act 2002 of this advice.

Failing to report (nominated officer)

POCA creates an offence of failing to report suspicious activity (failure to disclose). Where a person nominated by the operator to receive disclosures fails to comply with the obligation to make a report to the NCA as soon as practicable after the information is received, that person is open to criminal prosecution.

! **Warning The criminal sanction under POCA is a prison term of up to five years and/or a fine.**

The offence of failing to report is discussed in Failing to report (nominated officer) of this advice.

After a report has been made

When an enquiry is under investigation, the investigating officer may contact the operator to ensure that they have all the relevant information which supports the original disclosure.

The investigating officer will work closely with the operator, who will normally receive direct feedback on the stage reached in the investigation.

This is discussed in more detail in after a report has been made.

Prejudicing an investigation

Where a confiscation investigation, a civil recovery investigation or a money laundering investigation is being, or is about to be, conducted, it is a criminal offence for anyone to release information which is likely to prejudice the investigation. It is also a criminal offence to falsify, conceal, destroy or otherwise dispose of documents which are relevant to the investigation (or to cause or permit these offences).

There are a number of defences to the offence, including that the person did not know or suspect that the disclosure is likely to prejudice the investigation. The offence of prejudicing an investigation can be committed before or after a disclosure has been made.

Reasonable enquiries of a customer regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity, and may be driven by social responsibility concerns, should not result in the offence of prejudicing an investigation, unless you know or suspect that an investigation is current or impending and, importantly, make the enquiries in a way that it discloses those facts.

The prejudicing an investigation offence is discussed in Prejudicing an investigation of this advice.

Training

Under POCA, employees face criminal penalties if they are involved in money laundering, unless they make a report of known or suspected money laundering activity. It is important, therefore, that employees are made aware of their legal obligations and how to correctly discharge them.

Operators should also take reasonable steps to ensure that employees are aware of the money laundering risks faced by the operator, the operator’s procedures for managing those risks, the identity and responsibilities of the person responsible for making reports to the NCA, and the potential effect of a breach of POCA on the operator and its employees.

Training is discussed further in Part 2 - the advice in this guide.

Terrorist financing

The Terrorism Act 2000 (opens in a new tab) establishes several offences about engaging in or facilitating terrorism, as well as raising or possessing funds for terrorist purposes. The Terrorism Act also contains defences to the principal terrorist property offences, in a similar way to POCA. Operators should report instances of suspected terrorist financing to the NCA using the same methods as those for the reporting of known or suspected money laundering activity.

Terrorist financing is discussed in Terrorist financing of this advice.

The advice

What is meant by the proceeds of crime and money laundering?

Broadly, the term 'proceeds of crime' or 'criminal proceeds' refers to all property from which a person benefits directly or indirectly, by being party to criminal conduct, for example, money from drug dealing or stolen in a burglary or robbery (this is commonly referred to as criminal property). It also includes property that a person gains by spending the proceeds of criminal conduct, for example, if a person uses money earned from drug dealing to buy a car or a house, or spends money gained in a bank robbery to gamble.

Typically, classic money laundering consists of a number of stages:

- placement
- layering
- integration.

1. ## Placement

Placement is the first stage in the money laundering cycle. The laundering of criminal proceeds is often required because of the cash-intensive nature of the underlying crime (for example, drug dealing where payments take the form of cash, often in small denominations). The monies are placed into the financial system or retail market, or are smuggled to another country. The aim of the

money launderer is to avoid detection by the authorities and to then transform the criminal proceeds into other assets.

---

2. Layering

Layering is the next stage and is an attempt to conceal or disguise the source and ownership of the criminal proceeds by creating complex layers of financial transactions which obscure the audit trail and provide anonymity. The purpose of layering is to disassociate the criminal proceeds from the criminal activity which generated them. Typically, layers are created by moving monies in and out of various accounts and using electronic fund transfers.

---

3. Integration

Integration is the final stage in the process. It involves integrating the criminal proceeds into the legitimate economic and financial system, and assimilating it with other assets in the system. Integration of the 'clean' money into the economy is accomplished by the money launderer making it appear to have been legally earned.

There is potential for the money launderer to use gambling at every stage of the process.

The land-based gambling industry is particularly vulnerable during the placement stage as the use of cash is prevalent and the provenance of such cash is not easy to determine. Although the remote gambling industry might appear less vulnerable as electronic transfers are required for placements, identify theft and identify fraud can enable the money launderer to move criminal proceeds with anonymity. Furthermore, the use of multiple internet transactions can facilitate the layering stage of money laundering.

Operators should be mindful that the offence of money laundering also includes simple criminal spend (the use of criminal proceeds to fund gambling as a leisure activity), and may not include all the typical stages of the laundering process (if any at all).

The Proceeds of Crime Act 2002

In section 340 of POCA (opens in a new tab), criminal property is defined as property which:

- constitutes a person's benefit from criminal conduct or represents such a benefit, in whole or in part, and whether directly or indirectly
- and the alleged offender knows or suspects it constitutes or represents such a benefit.

It is immaterial who carried out the criminal conduct, who benefited from it and whether the conduct occurred before or after the passing of POCA.

Criminal conduct, in turn, is defined as conduct which:

- constitutes an offence in any part of the United Kingdom
- or would constitute an offence in any part of the United Kingdom if it occurred there.

  This means that offences from which the proceeds of crime are generated are relevant for these purposes even if the principal offence was committed abroad, so long as the principal offence would also be a crime if it was committed in the United Kingdom.

A person benefits from conduct if they obtain property as a result of or in connection with the conduct. If a person benefits from criminal conduct, their benefit is the property obtained as a result of, or in connection with, the conduct. Property includes money, all forms of property, real (for example, land and buildings) or personal (for example, cars, furniture and clothing), inherited or moveable (for example, machinery and livestock), and intangible property (for example, trademarks, copyrights and patents). Property is obtained by a person if he obtains an interest in it. Property is 'criminal property' if it is a person's benefit from criminal conduct or it represents such benefit, either directly or indirectly, as long as the alleged offender knows or suspects that it constitutes or represents such a benefit.

If a person gains a financial advantage as a result of, or in connection, with criminal conduct, he is to be taken to have obtained a sum of money equal to the value of the financial advantage.

The principal money laundering offences specified within POCA criminalise a person's dealings with criminal property, subject to certain exceptions. The principal offences and the exceptions are discussed next.

Offences under the Proceeds of Crime Act 2002

The criminal offences of money laundering were first introduced in the United Kingdom in the Criminal Justice Act 1988 (opens in a new tab) and the Drug Trafficking Offences Act 1986 (opens in a new tab). POCA consolidated, updated and reformed the criminal law relating to money laundering to include any

dealing in criminal property, which is defined widely as the proceeds of any type of crime, however small the amount.

POCA applies to everyone, although certain offences relating to the failure to report (except in relation to a nominated officer) and 'tipping off' only apply to those operating in the regulated sector. The businesses that fall within the regulated sector are specified in Schedule 9 of POCA (opens in a new tab), and include credit institutions, financial institutions, auditors, insolvency practitioners, external accountants, tax advisers, independent legal professionals, trust or company service providers, estate agents, high value dealers and casino operators.

POCA creates several principal offences that apply to everyone and criminalise any involvement in the proceeds of any crime if the person knows or suspects that the property is criminal property (Sections 327 (opens in a new tab), 328 (opens in a new tab) and 329 (opens in a new tab) of POCA). These offences relate to the concealing, disguising, converting, transferring, acquisition, use and possession of criminal property, as well as an arrangement which facilitates the acquisition, retention, use or control of criminal property. For example, in the gambling industry, this may involve the taking of cash, cheque or card payments, based on funds which are the proceeds of crime, in the form of a bet or wager, or holding money on account for a customer for the purposes of gambling.

Section 327 (opens in a new tab) of POCA provides that a person commits an offence if they:

- conceal criminal property (for example, by depositing funds obtained through criminal activity into a gambling account)
- disguise criminal property (for example, by placing funds obtained through criminal activity into a gambling account and then withdrawing them at a later date)
- convert criminal property (for example, by placing bets in a gambling establishment and then cashing in the winnings)
- transfer criminal property (for example, by transferring property to another person or to a gambling operator)
- remove criminal property from the United Kingdom (for example, by taking their winnings overseas).

Concealing or disguising property includes concealing or disguising its nature, source, location, disposition, movement or ownership, or any rights with respect to it. Whilst 'converting' criminal property is not defined in POCA, it is suggested that this be given its conventional legal meaning, that is that the 'converter' has dealt with the property in a manner inconsistent with the rights of the true owner of the property. For example, a criminal steals cash in a bank robbery and then uses that cash to open a gambling account and place bets.

Section 328 (opens in a new tab) of POCA provides that a person commits an offence if they enter into or become concerned in an arrangement which they know or suspect facilitates, by whatever means, the acquisition, retention, use or control of criminal property by or on behalf of another person. An example of this in the gambling industry would be for an operator knowingly to accept stakes that are the proceeds of criminal activity.

Section 329(1) (opens in a new tab) of POCA provides that a person commits an offence if they:

- acquire criminal property
- use criminal property
- have possession of criminal property (for example, via stakes).

Acquisition, use and possession under section 329(1) (opens in a new tab) includes, for example, when a person carries, holds or looks after criminal property or acquires criminal property for 'inadequate consideration'. This means when a person buys or exchanges something which is significantly below market value (inadequate consideration). However, a person does not commit such an offence if they acquire or use or have possession of the property for adequate consideration.

The principal money laundering offences are wide and can be committed by anyone, including, for example, an employee of an operator, who has knowledge or suspicion that a customer is using the proceeds of crime, or has possession of the proceeds of criminal activity.

The offence of money laundering and the duty to report under POCA apply in relation to the proceeds of any criminal activity, wherever conducted, including abroad, that would constitute an offence if it took place in the United Kingdom. However, a person does not commit an offence of money laundering where it is known or believed, on reasonable grounds, that the relevant criminal conduct occurred outside the United Kingdom and the relevant conduct was not criminal in the country where it took place and is not of a description prescribed by an order made by the Secretary of State (Section 327(2A) (opens in a new tab) of POCA).

The money laundering offences assume that a criminal offence has occurred in order to generate the criminal property which is now being laundered. This is often known as a predicate offence. No conviction for the predicate offence is necessary for a person to be prosecuted for a money laundering offence (note that, following the decision in relation to R v Anwoir [2008] 2 Cr. App. R. 36, the Prosecution does not need to prove a specific criminal offence, but can instead show that it derived from conduct of a specific kind or kinds and that conduct of that kind or those kinds was unlawful, and by evidence of the circumstances in which the property had been handled, which were such as to give rise to the irresistible inference that it could only have been derived from crime).

While POCA places responsibilities on operators, the legislation also gives them protection if they report suspicious activity. Operators will have a defence to the principal money laundering offences in sections 327 (opens in a new tab), 328 (opens in a new tab) or 329 (opens in a new tab) of POCA if they:

- make an authorised disclosure under section 338 (opens in a new tab) of POCA prior to the offence being committed and obtain a defence (appropriate consent) under section 335 (opens in a new tab) of POCA (the consent defence)
- intended to make an authorised disclosure but had a reasonable excuse for not doing so (the reasonable excuse defence).

Authorised disclosures and requesting a defence (appropriate consent) are discussed in Duties under the Proceeds of Crime Act 2002 of this advice.

! **Warning The penalty for conviction on indictment for an offence under sections 327 (opens in a new tab), 328 (opens in a new tab) or 329 (opens in a new tab) of POCA is imprisonment for a term not exceeding 14 years, a fine, or both (Section 334 (opens in a new tab) of POCA).**

In addition, POCA contains provisions for the recovery of the proceeds of crime and forfeiture can be granted, regardless of whether a conviction for any offence has been obtained or is intended to be obtained. Under certain circumstances, criminal property can be recoverable even if it is disposed of to another person (Section 304 (opens in a new tab) of POCA).

Risk-based approach

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

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

The possibility of gambling facilities being used by criminals to assist in money laundering poses many risks for operators. These include criminal and regulatory sanctions for operators and their employees, civil action against the operator and damage to the reputation of the operator, leading to a potential loss of business.

Operators need to continually identify, assess and manage these risks, just like any other business risk. They should assess the level of risk in the context of how their business is structured and operated, and the controls in place to minimise the risks posed to their business by money launderers, including those engaged in criminal spend. The risk-based approach means that operators focus their resources on the areas which represent the greatest risk. The benefits of this approach include a more efficient and effective use of resources, minimising compliance costs and the flexibility to respond to new risks as money laundering methods change.

Most operators manage their commercial or business risks and measure the effectiveness of the policies, procedures and controls they have put in place to manage those risks. A similar approach is appropriate to managing the operator’s regulatory risks, including money laundering risks. Existing risk management systems should, therefore, address the regulatory and money laundering risks, or a separate system should be in place for that purpose. The detail and complexity of these systems will depend on the operator’s size and the complexity of their business.

Even though operators outside the regulated sector (clarified in Offences under the Proceeds of Crime Act 2002 are not obliged to have systems and procedures in place under AML legislation, the Commission nonetheless expects AML systems and procedures to be in place in accordance with the relevant licence conditions and codes of practice. Also, POCA imposes obligations on all operators that must be satisfied, as a breach can constitute a criminal offence (Sections 327 (opens in a new tab) to 332 (opens in a new tab) of POCA). Systems and procedures assist operators in complying with these obligations, particularly in relation to reporting suspicious activity.

In order to detect customer activity that may be suspicious, it is necessary to monitor all transactions or activity. The monitoring of customer activity should be carried out using a risk-based approach. Higher risk customers should be subjected to a frequency and depth of scrutiny greater than may be appropriate for lower risk customers. Operators should be aware that the level of risk attributed to customers may not correspond to their commercial value to the business.

Where a customer is assessed as presenting a higher risk, additional information in respect of that customer should be collected. This will help the operator judge whether the higher risk that the customer is perceived to present is likely to materialise, and provide grounds for proportionate and recorded decisions. Such additional information should include an understanding of where the customer’s funds and wealth have come from. The need to 'know your customer' (KYC) is particularly relevant here. While the Commission recognises that some relationships with customers will be transient or temporary in nature, operators still need to give consideration to this issue in relation to all customers.

Operators should satisfy themselves that the sources of information employed to carry out KYC checks are suitable to mitigate the full range of risks to which they might be exposed, and these include money laundering and social responsibility risks. For example, local or open source information, such as press reports, may be particularly helpful in carrying out these checks.

Deciding that a customer presents a higher risk of money laundering does not automatically mean that the person is a criminal or is laundering money. Similarly, identifying a customer as having a low risk of money laundering does not mean that the customer is definitely not laundering money or engaging in criminal spend. Operators, therefore, need to remain vigilant and use their experience and judgement in applying their risk-based criteria and rules.

No system of checks will detect and prevent all money laundering activity. A risk-based approach will, however, serve to balance the burden placed on operators and their customers with a realistic assessment of the threat of the operator being involved, albeit unintentionally, in money laundering. It focuses the effort where it is most needed and will have the most impact. It is not a blanket, one size fits all approach, and therefore operators have a degree of flexibility in the methods they employ.

A risk-based approach requires the full commitment and support of senior management, and the active co-operation of all employees. It should be part of the operator's philosophy and be reflected in an operator's policies, procedures and controls. There needs to be clear communication of the policies, procedures and controls to all employees, along with robust mechanisms to ensure that they are carried out effectively, weaknesses are identified and improvements are made, wherever necessary. Where the operator forms part of a larger group of companies, there needs to be sufficient senior management oversight of the management of risk.

Identifying and assessing the risks

The operator should assess its risks in the context of how it is most likely to be involved in money laundering and criminal spend. Assessment of risk is based on a number of questions, including:

Questions

- What risk is posed by the business profile and the profile of customers using the gambling facilities?
- Is the business high volume, consisting of many low spending customers?
- Is the business low volume, with high spending customers?

- Is the business a mixed portfolio, that is, customers are a mix of high spenders and lower spenders and/or a mix of regular and occasional customers?
- Are procedures in place to monitor customer transactions across outlets, products and platforms and mitigate any money laundering potential?
- Is the business local with regular and generally well known customers?
- Are there a large proportion of overseas customers using foreign currency or overseas based bank cheques or debit cards?
- Are customers likely to be engaged in a business which involves significant amounts of cash?
- Are there likely to be situations where the source of funds cannot be easily established or explained by the customer?
- Is the majority of business conducted through customer accounts or some other contractual arrangement?
- Is there a local clustering of gambling outlets which makes it easier for a person to launder criminal proceeds over multiple venues and products?
- Does the customer have multiple or continually changing sources of funds (for example, multiple bank accounts and cash, particularly where this is in different currencies or uncommon bank notes)?
- Are patterns of play or a high spend profile linked to specific sporting events?
- In relation to remote gaming, does the customer use shared internet protocol addresses, dormant accounts or virtual private network (VPN) connections (amongst other things, this could indicate that a group of people are using the same device or location to gamble for the purposes of committing fraud)?

As noted in Purpose of the advice, 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 is based, among other things, on the risks posed to the operator by 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.

The World Economic Forum provide an example (opens in a new tab) of good practice guidelines on conducting third party due diligence.

Risk assessments

A money laundering risk assessment is a product or process based on a methodology, agreed by the parties involved, that attempts to identify, analyse and understand money laundering risks. It serves as the first step in addressing the risks and, ideally, involves making judgments about threats, vulnerabilities and consequences.

Risk, therefore, is a function of three factors:

- **threats** – which are persons, or groups of people, objects or activities with the potential to cause harm, including criminals, terrorist groups and their facilitators, their funds, as well as past, present and future money laundering activities
- **vulnerabilities** – which are those things that can be exploited by the threat or that may support or facilitate its activities and means focussing on the factors that represent weaknesses in AML systems or controls or certain features of a country, particular sector, financial product or type of service that make them attractive for money laundering
- **consequences** – which refers to the impact or harm that money laundering may cause, including the effect of the underlying criminal and terrorist activity on financial systems and institutions, the economy and society more generally.

The key to any risk assessment is that it adopts an approach that attempts to distinguish the extent of different risks to assist with prioritising mitigation efforts. The risk assessment process should consist of the following standard stages:

- identification
- analysis
- evaluation.

The identification process begins by developing an initial list of potential risks or risk factors when combating money laundering. Risk factors are the specific threats or vulnerabilities that are the causes, sources or drivers of money laundering risks. This list will be drawn from known or suspected threats or vulnerabilities. The identification process should be as comprehensive as possible, although newly identified or previously unidentified risks may also be considered at any stage in the process.

Analysis involves consideration of the nature, sources, likelihood, impact and consequences of the identified risks or risk factors. The aim of this stage is to gain a comprehensive understanding of each of the risks, as a combination of threat, vulnerability and consequence, in order to assign a relative value or importance to each of them. Risk analysis can be undertaken with varying degrees of detail, depending on the type of risk, the purpose of the risk assessment, and the information, data and resources available.

The evaluation stage involves assessing the risks analysed during the previous stage to determine priorities for addressing them, taking into account the purpose established at the beginning of the assessment process. These priorities can then contribute to development of a strategy for the mitigation of the risks.

Money laundering risks may be measured using a number of factors. Application of risk categories to customers and situations can provide a strategy for managing potential risks by enabling operators to subject customers to proportionate controls and monitoring. The risk categories which should be considered are as follows:

- country or geographic risk
- customer risk
- transaction risk
- product risk.

The risk categories used by the Commission in **Money laundering and terrorist financing risk within the British gambling industry** are customer, product and means of payment.

Country/geographic risk

Some countries pose an inherently higher money laundering risk than others. In addition to considering their own experiences, operators (particularly those who operate in a remote environment) should take into account a variety of other credible sources of information identifying countries with risk factors in order to determine that a country and customers from that country pose a higher risk. Operators may wish to assess information available from non-governmental organisations which can provide a useful guide to perceptions relating to corruption in the majority of countries.

Customers that are associated with higher risk countries, as a result of their citizenship, country of business or country of residence may present a higher money laundering risk, taking into account all other relevant factors. Remote operators should check customer location because of the additional risks which arise from cross-border operations.

The country/geographic risk can also be considered in conjunction with the customer risk.

Customer risk

Determining the potential money laundering risks posed by a customer, or category of customers, is critical to the development and implementation of an overall risk-based framework. Based on their own criteria, operators should seek to determine whether a particular customer poses a higher risk and the potential impact of any mitigating factors on that assessment. Application of risk variables may mitigate or exacerbate the risk assessment. Categories of customers whose activities may indicate a higher risk include:

- unknown or anonymous customers
- high spenders – the level of spending which will be considered to be high for an individual customer will vary among operators, and among premises managed by the same operator
- disproportionate spenders – where appropriate, operators should obtain information about customers' financial resources so that they can determine whether customers' spending is proportionate to their income or wealth
- casual customers – this includes tourists and local customers who are infrequent visitors
- regular customers with changing or unusual spending patterns
- customers using forged or stolen identities to remain anonymous
- customers from high risk or non-cooperative jurisdictions (see, in particular a list of high risk and non-cooperative jurisdictions (opens in a new tab))
- customers who appear on international sanctions lists (see, in particular consolidated list of financial sanctions targets (opens in a new tab))
- customers who are citizens or residents of, or associated with, countries assessed by non-government organisations as high risk for corruption and financial crime (for example, Transparency

International (link opens in a new window) and Global Witness (opens in a new tab).

Transaction risk (including means of payment)

Operators should consider operational aspects (products, services, games, accounts and account activities) that can be used to facilitate money laundering. In addition, operators have the following potential transaction risks:

- proceeds of crime – there is a risk that the money used by a customer has been gained through criminal activity, so greater monitoring of high spenders will help to mitigate the risk
- cash – customers may use gambling premises to exchange large amounts of criminal proceeds, or may deposit criminal proceeds into an internet gambling account at gambling premises, including tracks
- transfers between customers – customers may borrow money from unconventional sources, including other customers, which can offer criminals an opportunity to introduce criminal proceeds into the legitimate financial system through the gambling operator
- depositing into accounts – criminals may use accounts to deposit criminal proceeds and then withdraw funds with little or no play
- redemption of tickets for cash or cheque, particularly after minimal or no play
- multiple gambling accounts or wallets – customers may open multiple accounts or wallets with an operator in order to obscure their spending levels or to avoid CDD threshold checks
- changes to bank accounts – customers may hold a number of bank accounts and regularly change the bank account they use for gambling purposes
- identity fraud – details of bank accounts may be stolen and used on, for example, remote gambling websites, or stolen identities may be used to open bank accounts or gambling accounts
- pre-paid cards – these cards pose the same risks as cash as operators normally cannot perform the same level of checks on the cards as they can on bank accounts
- e-wallets – some e-wallets accept cash on deposit or digital currencies, which pose a higher risk, and some customers may use e-wallets to disguise their gambling.

Product risk

Product risk includes the consideration of the vulnerabilities associated with the particular products offered by the gambling operator. In non-remote premises there are a number of gambling opportunities that offer the potential for a money launderer to place funds anonymously and generate winnings, or withdraw funds after minimal play. These are more fully discussed below, and include the use of cash and automated

ticket redemption facilities where there is little or no interaction with staff. Remote gambling products present a heightened money laundering risk as the customers who use the products are not present.

Examples of products which may pose a money laundering risk therefore include:

- gaming machines, which can be used to launder stained or fraudulent bank notes/coins
- the use of automated ticket redemption machines, which allow a customer to avoid interaction with staff
- scratchcards (in the lottery sector)
- interactive win games and draw-based games (in the lottery sector).

The risk categories or factors described above are not intended to be prescriptive or comprehensive. They will not apply universally to all operators and, even when they are present, there may be different risk outcomes for different operators and premises, depending upon a host of other factors. However, the factors are intended as a guide to help operators conduct their own risk assessments, and to devise AML/CTF policies, procedures and controls which accurately and proportionately reflect those assessments.

The weight given to the risk factors used by the operator in assessing the overall risk of money laundering, both individually or in combination, may vary from one operator or premises to another, depending on their respective circumstances. Consequently, operators also have to make their own determination as to the weight given to risk factors.

Risk levels may be impacted by a number of variables, which will also have an impact on the preventative measures necessary to tackle the risks in a proportionate manner. These variables include:

- whether the operator’s business model is focused on:
- attracting a large number of customers who gamble relatively small amounts
- attracting a small number of customers who gamble relatively large amounts
- speed and volume of business
- for non-remote operators, the size of the premises
- the customer profile, for example whether:
- the majority of customers are regular visitors or are members
- the operator relies on passing trade, including tourists
- types of financial services offered to customers
- types of customer payments and payment methods
- types of gambling products offered
- the customers’ gambling habits
- staffing levels, and staff experience and turnover
- the type and effectiveness of existing gambling supervision measures and mechanisms

- whether the operator:
- owns or manages other gambling establishments
- offers different types of gambling
- has other internet gambling websites
- whether the premises are standalone or integrated with other leisure facilities
- whether the operator is based in one country or has a gambling presence in multiple countries.

Many customers carry a lower risk of money laundering. These might include customers who are regularly employed or who have a regular source of income from a known source which supports the activity being undertaken (this applies equally to pensioners, benefit recipients or to those whose income originates from their partner's employment or income).

Conversely, many customers carry a higher risk of money laundering. These may include known criminals, customers who are not regularly employed or who do not have a regular source of income from a known source which supports the level of activity being undertaken, or problem gamblers.

Examples

A drug dealer, whose only legitimate source of income for ten years was > state benefits, spent more than £1million in various gambling establishments over the course of two years, and lost some £200,000. All the transactions appeared to involve cash.

A grandparent with no previous gambling history, on a state pension, began to make weekly bets of about £100. Investigations later revealed that the grandparent was placing the bets on behalf of a grandson, a known criminal, and that the money spent was the proceeds of his criminal activity.

An individual was in receipt of state benefits with no other apparent form of income, but then gambled significant amounts through a licensed operator. Deposits of over £2million were made to an online gambling account over the course of about two years from a multiple of sources, such as debit card and credit card, and various e-money and e-wallet services. Investigations revealed that their gambling was funded by criminal activity.

Over an extended period of time, an individual who claimed to be a gambling addict stole equipment worth a substantial amount of money from their employer and resold it for their own gain. They then used most of these criminal proceeds to gamble, depositing almost £6million into an online gambling account and losing almost £5million, involving about 40,000 individual gambling transactions. The individual remained in employment throughout this period.

Operators are best placed to identify and mitigate risks involved in their business activity. A crucial element of this is to ensure that systems are in place to identify and link player activity, and for senior management to oversee risk management and determine whether their policies and procedures are effective in design and application. Reliance on third parties to conduct risk assessment and management does not relieve the operator of its ultimate responsibility to assess and manage its own risks (in accordance with licence condition 12.1.1).

A money laundering risk assessment is not a one-off exercise. The relevant licence condition requires operators to review their money laundering risk assessments at least annually, but they 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.

Operators should ensure that their policies, procedures and controls for managing money laundering risks, including the detection of criminal spend, are kept under regular review. For example, industry innovation may expose operators to new risks and an appropriate assessment of the risk is recommended before implementing any new product, system, control, process or improvement.

Customer relationships

Operators should be mindful that some risk indicators (for example, a pattern of increasing spend or spend inconsistent with apparent source of income) could be indicative of money laundering, but also equally of problem gambling, or both. There may also be patterns of play (for example, chasing losses) that appear to be indicative of problem gambling that could also be considered to indicate other risks (for example, spend that is inconsistent with the individual's apparent legitimate income could be the proceeds of crime). While patterns of play may be one indicator of risk, operators should satisfy themselves that they have asked, or are prepared to ask, the necessary questions of customers when deciding whether to establish a business relationship, maintain the relationship or terminate the relationship. In summary, it is perfectly plausible that an individual attempting to spend criminal proceeds or launder money could also be a problem gambler, but one does not necessarily follow the other. The responsibility is on the operator to be in a position to understand these dynamics and mitigate any risks to the licensing objectives.

Operators are subject to both certain provisions of POCA and the Act (and the relevant licence conditions and codes of practice). Operators have the responsibility to comply with the licensing objectives and, therefore, they should carry out appropriate enquiries and assessments to ensure that they do so. While the conclusions drawn and actions taken may differ according to whether money laundering and/or social responsibility risks are identified, the effective identification and management of these risks rests upon the ability of operators to have a comprehensive knowledge of their customer relationships and for managers to be clear on their responsibilities.

It is also important that the operator is able to reconcile information relating to customers' gambling activities in different parts of the business so that they have a more complete picture of the risks posed by the activities of individual customers.

Commercial and business information should be considered for AML as well as social responsibility purposes when transacting with an individual. This should include arrangements for the monitoring of customers with whom a business relationship has been established. For example, information about customer spend can be used by the operator to proactively monitor high risk customers in relation to their money laundering risk.

Customer relationships need to be managed proficiently and records should be maintained as to what information was communicated to the customer, why it was communicated and what considerations were made. If players expect that customer interaction is likely should they play with large amounts of money, or for lengthy periods, and such interaction is consistently applied, there would be less reason for customers to question or become suspicious of the motives of these interactions. Operators may find it helpful to provide their customers with a leaflet which explains why they are being asked questions about their game play.

The Commission recognises that some operators may find their obligations under POCA challenging, particularly in relation to the management of customer relationships, but it is incumbent on operators to have policies, procedures and controls in place to ensure that they comply with all relevant provisions of POCA (and the Act and the relevant licence conditions and codes of practice), in particular in relation to

the reporting of money laundering activity by customers and the obtaining of a defence (appropriate consent) where necessary.

Customer relationships for AML purposes consist of three aspects:

- the establishment of the business relationship with the customer
- the monitoring of customer activity, including account deposits and withdrawals
- the termination of the business relationship with the customer.

At all stages of the relationship it is necessary to consider whether the customer is engaging in money laundering (including criminal spend); whether there is a need to report suspicious activity and seek a defence (appropriate consent); and any risks posed to the licensing objectives.

Establishment of business relationship

The establishment of a business relationship with a customer is likely to occur when, for example, the customer:

- places a wager or bet with the operator using cash or cheque, or pays using a bank or similar card
- opens a gambling account with the operator or joins a membership scheme (where one is offered by the operator)
- places money on account with the operator.

When establishing a business relationship, operators will need to give consideration to the following:

- the potential money laundering risk posed by the customer
- whether it is necessary to do KYC or due diligence checks on the customer
- whether it is known or suspected that the customer may launder money (including criminal spend).

Where the operator becomes aware that the customer is attempting to use the operator to launder criminal proceeds (including criminal spend), the operator must carefully consider whether either not to establish the business relationship, or to suspend or terminate the business relationship at the earliest opportunity. In either case, it is recommended that a SAR is submitted to the NCA and, where there are funds to be returned to the customer, seek a defence (appropriate consent) to a principal money laundering offence.

Customer monitoring

Where, through their customer profile or known pattern of gambling activity, the customer appears to pose a risk of actual or potential money laundering, the operator should monitor the gambling activity of the customer and consider whether further due diligence measures are required. This should include a decision about whether a defence (appropriate consent) should be sought for future transactions, or whether the business relationship with the customer should be terminated where the risk of breaches of POCA are too high.

Operators should ensure that the arrangements that they have in place to monitor customers and the accounts they hold across outlets, products and platforms (remote and non-remote) are sufficient to manage the risks that the operator is exposed to. This should include the monitoring of account deposits and withdrawals. Those operators that rely heavily on gaming machines should also have practical systems in place to effectively monitor and reconcile customer spend on gaming machines. Any suspicious activity should be reported by means of a SAR to the NCA.

Once knowledge or suspicion of criminal spend is linked to a customer in one area of the business (for example, over the counter bets), operators should monitor the customer’s activity in other areas of the

business (for example, gaming machine play).

If the customer's patterns of gambling lead to an increasing level of suspicion of money laundering, or to actual knowledge of money laundering, operators should seriously consider whether they wish to allow the customer to continue using their gambling facilities, otherwise the operator may potentially commit one of the principal money laundering offences.

Termination of business relationship

As already discussed, to avoid potentially committing one of the principal money laundering offences, operators need to consider ending the business relationship with a customer in the following circumstances:

- where it is known that the customer is attempting to use the operator to launder criminal proceeds or for criminal spend
- where the risk of breaches to POCA are considered by the operator to be too high
- where the customer's gambling activity leads to a steadily increasing level of suspicion, or actual knowledge, of money laundering.

Where the operator terminates a business relationship with a customer and they know or suspect that the customer has engaged in money laundering, they should seek a defence (appropriate consent) from the NCA before paying out any winnings or returning funds to the customer.

Duties under the Proceeds of Crime Act 2002

POCA imposes duties on all operators to:

- disclose instances where operators know or suspect that another person is engaged in money laundering
- and make disclosures in the prescribed form and manner
- and obtain a defence (appropriate consent) to do a prohibited act, where appropriate.

Authorised disclosures

If a person carries out any action contemplated under the principal offences discussed in Offences under the Proceeds of Crime Act 2002, the person can potentially commit one or more of the principal offences, except if an authorised disclosure is made prior to carrying out the action. The principal offences can be committed by any employee of the operator, except if a report is made to the NCA and, where applicable, a defence (appropriate consent) is obtained from the NCA (Sections 327 (2) (opens in a new tab), 328 (2) (opens in a new tab) and 329 (2) (opens in a new tab) of POCA). These authorised disclosures or reports

are referred to as SARs. A SAR is submitted where someone has knowledge, suspicion or belief that another person is laundering money.

The SAR regime for money laundering is administered by the UKFIU, which is part of the NCA. The UKFIU works with UK law enforcement, government agencies, supervisors and other international financial intelligence units to prevent and disrupt money laundering. SARs submitted to the UKFIU are processed, analysed and disseminated to UK law enforcement and other government bodies, and via the international network of financial intelligence units.

In all instances where customers' funds are known or suspected to have criminal origins, a SAR must be submitted to the NCA at the earliest opportunity using the methods set out on the NCA's website.

Operators should have a system clearly setting out the requirements for submitting SARs to the NCA. This system should include:

- the circumstances in which a disclosure (SAR) is likely to be required
- how and when information is to be provided to the person responsible for making reports to the NCA
- resources which can be used to resolve difficult issues regarding a disclosure (SAR)
- how and when a SAR is to be submitted to the NCA
- how employees can manage a customer when a SAR has been submitted and a defence (appropriate consent) is awaited
- the need to be alert to circumstances which could lead to offences of prejudicing an investigation.

Appointment of nominated officer

Whilst it is only incumbent upon those companies in the regulated sector (which, in the gambling industry, at the time of writing, includes non-remote and remote casinos) to appoint nominated officers, the Commission recommends that operators in the non-regulated sector also consider appointing a nominated officer, as this will help them meet their obligations under POCA more effectively. This can particularly assist in the reporting of suspicious activity to the NCA, as it is the nominated officer who will have this duty. The nominated officer can also give 'appropriate consent' to a transaction going ahead (this is discussed in more detail in the section Requesting a defence). Employees will also have protection from prosecution because, so long as they report any known or suspected money laundering activity to the

nominated officer (this is called 'internal disclosure'), they will have a defence to the principal money laundering offences under POCA, as the decision whether to report or not to report to the NCA and request a defence (appropriate consent) is the sole responsibility of the nominated officer.

In determining the status of the nominated officer and identifying the appropriate position for this officer within the overall organisational structure, operators need to ensure their independence within the business and that they have access to all relevant information to enable them to discharge their duties. Responsibilities will include objectively reviewing decisions and, on occasions, making recommendations that may conflict with, for instance, short term operational goals.

It is important to note, however, that the position of a nominated officer brings with it responsibilities and associated offences, if the nominated officer fails to take the required action, even though the operator may be outside the regulated sector. The responsibilities of the nominated officer and the associated offences are discussed below. Further details can be found in Part 7 (opens in a new tab) of POCA.

Where operators do not formally appoint a nominated officer, it is still advisable for an appropriately senior manager to take particular responsibility for complying with the operator's obligations under POCA. The appointment of an individual responsible for and well versed in identifying, assessing, monitoring and effectively managing money laundering risk in a comprehensive manner (proportionate to the scale and nature of the operator's activities), who can be held to account both within the operator and by external agencies, is a practical and transparent solution.

The Commission recognises that some operators (particularly small scale operators) may have a structure in which the nominated officer will hold other roles and responsibilities. The Commission is content, for example, that the nominated officer may take on other compliance roles and responsibilities. However, this is subject to the key principles set out here, including the ability to report directly to the board (or the head of the organisation) and the NCA, and the ability to make AML decisions independently of operational concerns.

Role of nominated officer

The role of the nominated officer is to apply the same rigour in their approach to managing money laundering risk as the operator does in managing its commercial systems. The nominated officer should report to the board internally (or to the chief executive for small organisations), and direct to the NCA in relation to known or suspected money laundering activity (including criminal spend) and/or to request a defence (appropriate consent).

Where a nominated officer is appointed, he will normally be responsible for ensuring that, when appropriate, information or any other matter leading to knowledge or suspicion of money laundering is properly reported to the NCA. The decision to report or not to report suspicious activity is the personal responsibility of the nominated officer. The nominated officer must also liaise with the NCA or law enforcement agencies on the issue of whether to proceed with a transaction or what information may be disclosed to customers or third parties.

Where one has been appointed by an operator, the nominated officer will:

- receive internal disclosures (internal reports) under Part 7 (opens in a new tab) of POCA
- decide whether these should be reported to the NCA
- if appropriate, make such external reports to the NCA

- ensure that a defence (appropriate consent) is requested, as necessary.

The nominated officer should record all decisions made in this regard.

The nominated officer should be able to monitor the day-to-day operation of the operator's AML policies, and respond promptly to any reasonable request for information made by the Commission or law enforcement bodies. The Commission expects the nominated officer to take ultimate managerial responsibility for AML issues, but this does not diminish senior management responsibility for AML.

Where an operator's nominated officer delegates to another employee, the nominated officer remains responsible for AML issues and is likely to remain liable for the commission of any criminal offences relating to POCA. The Commission strongly recommends that, in such circumstances:

- the fact, date and time of such delegation be entered immediately in a written record
- the delegate should counter-sign by way of acceptance of responsibility
- all employees who need to be aware of the delegation should be notified immediately.

Suspicious activities and reporting

All operators are required to make a report to the NCA in respect of information that comes to them within the course of their business:

- where they know
- or where they suspect

that a person is engaged in money laundering (including criminal spend) or attempting to launder money, if they want to avoid committing one or more of the principal offences.

Operators will only need to consider making a report if they have actual knowledge or subjective suspicion of money laundering.

In order to provide a framework within which SARs may be raised and considered:

- each operator should ensure that employees make reports to the operator's nominated officer (where one has been appointed) or an employee in a managerial capacity, where they know or suspect that a person or customer is engaged in money laundering
- the nominated officer, or the responsible manager, should consider each report, and determine whether it warrants the submission of a SAR to the NCA
- operators should ensure that employees are appropriately trained in their obligations, and the requirements for making reports to their nominated officer or the responsible manager.

If the nominated officer or responsible manager determines that a report warrants the submission of a SAR, he must report the matter to the NCA. Under POCA, the nominated officer or responsible manager is required to make a report to the NCA as soon as is practicable if he has grounds for suspicion that another person, whether or not that person is a customer, is engaged in money laundering.

What is meant by knowledge and suspicion?

In the context of POCA, knowledge means actual knowledge. Having knowledge means actually knowing something to be true. In a criminal court, it must be proved that the individual in fact knew that a person was engaged in money laundering. Knowledge can be inferred from the surrounding circumstances, so, for example, a failure to ask obvious questions may be relied upon by a court to infer knowledge (refer to Baden v Societe Generale pour Favouriser le Developpement du Commerce et de l'Industrie en France [1983] BCLC 325 and [1993] 1 WLR 509). Whether knowledge is proved to the criminal standard will depend upon the exact circumstances of the case. The knowledge must, however, have come to the operator (or to an employee) in the course of business or (in the case of a nominated officer) as a consequence of a disclosure by another employee. Information that comes to the operator or employee in other circumstances does not come within the scope of the obligation to make a report.This does not preclude a report being made should the operator choose to do so. Employees may also be obliged to make a report by other parts of POCA. Further information can be found in Part 7 (opens in a new tab) of POCA.

In the case of Da Silva [2006] EWCA Crim 1654, the Court of Appeal stated the following in relation to suspicion:

"It seems to us that the essential element in the word ‘suspect’ and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice."

There is thus no requirement for the suspicion to be clear or firmly based on specific facts, but there must be a degree of satisfaction, not necessarily amounting to belief, but at least extending beyond mere speculation, that an event has occurred or not.

Whether a person holds suspicion or not is a subjective test. If a person thinks a transaction is suspicious, they are not required to know the exact nature of the criminal offence or that particular funds are definitely those arising from the crime. The person may have noticed something unusual or unexpected and, after making enquiries, the facts do not seem normal or make commercial sense. It is not necessary to have evidence that money laundering is taking place to have suspicion. Whether a person has a suspicion is a matter for their own judgement. If they have not yet formed a suspicion but simply have cause for concern, they may choose to ask the customer or others more questions. This choice will depend on what is known about the customer and how easy it is to make enquiries.

A transaction that appears to be unusual is not necessarily suspicious. Many customers will, for perfectly legitimate reasons, have an erratic pattern of gambling transactions or account activity. Even customers with a steady and predictable gambling profile will have periodic transactions that are unusual for them. So an unusual transaction may only be the basis for further enquiry, which may in turn require judgement as to

whether the transaction or activity is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report the activity then arises. Likewise, if concern escalates following further enquiries, it is reasonable to conclude that the transaction is suspicious and will need to be reported to the NCA.

Unusual patterns of gambling, including the spending of unusually large amounts of money in relation to the premises or customer's profile, should receive attention, but unusual behaviour should not necessarily lead to grounds for knowledge or suspicion of money laundering, or the making of a report to the NCA. The nominated officer or the manager assigned AML duties should assess all of the circumstances and, in some cases, it may be helpful to ask the customer or others more questions. The choice depends on what is already known about the customer and the transaction, and how easy it is to make enquiries.

In order for a SAR to be made, it is not necessary to know or to establish the exact nature of any underlying criminal offence, or that the particular funds or property were definitely those arising from a crime. Furthermore, it is not necessary to await conviction of a customer for money laundering or other criminal offences in order to have suspicion that money laundering has taken place.

What constitutes suspicious activity?

There are numerous things that can make someone either know or suspect that they are dealing with the proceeds of crime. Some examples of how suspicions may be raised are listed below, although this is not an exhaustive list and there may be other circumstances which raise suspicion.

Examples

A man convicted of dealing in drugs is released from prison and immediately starts gambling large amounts of money. He is known to be out of work and other customers inform employees that he is supplying drugs again. This will give rise to the suspicion that he is spending the proceeds of his criminal activity.

Stakes wagered by a customer become unusually high or out of the ordinary and the customer is believed to be spending beyond his or her known means. This requires some knowledge of the customer but, nevertheless, there may be circumstances that appear very unusual and raise the suspicion that they are using money obtained unlawfully. It may be that the customer lives in low cost accommodation with no known source of income but nonetheless is spending money well above their apparent means. There is no set amount which dictates when a SAR should be made and much will depend on what is known, or suspected, about the customer.

A customer exhibits unusual gambling patterns with an almost guaranteed return or very little financial risk, including betting where the customer places bets on all possible outcomes of an event (sometimes across multiple operators). It is accepted that some customers prefer to gamble in this way but, in some instances, the actions may raise suspicion because they are different from the customer’s normal gambling practices.

Money is deposited by a customer or held over a period and withdrawn by the customer without being used for gambling. For instance, suspicions should be raised by any large amounts deposited in gaming machines or gambling accounts that are then cashed or withdrawn after very little game play or gambling.

A customer regularly gambles large amounts of money and appears to find a level of losses acceptable. In this instance, the customer may be spending the proceeds of crime and sees the losses as an acceptable consequence of the process of laundering those proceeds.

A customer's spend increases over a period of time, thereby masking high spend and potential money laundering.

A customer spends little, but often, and their annual aggregate spend is high and out of kilter with his expected spend. This could indicate potential money laundering.

It is important to note that, once knowledge or suspicion of criminal spend is linked to a customer in one area of the business (for example, over the counter bets), it is good practice to monitor the customer's activity in other areas of the business (for example, gaming machine play).

Suspicious activity reports (SARs)

The operator or operator's nominated officer (where one has been appointed) must report to the NCA any transaction or activity that, after evaluation, it is known or suspected it may be linked to money laundering. A disclosure to the NCA is made by submitting a SAR to the UKFIU. Such reports must be made as soon as is practicable after the information comes to the operator, nominated officer or responsible manager.

The NCA accepts the submission of SARs in three main ways:

SAR online

A secure web-based reporting system for small or medium sized reporting entities with access to the internet, which allows SARs to be submitted electronically through NCA SAR Online System (opens in a new tab).

It is the NCA's preferred method of reporting. Reporters must register themselves as a source (reporting entity) on the system once, and then submit SARs by completing linked electronic screens that reflect the fields included in the paper based reports.

Requests for a defence (consent) can be submitted using SAR Online, and as long as the box for consent is checked at the start of the process, the system alerts the Consent Team automatically, ensuring swift identification and management of requests for a defence (appropriate consent). It is not necessary to send the request by fax as well as submission online.

SAR online is the NCA's preferred method for small and medium sized reporters to submit SARs. The benefit to the reporter is 24/7 reporting, an automatic acknowledgment of receipt with the ELMER reference number, an initial feedback report on the quality of the SARs submitted after six months, and investigators are able to access the information more rapidly.

Paper-based reporting

Use the standard NCA Suspicious Activity Report Form. The NCA prefers submissions to be typed to enable them to be scanned and prevent errors in data entry. The form and guidance on using the form is available from the NCA website. Completed forms should be posted to:

UKFIU
PO Box 8000
London
SE11 5EN

If using the form to request a defence (appropriate consent), it should be faxed immediately to 0207 238 8286, but it is not necessary to post and fax a consent request.

The paper based reporting system will not elicit an acknowledgment of receipt or an ELMER reference number for your records, and the SAR will take some time to reach investigators.

Encrypted bulk data exchange

Used by high volume reporters, namely reporters with more than 10,000 reports a month. If an operator believes this would be the most appropriate method of reporting for their group, they should contact the UKFIU on 0207 238 8282 to discuss the matter.

Operators should include in each SAR as much relevant information about the customer, transaction or activity that it has in its records. The NCA has published a glossary of terms (opens in a new tab) which they prefer operators to use when completing SARs. This will assist in consideration of the report by the NCA.

Operators should ensure that they check all the facts they have about the customer and include all relevant information when submitting a SAR, which may include the following:

- Do the staff at the local outlet know the customer’s identity?
- Is a physical description of the customer available?
- Has the customer provided any records that will assist in identifying him, for example credit or debit card details?
- Has the customer ever self-excluded?

- What are the customer's product preferences and does he hold other gambling accounts (for example, prefers over the counter betting, but also uses telephone and online gambling facilities)?

In order that an informed overview of the situation may be maintained, all contact between the operator and law enforcement agencies should be controlled through, or reported back to, the nominated officer or a deputy acting in the absence of the nominated officer, or the responsible manager. The NCA may apply to the magistrates' court (or, in Scotland, the sheriff) for an order (a further information order), following the submission of a SAR, requiring the nominated officer (or reporter) to provide more information in respect of the SAR (Section 339ZH (opens in a new tab) of POCA). Law enforcement agencies may also apply for a disclosure order requiring any person considered to have information relevant to an investigation to answer questions, provide information or to produce documents (Sections 357 (opens in a new tab), 358 (opens in a new tab), 391 (opens in a new tab) and 392 (opens in a new tab)of POCA).

Requesting a defence

If operators handle any proceeds of crime they may commit one of the principal money laundering offences in POCA. However, if the operator submits a SAR to the NCA, this can provide a defence. There is a statutory mechanism which allows the NCA either to grant or refuse the 'prohibited act' going ahead, or to prevent the suspected money laundering going ahead (Section 335 (opens in a new tab) of POCA). This statutory mechanism is called 'appropriate consent' and is referred to by the NCA as Requesting a defence from the NCA under POCA and TACT.

The decision whether or not to obtain a defence (appropriate consent) will arise in the following scenarios:

- concealing, disguising, converting, transferring or removing criminal property (Section 327 (opens in a new tab) of POCA)
- facilitating the acquisition, retention, use or control of criminal property by, or on behalf of, another person (Section 328 (opens in a new tab) of POCA)
- acquisition, use or possession of criminal property (Section 329 (opens in a new tab) of POCA).

These are referred to as 'prohibited acts'.

In any of these scenarios, operators will have two choices. They may choose not to go ahead with the activity in question, or they may choose to proceed. A decision to proceed will mean that the operator may be committing a money laundering offence. However, if they have made an authorised disclosure and have obtained a defence (appropriate consent), they will not be committing an offence.

Operators will need to consider how they will approach their reporting obligations and consider:

- the timing of the report(s) – particularly second or subsequent reports
- whether the operator wishes to continue to do business with the customer while awaiting a defence (appropriate consent).

A nominated officer (where one has been appointed by the operator), police constable, NCA employee or customs officer can give a person (which may include, for example, employees of the operator) actual 'appropriate consent' to a suspect transaction proceeding (Section 335(1) (opens in a new tab) of POCA). However, it should be noted that the NCA is the only body able to issue formal notification of a defence (consent) by means of an official NCA letter, which can then be retained by the operator for their records.

Alternatively, a person will be treated as having the appropriate consent if notice is given to a police constable or customs officer (but, note, not the nominated officer) and either:

- consent is not refused within seven working days (beginning with the day after the notice is given)
- if consent is refused and following such refusal, the 'moratorium period' (31 calendar days starting with the day on which the person receives notice that consent to the doing of the act is refused) has expired (Section 335(2) (opens in a new tab) of POCA).

Although notice can be given to a constable or customs officer, there is a need to ensure that the practices of all law enforcement agencies are consistent in this area. Therefore, the NCA operates as the national centre for all SARs and for the issue of decisions concerning the granting or refusal of a defence (appropriate consent). To avoid confusion requests for a defence (consent) should be routed through the NCA. See Applying for a defence for more detail.

Operators should be aware that the NCA and other authorities, such as the Financial Conduct Authority and Serious Fraud Office, can apply to the Crown Court (or, in Scotland, the sheriff) for an order to extend the moratorium period for a further 31 days. An order can be given on up to six occasions, which allows the moratorium period to be extended for a maximum period of 186 days in total.

To grant an order for an extension, in each case the Court must be satisfied that the NCA or other authority's investigation is being carried out "diligently and expeditiously", additional time is needed to complete the investigation and the extension would be reasonable in the circumstances (Section 336A (opens in a new tab) of POCA).

However, POCA provides that a nominated officer must not give the appropriate consent unless he has himself already made a disclosure to an authorised officer of the NCA and, either:

- the NCA employee has provided a defence (consented to the transaction)
- a defence (consent) is not refused within seven working days (beginning with the day after the notice is given)
- if a defence (consent) is refused and following such refusal, the 'moratorium period' (31 calendar days starting with the day on which the person receives notice that consent to the doing of the act is refused) has expired (but see Requesting a defence) (Section 336 (opens in a new tab) of POCA).

Reporting suspicious activity before or reporting after the event are not equal options which an operator can choose between, and retrospective reporting is unlikely to be seen in the same light as reporting prior to the event. A report made after money laundering has already taken place will only be a legal defence if there was a 'reasonable excuse' for failing to make the report before the money laundering took place (Section 327(2)(b) (opens in a new tab) of POCA). Where a customer request is received prior to a transaction or activity taking place, or arrangements being put in place (for example, where a customer requests the opening of a gambling account), and there is knowledge or suspicion that the transaction, arrangements, or the funds/property involved, may relate to money laundering, a SAR must be submitted to the NCA and a defence (consent) sought to proceed with that transaction or activity. In such circumstances, it is an offence for a nominated officer to agree to a transaction or activity going ahead within the seven working day notice period calculated from the working day following the date of disclosure, unless the NCA provides a defence (gives consent) (Section 336(3) (opens in a new tab) and (4) (opens in a new tab) of POCA).

The defence (consent provisions can only apply where there is prior notice to the NCA of the transaction or activity. The NCA cannot provide a defence (consent) after the transaction or activity has occurred. A

defence (consent) request which is received after the transaction or activity has taken place will therefore be dealt with as an ordinary SAR.

In the gambling industry, business is often conducted out of normal office hours. In addition, gambling transactions may sometimes be more 'immediate' than, for example, depositing funds into a bank account where the funds may be withdrawn at a later date. In these circumstances it may sometimes not be feasible or practical to obtain a defence (appropriate consent) prior to or during a transaction. Knowledge or suspicion of money laundering may be triggered after a customer has completed all the stages of a gambling transaction. Under those circumstances, it may be reasonable to report after the transaction. However, the defence of 'reasonable excuse' when reporting after the transaction is untested by case law and should be considered on a case-by-case basis (Section 327(2)(b) (opens in a new tab) of POCA). Where the relationship with the customer is expected to have an element of duration and involve numerous transactions, it is advisable to seek a defence (consent) prior to transacting with the customer.

If knowledge or suspicion of money laundering is present, particularly if this occurs out of normal office hours, there must be a mechanism for involvement of the senior manager on duty and contact with the nominated officer (where one has been appointed) as soon as is practicable. In circumstances where this is not possible, it is advisable to report the matter to the NCA directly, where feasible.

Operators or nominated officers will need to think very carefully about whether or not to continue to do business with a customer suspected of money laundering. Relevant considerations should be the potential for criminal offences under POCA, as well as potential damage to business reputation and other commercial factors.

Operators should also note that the reporting defence is not intended to be used repeatedly in relation to the same customer. In the case of repeated SAR submissions on the same customer, it is the Commission’s view that this is not a route by which operators can guarantee a reporting defence retrospectively. If patterns of gambling lead to an increasing level of suspicion of money laundering, or to actual knowledge of money laundering, operators must seriously consider whether they wish to allow the customer to continue using their gambling facilities. Operators are, of course, free to terminate their business relationships if they wish, and provided this is handled appropriately there should be no risk of prejudicing an investigation. However, operators should think about liaising with the law enforcement investigating officer to consider whether it is likely that termination of the business relationship would alert the customer or prejudice an investigation in any other way.

How customers suspected of money laundering will be dealt with is an important area of risk management for all operators. They should deal with the issue in their policies, procedures and controls. As all gambling operators are at risk of committing the principal offences, it is advisable to consider these issues carefully before they arise in practice.

For example, the operator may consider one transaction to be suspicious and reports it to the NCA as such, but the operator may be less concerned that all of an individual’s future transactions are suspicious. In these circumstances, each transaction should be considered on a case-by-case basis and reports made accordingly, and a defence (appropriate consent) sought where necessary. Where subsequent reports are also made after actual or suspected money laundering has taken place or appears to have taken place, operators are encouraged to keep records about why reporting was delayed, and about why a defence (appropriate consent) was not requested before the suspected money laundering took place.

Applying for a defence

Where SAR Online is used and a defence (appropriate consent) is needed, this can be done by ticking the 'consent requested' box. Alternatively, requests can be faxed to the NCA UKFIU Consent Desk (see the NCA (opens in a new tab) for more information). You are advised to make it explicit in your report that you are seeking a defence (consent) from the NCA.

Requests must be for a specified activity (or specified series of activities) and should not be open-ended, such as seeking a defence (consent) to 'handle all business dealings or transactions' relating to the subject of the request or the relevant account.

The SAR requesting a defence (appropriate consent) should set out concisely:

- who is involved
- what and where the criminal property is and its value
- when and how the circumstances arose and are planned to happen
- why you have knowledge or are suspicious.

The UKFIU Consent Desk applies the criteria set out in the **Home Office Circular 029/2008 Proceeds of Crime Act 2002: Obligations to report money laundering – the consent regime** to each request for a defence (consent), carry out the necessary internal enquiries, and will contact the appropriate law enforcement agency, where necessary, for a consent recommendation. Once the NCA's decision has been reached, the disclosing operator will be informed of the decision by telephone, and be given a consent number, which should be recorded. A formal letter from the NCA will follow.

Home Office Circular 029/2008 contains guidance on the operation of the consent regime in POCA. It was issued to ensure consistency of practice on the part of law enforcement in considering requests for consent under Part 7 (opens in a new tab) of POCA. This was in response to concerns from the financial services industry and other sectors and professions that decisions should be taken in an effective and proportionate way, with due engagement with all participants. The circular was formulated in agreement with key partner agencies and sets out the high-level principles by which the law enforcement agencies should make decisions on consent, and how these principles should be applied.

Although POCA provides that consent can be granted by a constable (which includes authorised NCA officers) or a customs officer, there is a need to ensure that the practices of all law enforcement agencies are consistent in this area. Therefore, as a result of the circular, the NCA operates as the national centre for all authorised disclosures and also for the issue of decisions concerning the granting or refusal of a defence (consent). To avoid confusion those making requests for a defence (consent) should route requests through the NCA. The decision making process will consist of a collaborative effort between the

NCA and the other law enforcement agencies, with the latter providing a recommendation to the NCA. While the final decision will be taken by the NCA, in most cases it is likely to be based largely on the recommendation provided by the interested law enforcement agency.

All requests for a defence (consent) are dealt with by the NCA on a case-by-case basis. It may take the maximum of seven working days to deal with a defence (consent) request, however, in most cases the NCA is able to respond to requests for a defence (consent) within three days (NCA Annual Report). Operators should take this into account when deciding whether it is practical and reasonable to request a defence (consent) prior to the transaction or activity rather than making a report after the transaction or activity.

In the event that the NCA does not refuse a request for a defence (consent) within seven working days (the notice period) following the working day after the report is made, the operator may continue to transact with the customer. However, if the request for a defence (consent) is refused within that period, the NCA can prevent the transaction or activity for a further 31 calendar days (the moratorium period) from the day the request for a defence (consent) is refused.

Once a matter has been appropriately reported to the NCA, the decision to proceed or not to proceed with a transaction or arrangement remains with the operator. Even if a defence (consent) is obtained from the NCA, the operator is not obliged to proceed with the transaction or arrangement.

Operators should note that a defence (consent) only applies in relation to individual prohibited acts, and cannot provide cover to deal with a particular customer. Any subsequent activity will require separate consideration and, if necessary, separate requests for a defence from the NCA. Where a single money laundering offence consists of a course of conduct, the NCA may give consent for a series of similar transactions over a specified period. In cases where there is a range of different money laundering offences that may be committed, such as acquiring (section 329(1)(a) of POCA) and transferring (section 327(1)(d) (opens in a new tab) of POCA) criminal property, the NCA may give a single consent to that person being concerned in an arrangement to facilitate acquisition and use under section 328(1) (opens in a new tab) of POCA.

The NCA's ability to grant a defence (consent) in such circumstances will depend on having sufficient detail about the future course of activity or repeated transactions in order to make an informed decision. This is considered on a case-by-case basis. It is not possible for the NCA to give 'blanket' consent for a reporter to carry out all activity and transactions on a suspicious account, individual or arrangement.

The NCA cannot give advice to operators in relation to the specific circumstances where SARs should be submitted or the terms for requesting a defence (appropriate consent). Comprehensive guidance on requesting a defence is available on the NCA's website. Attention is drawn, in particular, to the following NCA publication: Requesting a defence from the NCA under POCA and TACT (opens in a new tab).

Suspicious activity reporting requirements for remote operators

For the purposes of this section, 'British customer' is inferred to mean a customer who is physically located in Great Britain when they use gambling facilities provided in reliance on a remote operating licence issued by the Commission, regardless of their usual residential address.

'Non-British customer' on the other hand means a customer who is not physically located in Great Britain when they use gambling facilities provided in reliance on a remote operating licence issued by the Commission, regardless of their usual residential address.

The Commission is aware that some remote operators not physically located in Great Britain may be required by local law to report instances of known or suspected money laundering activity by British customers to the FIU of the jurisdiction in which the operator is situated, rather than the NCA.

The Commission is of the view that remote operators should report suspicious activity to the authorities in the area where the remote gambling equipment used in the specific suspicious transaction is located. However, in relation to transactions concerning British customers, it is the Commission's view that such reports should also be received by the authorities in this jurisdiction.

Suspicious activity reporting

Where any of the remote gambling equipment used in a transaction which is known or suspected to involve money laundering is located in Great Britain (as well as equipment located in Northern Ireland), the known or suspected money laundering activity must be reported to the NCA. Operators must provide the Commission with the unique reference numbers allocated by the UKFIU of the NCA, for reports submitted by them, as soon as reasonably practicable and in any event within five working days of receipt thereof, in accordance with licence condition 15.2.1.

Where the remote gambling equipment used in a transaction which is known or suspected to involve money laundering is located outside Great Britain, but involves a British customer, and the jurisdiction in which the equipment is located is not a member of the Egmont Group (or the jurisdiction does not include gambling businesses under AML or CTF legislation, or prohibits online gambling), the known or suspected money laundering activity must be reported to the NCA. Operators must provide the Commission with the unique reference numbers allocated by the UKFIU of the NCA, for reports submitted by them, as soon as reasonably practicable and in any event within five working days of receipt thereof, in accordance with licence condition 15.2.1.

In all other cases, the known or suspected money laundering activity must be reported to the FIU of the jurisdiction in which the remote gambling equipment used in a transaction, which is known or suspected to involve money laundering, is located. The relevant report will then be shared with the NCA through the Egmont Group, where appropriate (note that in the case of operators where the remote gambling equipment used in a transaction which is known or suspected to involve money laundering is located in Gibraltar and involves a British customer, known or suspected money laundering activity must be reported to the Gibraltar FIU and the UKFIU). Where circumstances permit, operators should provide the Commission with the unique reference numbers allocated by the applicable FIU, for reports concerning British customers, within five days of receipt thereof.

These reporting requirements are summarised in the table below:

Reporting requirements

Customer	Location of remote gambling equipment	Member of Egmont Group?	Report suspicious activity to	Unique reference numbers (URNs)
British or Non-British customer*	Britain** or Northern Ireland	Yes	NCA	Operators should provide the Commission with the URNs allocated by the NCA within five working days
British customer*	Outside Britain**	No	NCA	Operators should provide the Commission with the URNs allocated by the NCA within five working days
		Yes, but domestic FIU does not receive gambling SARs		
		Country prohibits online gambling		
British or Non-British customer*	Outside Britain**	Yes	Domestic FIU***	Where circumstances permit, operators should provide the Commission with the URNs allocated by the FIU, for reports concerning British customers, within five working days

- See paragraphs 20.61 and 20.62
- ◦ Britain means England, Scotland and Wales
- ** In the case of operators where the remote gambling equipment used in a transaction which is known or suspected to involve money laundering is located in Gibraltar and involves a British customer, known or suspected money laundering activity must be reported to the Gibraltar FIU and the UKFIU.

Applying for a defence

Where remote operators wish to make use of the defences provided by sections 327(2)(a) (opens in a new tab), 328(2)(a) (opens in a new tab) and 329(2)(a) (opens in a new tab) of POCA where they believe that, by proceeding with a transaction with a British customer, they will be committing a prohibited act, they should apply for a defence (appropriate consent), in accordance with section 335 (opens in a new tab) of POCA, from the NCA.

Failing to report (nominated officer)

POCA creates an offence of failing to report suspicious activity (failure to disclose). Where a person nominated by the operator to receive disclosures (the nominated officer) fails to comply with the obligation to make a report to the NCA as soon as practicable after the information is received, they are open to criminal prosecution (Section 332 (opens in a new tab) of POCA).

! **Warning The criminal sanction under POCA for conviction on indictment is a prison term of up to five years and/or a fine (Section 334 (opens in a new tab) of POCA).**

For all failure to disclose offences it will be necessary to prove that the nominated officer either:

- knows the identity of the money launderer or the whereabouts of the laundered property
- believes the information on which the suspicion was based may assist in identifying the money launderer or the whereabouts of the laundered property.

Operators and nominated officers, therefore, are strongly advised to comply with the reporting requirements imposed on them by POCA.

After a report has been made

When an enquiry is under investigation, the investigating officer may contact the operator to ensure that he has all the relevant information which supports the original SAR. This contact may also include seeking supplementary information or documentation from the reporting operator and from other sources by way of a court order.

The investigating officer will therefore work closely with the operator, who will usually receive direct feedback on the stage reached in the investigation. There may, however, be cases when the operator cannot be informed of the state of the investigation, either because of the confidential nature of the enquiry, or because the case is currently under consideration by a court.

Prejudicing an investigation

Under section 342 (opens in a new tab) of POCA, a person commits an offence if they:

- know or suspect 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
- make a disclosure which is likely to prejudice the investigation, or
- falsify, conceal, destroy or otherwise dispose of, or cause or permit the falsification, concealment, destruction or disposal of, documents which are relevant to the investigation (Section 342(1) (opens in a new tab) and (2) (opens in a new tab) of POCA).

It is, however, a defence if the person does not know or suspect that disclosure of the information is likely to prejudice the investigation, if the disclosure is made in compliance with other provisions of POCA or similar laws, or if the person does not know or suspect that the documents are relevant to the investigation or the person does not intend to conceal any facts disclosed by the documents (Section 342(3) (opens in a new tab) and (6) (opens in a new tab) POCA). The offence can be committed before or after a disclosure has been made.

Those working in the gambling sector should be aware of the provisions in relation to this offence. 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 should not result in the offence of prejudicing an investigation, unless you know or suspect that an investigation is current or impending and make the enquiries in a way that discloses those facts.

It is important to note that the offence of prejudicing an investigation is not the same as the ‘tipping off’ offence. The tipping off provisions are directed at the individual employed in the regulated sector (non-

remote and remote casinos) who knows or suspects that a disclosure has been made, whereas the offence of prejudicing an investigation relates to any individual regarding the disclosure of the knowledge of the existence of an investigation which could prejudice the investigation.

Interaction with customers

Normal customer enquiries will not, in the Commission's view, amount to prejudicing an investigation under POCA, unless it is known or suspected that a SAR has already been submitted and that an investigation is current or impending and make the enquiries of the customer in a way that it discloses those facts. Indeed, such customer enquiries are likely to be necessary not only in relation to money laundering but also in connection with social responsibility duties (for example, problem gambling). In regard to this offence, counter or frontline staff may not be aware that the nominated officer has submitted a SAR to the NCA. Reasonable and tactful enquiries regarding the background to a transaction or activity that is inconsistent with the customer's normal pattern of activity is good practice, forms an integral part of KYC measures (and may be driven by social responsibility concerns) and should not give rise to the prejudicing of an investigation.

If patterns of gambling lead to an increasing level of suspicion of money laundering, or even to actual knowledge of money laundering, operators should seriously consider whether they wish to allow the customer to continue using their gambling facilities. If an operator wishes to terminate a customer relationship, and provided this is handled sensitively, there will be low risk of prejudicing an investigation. However, if the decision has been made to terminate the relationship and there is a remaining suspicion of money laundering with funds to repatriate, consideration should be given to asking for a defence (appropriate consent).

In circumstances where a law enforcement agency requests an operator to continue trading with a customer as they conduct further investigations, the operator is advised to record the factors considered when agreeing or declining to do so (for example, the risks of participating in such activity, assurances provided by law enforcement, possible money laundering offences, relevant timescales provided, the gravity of the offences being investigated and the purpose of the request), and how this may change the management of risks to the licensing objectives. Given the operator's heightened exposure to risk, it is advisable for the operator to ask for confirmation in writing of such requests from law enforcement. The operator should also continue to submit SARs and/or seek a defence (consent) from the NCA if they decide to continue with a business relationship with such customers.

Training

All operators should consider awareness training for all relevant employees so that they have an understanding of what obligations are placed upon them and what action they must take to ensure that details are forwarded to and considered immediately by the nominated officer, manager or other employee responsible for making reports to the NCA. In the case of solo operators or operators without specific AML employees, advice is available on the NCA website (opens in a new tab).

One of the most important controls over the detection and prevention of money laundering is for an operator to have employees who are alert to the risks of money laundering and who are well trained in the identification of unusual activities or transactions which appear to be suspicious. The effective application of even the best designed control systems can be quickly compromised if the employees applying those

systems are not adequately trained. The effectiveness of the training will therefore be important to the overall success of the operator's AML strategy.

Under POCA, individual employees face potential criminal penalties if they are involved in money laundering activity, unless they make a report of known or suspected money laundering activity. It is important, therefore, that employees are made aware of their legal obligations and how to correctly discharge them.

Operators should devise and implement a clear and well-articulated policy and procedure for ensuring that relevant employees are aware of their legal obligations in respect of POCA. They should also provide employees with regular training in the identification and reporting of customer activity that gives grounds for suspecting money laundering.

Operators should also take reasonable steps to ensure that relevant employees are aware of:

- their responsibilities under the operator's policies and procedures for the detection and prevention of money laundering
- the money laundering risks faced by an operator
- the operator's procedures for managing those risks
- the identity and responsibilities of the nominated officer (where one has been appointed) or the person responsible for making reports to the NCA the potential effect of a breach of POCA on the operator and its employees.

The content of any employee training, the frequency of training and the assessment of competence following training are matters for each operator to assess and decide in the light of the money laundering risks they identify. The Commission advises that such issues are covered in each operator's policies and procedures.

Where a nominated officer has been appointed, they should be actively involved in devising and managing the delivery of the training, taking particular care to ensure that systems are in place to cover all part-time or casual employees.

The NCA publishes a range of material, such as threat assessments and risk profiles, of which operators may wish to make their employees aware. The information on the NCA website could usefully be incorporated into operators' training materials.

It is also recommended that operators consult the Commission's AML hub, which has useful information and links to other AML resources.

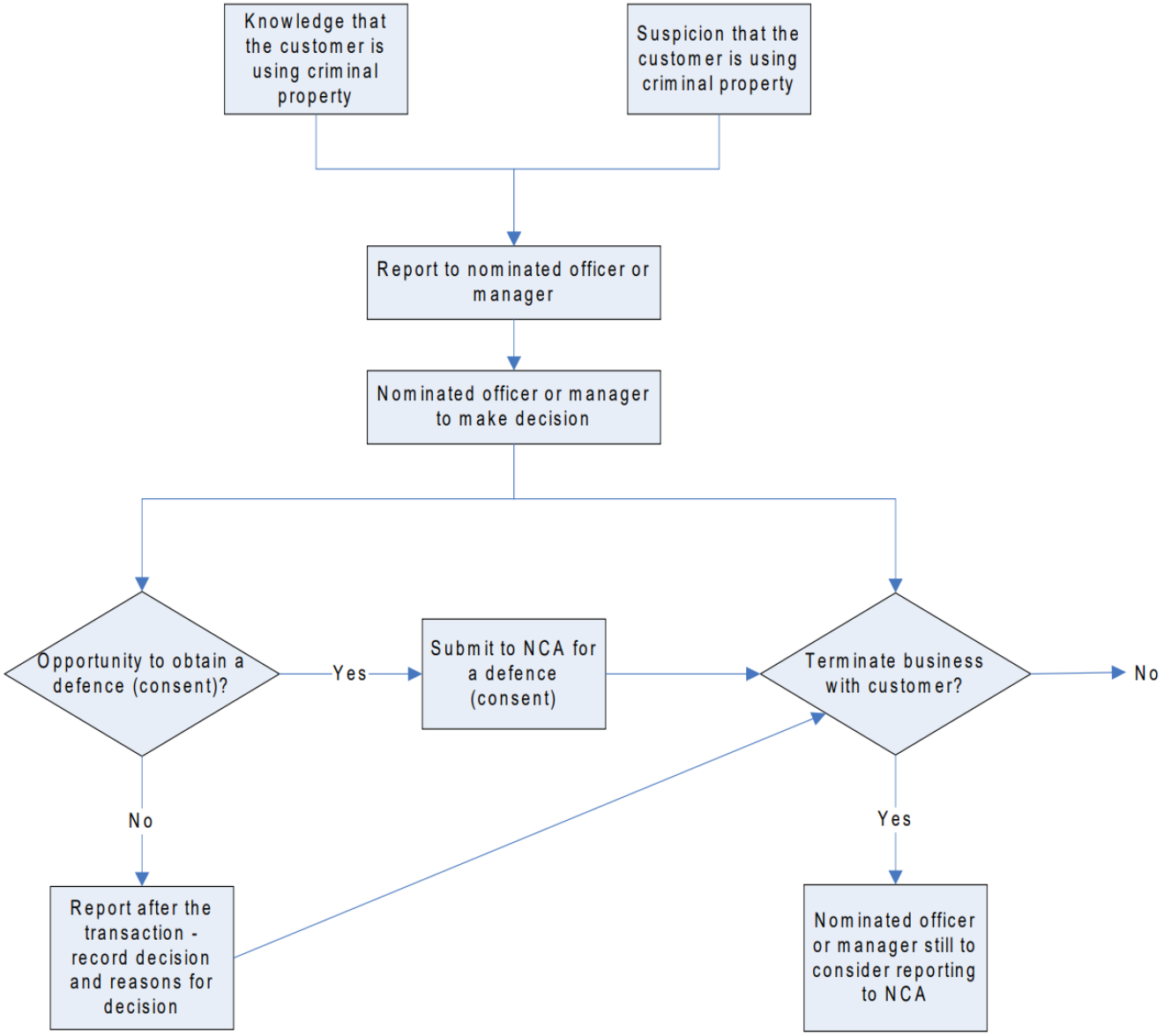
Terrorist financing

The Terrorism Act establishes several offences about engaging in or facilitating terrorism, as well as raising or possessing funds for terrorist purposes. It establishes a list of proscribed organisations that are believed to be involved in terrorism. The Terrorism Act also contains defences to the principal terrorist property offences, in a similar way to POCA.

The Terrorism Act applies to all persons, and includes obligations to report suspected terrorist financing. Operators should, therefore, report instances of suspected terrorist financing to the NCA using the same methods as those for the reporting of known or suspected money laundering activity.

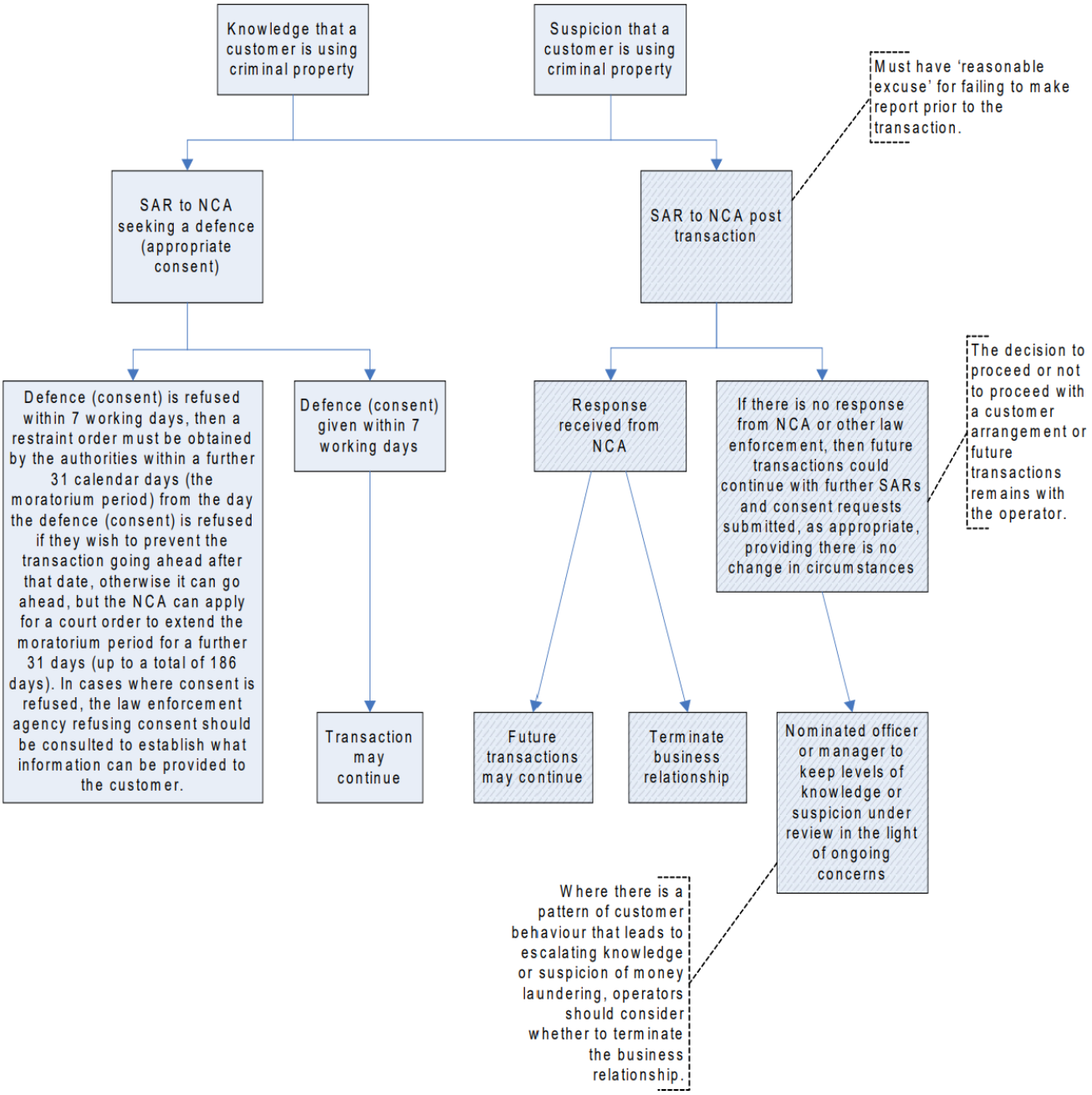
Flowcharts

Knowledge or suspicion of money laundering (subjective test)



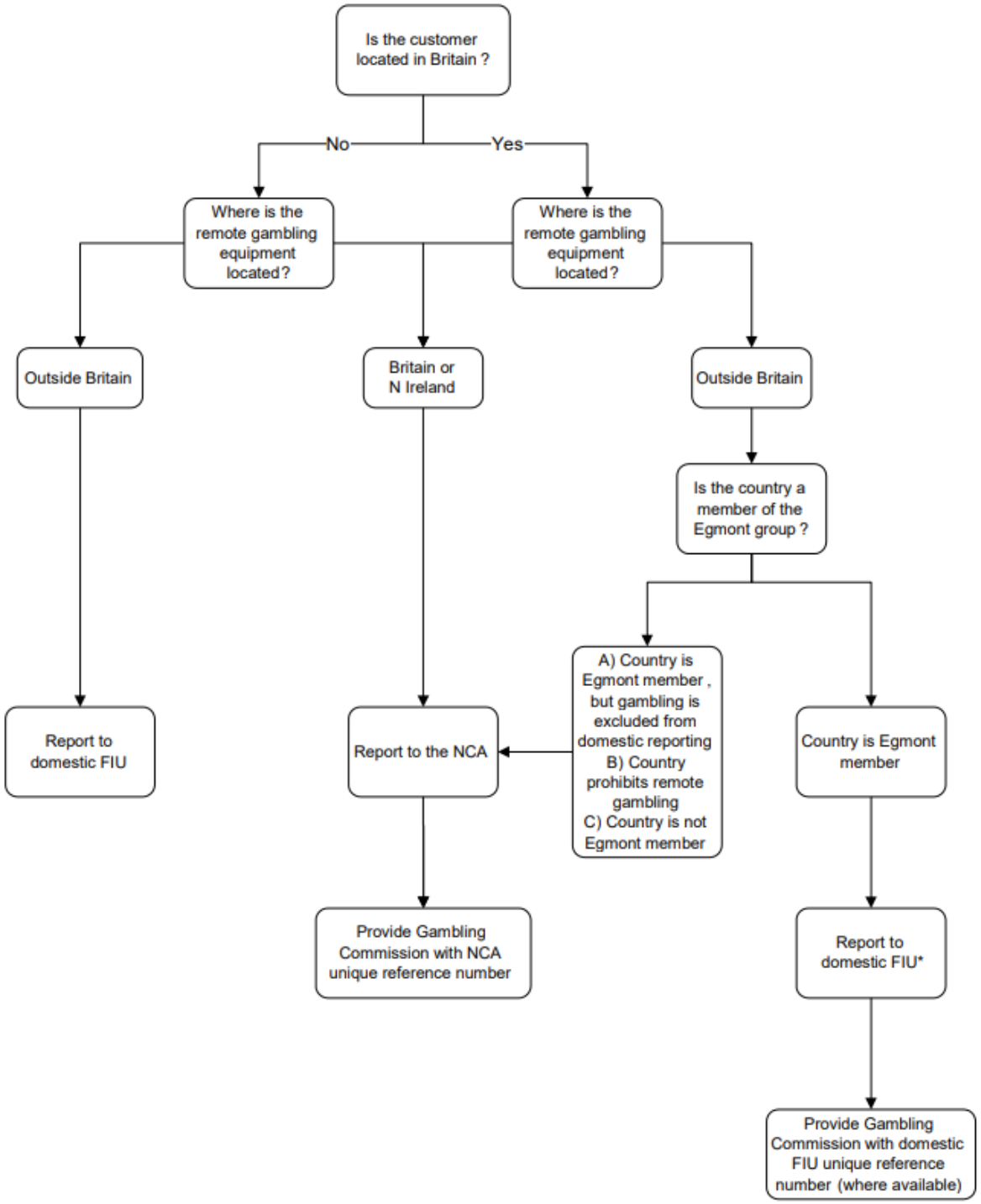
Flowchart of Knowledge or suspicion of money laundering (subjective test)

Requesting a defence



Flowchart of requesting a defence

Suspicious activity reporting requirements for remote operators



Flow chart of Suspicious activity reporting requirements for remote operators.

*In the case of operators where the remote gambling equipment used in a transaction which is known or suspected to involve money laundering is located in Gibraltar and involves a British customer, known or suspected money laundering activity must be reported to the Gibraltar FIU and the UKFIU.

Glossary of terms

AML
: Anti-money laundering

Beneficial ownership
: Beneficial ownership is enjoyed by anyone who has the benefits of ownership of property, but does not apparently own the asset itself

Business relationship
: A business, professional or commercial relationship between an operator and a customer, which is expected to have an element of duration

Business-to-business
: A term used to describe commerce transactions between businesses, or the exchange of products, services or information between businesses. In other words, it is business which is conducted between firms, rather than between firms and consumers (or customers)

Criminal spend
: In the context of gambling, the use of the proceeds of crime to fund gambling as a leisure activity (otherwise known as lifestyle spend)

Money laundering
: The process by which criminal or 'dirty' money is legitimised or made 'clean', including any action taken to conceal, arrange, use or possess the proceeds of any criminal conduct. Defined in section 340 of POCA

Operators
: Firms holding an operating licence issued by the Commission

POCA
: The Proceeds of Crime Act 2002, which is intended to reduce money laundering and the profitability of organised crime through the use of tools such as asset recovery

Proceeds of crime
: Property from which a person benefits directly or indirectly, by being party to criminal activity, for example stolen money, money from drug dealing or property stolen in a burglary or robbery

SAR
: A suspicious activity report – the means by which suspicious activity relating to possible money laundering or the financing of terrorism is reported to the NCA under POCA or the Terrorism Act

Source of funds

Where the funds, money or cash to finance the transaction come from

The Act

The Gambling Act 200

The Commission

The Gambling Commission

The NCA

The National Crime Agency, which became operational in October 2013, is a crime-fighting agency with national and international reach that works in partnership with other law enforcement organisations to cut serious and organised crime. The NCA is the organisation to which suspicious activity is reported

The Terrorism Act

The Terrorism Act 2000