



Anti-Money Laundering Regulations
&
Risk Assessment

Guidance Document

CONTENTS

Executive Summary		4
Part 1 - Introduction and summary of the advice		6
1. Purpose		6
2. Who is this intended for?		6
3. The role of gambling operators		6
4. The role of the Commission		7
5. The Proceeds of Crime Act 2002		8
6. Risk-based approach		8
7. Customer relationships		9
8. Duties under the Proceeds of Crime Act 2002		9
Nominated Officers		9
Suspicious activity reporting		9
9. Failing to report (nominated officer)		11
10. After a report has been made		11
11. Prejudicing an investigation		12
12. Training		12
Part 2 - The advice		13
13. What is meant by the proceeds of crime and money laundering?		13
14. The Proceeds of Crime Act 2002		14
15. Offences under the Proceeds of Crime Act 2002		14
Risk-based approach		16
Introduction		16
Identifying and assessing the risks faced by the operator		18

16.	Customer relationships	20
	Establishment of business relationship	21
	Customer monitoring	22
	Termination of business relationship	22
17.	Duties under the Proceeds of Crime Act 2002	23
	Authorised disclosures	23
	Appointment of nominated officer	24
	Role of nominated officer	25
	Suspicious activities and reporting	26
	What is meant by knowledge and suspicion?	26
	What constitutes suspicious activity	27
	Suspicious activity reports (SARs)	29
	Appropriate Consent	32
	Applying for appropriate consent	34
18.	Failing to report (nominated officer)	38
19.	After a report has been made	38
20.	Prejudicing an investigation	38
	Customer interaction	39
21.	Training	40
	Figures	
	Figure 1 – Knowledge or suspicion of money laundering (subjective test)	31
	Figure 2 – Appropriate consent	37
	Appendix A	
	Glossary of terms	42
	Appendix B	
	Template of an example risk assessment model	44
	Useful Links	46

EXECUTIVE SUMMARY

Article 7 of the European Union 4th Anti-Money Laundering Directive (4th AML Directive) was adopted by the European Commission on 5th June 2015 and is currently moving through a two-year transposition process. The Directive brings all providers of gambling services into the regulated sector and subject to the Money Laundering Regulations with consideration to the following caveat:

The 4th AML Directive creates the potential for EU member states to exempt (in full or in part) certain providers of gambling services where they are able to demonstrate proven low risk following an appropriate risk assessment, taking into account the nature and, where appropriate, the scale of the operations of the services.

Member states must consider the following factors in their risk assessments:

- how vulnerable their transactions and payment methods are to money laundering, and
- whether they are affected by findings issued in supranational assessments issued by the European Commission.

The Gambling Act 2005 places a responsibility on all gambling operators to keep financial crime out of gambling. This is derived from the licensing objective to prevent gambling from being a source of crime and disorder.

The Proceeds of Crime Act 2002 (POCA) places a further obligation on gambling operators to be alert to attempts by customers to gamble money acquired unlawfully. This applies to all forms of money laundering including 'cleaning' dirty money, attempting to disguise the criminal source of the funds, or simply using criminal proceeds to fund gambling.

It is largely accepted that the Adult Gaming Centre (AGC) and Licensed Family Entertainment Centre (LicFEC) sectors of the betting and gaming industry pose low risk to money laundering activities, but it is important nevertheless that all companies are aware of POCA and the need to assess what level of risk their companies are exposed to in respect of potential money laundering activities., especially with regard to TITO products and change machines.

The policy and procedure document relating to suspicious monetary transactions in the bacta toolkit condenses the requirements and remains appropriate as a guide to ensure that junior members of staff who interact with customers are compliant.

Once the potential level of risk to your company has been established it is very unlikely that all of your customers and services will pose the same level of risk. As such it is unlikely that you will need to know all your customers equally. It is recommended that you adopt three levels of due diligence:

- Low diligence to reflect very low risk
- Standard diligence to reflect low risk
- Enhanced diligence to reflect medium to high risk.

Under POCA, all gambling operators have a responsibility to report instances where they know or suspect that a customer is using the proceeds of crime to gamble, or is using their gambling facilities to launder money.

All operators are required to assess and manage the risks of their business being used for money laundering and terrorist funding. However, the assessment should be proportionate and appropriate to:

- the size of the company
- the business model, and
- the style of delivery to consumers

Where an assessment reveals low risk, plans and procedures to mitigate these will be proportionate.

The approach you take to due diligence should reflect the level of risk that your company is exposed to. Whether that be in relation to your customers, the services or products that you provide or the geographical location where your company is located. By identifying these risks, they can then be mitigated by implementing adequate policies and procedures that are proportionate to these risks. Having these adequate policies and procedures in place, provides a certain level of protection in investigations regarding money laundering.

The initial step to determining your risk based approach is to identify potential risks. The following table provides key areas that should be reviewed and considered

Area	Consideration
Customer	Type of customer (demographic) Relationship with your customers. Location of your customer base
Product/Service	Gambling machine categories and other products you provide. Risk these machines and products pose for money laundering
Delivery method	Location of your business (local risk assessment) Method(s) of payment delivery

An example risk assessment model is produced at Appendix 'B'.

Part 1 - Introduction and summary of the advice

1 Purpose

- 1.1 All gambling operators have a responsibility to keep financial crime out of gambling. The Proceeds of Crime Act 2002 (POCA) places a legal 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.
- 1.2 This advice document, the contents of which emanate from advice published by the Gambling Commission and other regulatory or authoritative sources, explains how operators can make sure they and their employees comply with their legal obligations under POCA. It sets out a number of matters operators need to be aware of and explains their duties and responsibilities under POCA.
- 1.3 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.

2 Who is this intended for?

- 2.1 This advice is directed at holders of AGC and LicFEC operating licences issued by the Gambling Commission (the Commission), and are members of bacta.
- 2.2 The advice is detailed and aimed primarily at operators with a number of employees, either full time or part time. However, it remains the responsibility of all operators to understand and comply with the requirements of POCA.

3 The role of gambling operators

- 3.1 Operators have a responsibility to uphold the three licensing objectives set out in the Gambling Act 2005 (the Act). The first of those licensing objectives is to prevent gambling being a source of crime or disorder, being associated with crime and disorder, or being used to support crime.
- 3.2 As described in paragraph 1.1, 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).
- 3.3 Operators should report instances of money laundering or attempts by customers to launder money to the National Crime Agency (the NCA) and, where appropriate consent is requested, wait for such consent to deal with a transaction or an arrangement involving the customer, or wait until a set period has elapsed before proceeding.
- 3.4 Operators should be aware that there is no *de minimis* threshold for the management and reporting of money laundering activity.

4 The role of the Commission

- 4.1 The Commission licenses operators and requires them to uphold the three licensing objectives set out in the Act. The first of those licensing objectives is 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 National Crime Agency (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 will assist operators to meet their obligations under POCA, where appropriate.
- 4.2 The Commission adopts a risk-based approach to its role and therefore focuses attention on circumstances where the processing of criminal funds or criminal spend indicates serious failures of 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. **Where criminal spend is concerned, the Commission recognises the challenges faced by the gambling industry in identifying lower level activity.**
- 4.3 Where operators fail to uphold the licensing objectives, for example by being ineffective in applying anti-money laundering (AML) controls or ignoring their responsibilities under POCA, the Commission will consider reviewing the suitability of the operator to carry on the licensed activities, under section 116 of the Act. This could result in the suspension or revocation of the operator's licence under sections 118 and 119 of the Act.
- 4.4 The Commission has the powers of accredited financial investigators under POCA. This means, amongst other things, that (in England and Wales) the Commission can apply for orders and warrants in relation to money laundering, for the purpose of:
- requiring a specified person to produce certain material
 - permitting the search of and seizure of material from specified premises

- requiring a financial institution to provide customer information relating to a specified person.

5 The Proceeds of Crime Act 2002

- 5.1 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.
- 5.2 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.
- 5.3 A person benefits from criminal conduct if he obtains property as a result of or in connection with the conduct. If a person benefits from criminal conduct, his or her benefit is the property obtained as a result of, or in connection with, the conduct. Property is gained by a person if he obtains an interest in it.
- 5.4 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. 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.
- 5.5 POCA and the offences under POCA are discussed in sections 14 and 15 of this advice document.

6 Risk-based approach

- 6.1 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 cooperation of all employees.
- 6.2 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 and procedures to manage and mitigate the risks
 - monitoring and improving the effective operation of these controls recording what has been done, and why.

- 6.3 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.
- 6.4 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.
- 6.5 The risk-based approach is discussed in section 16 of this advice document.

7 Customer relationships

- 7.1 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).
- 7.2 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.
- 7.3 Customer relationships consist of the following three aspects:
- the establishment of the business relationship with the customer
 - the monitoring of customer activity
 - the termination of the business relationship with the customer.
- 7.4 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 appropriate consent where appropriate, as well as considering any risk to the licensing objectives.
- 7.5 Customer relationships are discussed in section 17 of this advice document.

8 Duties under the Proceeds of Crime Act 2002

- 8.1 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 appropriate consent to do a prohibited act, where appropriate.
- 8.2 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, appropriate consent is obtained from the NCA. Therefore, in all instances where customers' funds are known or suspected of having criminal origins, a report must be made to the NCA at the earliest opportunity.

Nominated officer

- 8.3 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, **it is recommended that operators in the AGC and LicFEC sectors should also consider appointing a nominated officer, as this will help them meet their obligations under POCA more effectively.**
- 8.4 Where a nominated officer is appointed, he or she 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.
- 8.5 The nominated officer will:
- receive internal disclosures under Part 7 of POCA
 - decide whether these disclosures should be reported to the NCA
 - if appropriate, make such external reports to the NCA
 - ensure that appropriate consent is applied for, as necessary. The nominated officer should record all decisions made in this regard.

Suspicious activity reporting

- 8.6 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, or
 - where they suspect that a person is engaged in money laundering, including criminal spend.

- 8.7 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.
- 8.8 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.**
- 8.9 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.
- 8.10 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.
- 8.11 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'.
- 8.12 Appropriate consent is granted by the NCA 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 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 reference number, which should be recorded, along with the operator's record of decisions made.
- 8.13 Operators duties under POCA, the status and role of the nominated officer, suspicious activity and reporting, and appropriate consent are discussed in section 18 of this advice document.

9 Failing to report (nominated officer)

- 9.1 POCA creates an offence of failing to report suspicious activity. 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. The criminal sanction under POCA is a prison term of up to five years and/or a fine.

9.2 The offence of failing to report is discussed in section 19 of this advice document.

10 After a report has been made

10.1 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 disclosure.

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

10.3 This is discussed in more detail in section 20 of this advice document.

11 Prejudicing an investigation

11.1 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).

11.2 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.

11.3 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.

11.4 The prejudicing an investigation offence is discussed in section 21 of this advice document.

12 Training

- 12.1 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.
- 12.2 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.
- 12.3 Training is discussed in section 22 of this advice document.

Part 2 - The advice

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

- 13.1 Broadly, the term 'proceeds of crime' or 'criminal proceeds' refers to 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 (this is commonly referred to as criminal property). It also includes property that a person gains by spending the proceeds of criminal activity, 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.
- 13.2 Classic money laundering consists of a number of stages:
- placement
 - layering
 - integration.
- 13.3 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.
- 13.4 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.

- 13.5 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.
- 13.6 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.
- 13.7 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).

14 The Proceeds of Crime Act 2002

- 14.1 In section 340 of POCA, 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.
- 14.2 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.
- 14.3 A person benefits from conduct if he obtains property as a result of or in connection with the conduct. If a person benefits from criminal conduct, his or her 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.

- 14.4 If a person gains a pecuniary 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 pecuniary advantage.
- 14.5 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.

15 Offences under the Proceeds of Crime Act 2002

- 15.1 The criminal offences of money laundering were first introduced in the United Kingdom in the Criminal Justice Act 1988 and the Drug Trafficking Offences Act 1986. POCA consolidated, updated and reformed the criminal law relating to money laundering to cover all criminal offences, including any dealing in criminal property.
- 15.2 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 to POCA, 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.
- 15.3 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. 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. In respect of the gambling industry, this generally could involve the taking of cash, cheque or card payments in the form of a bet or wager, or holding money on account for a customer for the purposes of gambling.
- 15.4 Section 327 of POCA provides that a person commits an offence if he:
- conceals criminal property (for example, by depositing funds obtained through criminal activity into a gambling account)
 - disguises criminal property (for example, by placing funds obtained through criminal activity into a gambling account and then withdrawing them at a later date)
 - converts criminal property (for example, by placing bets in a gambling establishment and then cashing in the winnings)
 - transfers criminal property (for example, by transferring property to another person or to a gambling operator)
 - removes criminal property from the United Kingdom (for example, by taking his 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.

- 15.5 Section 328 of POCA provides that a person commits an offence if he enters into or becomes concerned in an arrangement which he knows or suspects 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.
- 15.6 Section 329(1) of POCA provides that a person commits an offence if he:
- acquires criminal property
 - uses criminal property
 - has possession of criminal property (for example, via stakes).
- Acquisition, use and possession under section 329(1) 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 he acquired or used or had possession of the property for adequate consideration.
- 15.7 The principal money laundering offences are wide and can be committed by anyone, including employees of an operator, who have actual knowledge or suspicion that a customer is laundering money.
- 15.8 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 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.
- 15.9 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.
- 15.10 While POCA places responsibilities on operators, the legislation also gives them protection if they report suspicious activity. You will have a defence to the principal money laundering offences in sections 327, 328 or 329 of POCA if you:
- make an authorised disclosure under section 338 of POCA prior to the offence being committed and you obtain appropriate consent under section 335 of POCA (known as the consent defence)
 - intended to make an authorised disclosure but had a reasonable excuse for not doing so (known as the reasonable excuse defence).

Authorised disclosures and appropriate consent are discussed in Part 18 of this advice document.

- 15.11 The penalty for conviction of an offence under sections 327, 328 or 329 of POCA is imprisonment for a term of a maximum of 14 years, a fine not exceeding the statutory maximum, or both. In addition, POCA contains provisions for the recovery of the proceeds of crime, regardless of whether a conviction for any offence has been obtained or is intended to be obtained. Criminal property can be recoverable even if it is disposed of to another person.

16 Risk-based approach

Introduction

- 16.1 A risk-based approach involves a number of discrete steps to assess the most proportionate way to manage and mitigate the risks faced by the operator. These steps should include:
- identifying the money laundering risks that are relevant to the operator
 - designing and implementing policies and procedures to manage and mitigate the assessed risks
 - monitoring and improving the effective operation of these controls
 - recording what has been done, and why.
- 16.2 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, civil action against the operator and damage to the reputation of the operator, leading to a loss of business.
- 16.3 Operators need to continually identify, assess and manage 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 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.**
- 16.4 Most operators manage their commercial or business risks and measure the effectiveness of the policies and procedures 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.

- 16.5 Even though operators outside the regulated sector (clarified in paragraph 15.2) are not obliged to have systems and procedures in place under money laundering legislation, the Commission would nonetheless expect 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. Systems and procedures can assist operators in complying with these obligations, particularly in relation to reporting suspicious activity.
- 16.6 In order to detect customer activity that may be suspicious, it is necessary to continually 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. This should not be confused with customers who are either of high or low commercial value to the operator.
- 16.7 Where a customer is assessed as presenting a higher risk it would be expected that additional information in respect of that customer is collected. This will help the operator to 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.
- 16.8 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 would 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.
- 16.9 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 common sense in applying their risk-based criteria and rules.
- 16.10 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.
- 16.11 **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.

- 16.12 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 and procedures 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 over the management of the risk.

Identifying and assessing the risks faced by the operator

- 16.13 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:
- What risk is posed by the business profile and the profile of customers using the gambling facilities?
 - What risk is posed to the operator by transactions with business associates and suppliers, including their beneficial ownership and source of funds?
 - 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, bank account, cash, etc.)?
 - 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 (which could indicate that a group of people are using the same device or location to gamble for the purposes of committing fraud)?

- 16.14 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).
- 16.15 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 his 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 his employer and resold it for his own gain. He 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.
 - An individual 'feeding' dyed banknotes stolen in the course of an armed robbery into change machines within a wide range of gambling establishments.
 - Instances of money being put into Ticket In Ticket Out (TITO) machines with little actual gambling.
- 16.16 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.

- 16.17 Money laundering risk assessment is not a one-off exercise. Operators should ensure that their policies and procedures 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.

17 Customer relationships

- 17.1 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 only to be indicative of problem gambling, but could also be considered as a proxy for other risks (for example, spend that is inconsistent with the individual's apparent legitimate income being associated with 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.
- 17.2 Operators are subject to both certain provisions of POCA and the Act (and the relevant licence conditions and codes of practice). Given, therefore, 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. 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.
- 17.3 It is also important that the operator is able to resolve information relating to gambling activity in different parts of the business back to the same customer so that they have a more complete picture of the risks to which the operator is exposed.
- 17.4 Clearly customer relationships need to be managed proficiently and records maintained to provide information as to what was communicated to the customer, why and what considerations were made. The management of player expectations is one way in which the industry can obtain the assurances they require in a familiar and

efficient way and promote their commitment to safeguarding the interests of their customers. 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 players to question or become suspicious of the motives of these interactions.

17.5 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 and procedures 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 relation to the reporting of money laundering activity by customers, and obtaining appropriate consent where necessary.

17.6 Customer relationships 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.

17.7 At all stages of the relationship it is necessary to consider whether the customer is engaging in money laundering, including criminal spend, report suspicious activity and seek appropriate consent, where necessary, as well as considering any risk to the licensing objectives.

Establishment of business relationship

17.8 The establishment of a business relationship with a customer will occur when the customer either:

- 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
- places money on account with the operator.

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

- the potential 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.

17.10 Where it is known that the customer is attempting to use the operator to launder criminal proceeds or for criminal spend, the operator should either not establish the business relationship, or terminate the business relationship at the earliest opportunity. In both circumstances, it is recommended that a SAR is submitted to the NCA and, where there are funds to be returned to the customer, seek appropriate consent.

Customer monitoring

- 17.11 Where, through their customer profile or known pattern of gambling activity, it is determined that the customer poses 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 whether 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.
- 17.12 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.
- 17.13 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).
- 17.14 If the customer's patterns of gambling lead to a steadily 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 gaming facilities, otherwise they may potentially commit one of the principal money laundering offences.

Termination of business relationship

- 17.15 As already discussed, 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, otherwise they may potentially commit one of the principal money laundering offences.
- 17.16 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 appropriate consent before paying out winnings or returning funds to the customer

18 Duties under the Proceeds of Crime Act 2002

18.1 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 appropriate consent to do a prohibited act, where appropriate.

Authorised disclosures

- 18.2 If a person carries out any action contemplated under the principal offences discussed in paragraphs 15.3 to 15.6, 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, appropriate consent is obtained from the NCA. These authorised disclosures or reports are referred to as SARs.
- 18.3 The NCA became operational in October 2013. The functions of the UKFIU are placed within the NCA. In addition, the NCA undertakes civil recovery and tax investigations in England, Wales and Northern Ireland. The NCA is a crime-fighting agency with national and international reach that works in partnership with other law enforcement organisations to reduce serious and organised crime.
- 18.4 The SAR regime for money laundering is run by the UKFIU. It receives and analyses SARs concerning instances of known or suspected money laundering or terrorist financing in order to counter money laundering and terrorist financing, and makes those SARs available to law enforcement and taxation agencies so they can take appropriate action.
- 18.5 In all instances where customers' funds are known or suspected of having criminal origins, a disclosure must be made to the NCA at the earliest opportunity using the methods set out on the NCA website: www.nationalcrimeagency.gov.uk.
- 18.6 Operators should have a system clearly setting out the requirements for making a disclosure. This system could include:
- the circumstances in which a disclosure 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
 - how and when a disclosure is to be made to the NCA
 - how employees can manage a customer when a disclosure has been made and consent is awaited
 - the need to be alert to circumstances which could lead to charges of prejudicing an investigation.

Appointment of nominated officer

- 18.7 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, it is recommended that operators in the non-regulated sector should 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 paragraphs 18.39 and 18.41 below). **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 offences under POCA, as the decision whether to report or not to report to the NCA and request appropriate consent is the sole responsibility of the nominated officer.**
- 18.8 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.
- 18.9 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 of POCA.
- 18.10 Where the operator appoints a nominated officer, it may be appropriate for that individual to hold a Personal Management Licence issued by the Commission.
- 18.11 Where operators do not formally appoint a nominated officer, it is still advisable for a 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.
- 18.12 The Commission recognises that some operators (particularly smaller 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

- 18.13 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 appropriate consent.
- 18.14 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 disclosed 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.
- 18.15 Where an operator has appointed a nominated officer, he will:
- receive internal disclosures under Part 7 of POCA
 - decide whether these disclosures should be reported to the NCA
 - if appropriate, make such external reports to the NCA
 - ensure that appropriate consent is applied for as necessary. The nominated officer should record all decisions made in this regard.
- 18.16 The nominated officer should be able to monitor the day-to-day operation of the operator's AML policies in general, including policies to deal with money laundering by customers, and respond promptly to any reasonable request for information made by the Commission or law enforcement bodies. The nominated officer is expected to take ultimate managerial responsibility for AML issues, but this does not diminish senior management responsibility for AML.
- 18.17 Where AML tasks are delegated by an operator's nominated officer to another employee, the nominated officer remains responsible for AML issues and he 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 any 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

- 18.18 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

- or where they suspect, that a person is engaged in money laundering, including criminal spend, if they want to avoid committing one or more of the principal offences.
- 18.19 Operators will only need to consider making a report if they have actual knowledge or subjective suspicion.
- 18.20 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 manager, should consider each report, and determine whether it warrants the submission of a SAR
 - operators should ensure that employees are appropriately trained in their obligations, and the requirements for making reports to their nominated officer or manager.
- 18.21 If the nominated officer or 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 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?

- 18.22 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 jury to infer knowledge. 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, or be obliged to do so by other parts of POCA. Further information can be found in Part 7 of POCA.
- 18.23 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.
- 18.24 Whether you hold suspicion or not is a subjective test. If you think a transaction is suspicious, you are not required to know the exact nature of the criminal offence or that the funds were definitely those arising from the crime. You may notice something unusual or unexpected and, after making enquiries, the facts do not seem normal or do not make

commercial or financial sense. You do not have to have evidence that the customer is using the proceeds of crime to have suspicion. Whether you have a suspicion is a matter for your own judgement. If you have not yet formed a suspicion but simply have cause for concern, you may choose to ask the customer or others more questions. This choice will depend on what you already know about the customer and how easy it is to make enquiries.

- 18.25 A transaction that appears to be unusual is not necessarily suspicious. Many customers will, for perfectly good 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 make a report to the NCA.
- 18.26 Unusual patterns of gambling by customers, including gambling involving unusually large amounts of money, should receive attention, but unusual patterns of behaviour should not necessarily lead to knowledge or suspicion of money laundering, or the submission of a report to the NCA. Nominated officers or managers assigned AML duties should assess all of the circumstances. In cases where it is feasible, it may be helpful to ask customers discretely for more information, such as why they have a large amount to spend.
- 18.27 In order for a SAR to be made, again 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.

What constitutes suspicious activity?

- 18.28 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 well 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 he is 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 his or her 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 his annual aggregate spend is high and out of kilter with his expected spend. This could indicate potential money laundering.
- A customer displays gambling patterns where spend is high but the risk is low, for example gambling on red and black in roulette, betting on events with only two possible outcomes (for example, tennis matches). The customer could be laundering money in a way that guarantees minimal loss.
- Instances of high spend by customers that lead to commercial risk for the operator may also indicate suspicious activity.

18.29 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)

18.30 The operator or operator's nominated officer (where one has been appointed) must report to the NCA any transaction or activity that, after his evaluation, he knows or suspects 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 reasonably practicable after the information comes to the operator or nominated officer.

18.31 The NCA accepts the submission of SARs in the following ways:

- SAR Online, which is a secure web-based reporting system for small or medium sized reporting entities with access to the internet, allowing SARs to be submitted electronically through <https://www.ukciu.gov.uk/saronline.aspx>. 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.

Consent requests 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 appropriate consent. It is not necessary to send a consent fax as well as a 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, using 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 at: www.nationalcrimeagency.gov.uk/aboutus/what-wedo/specialist-capabilities/ukfiu/how-to-report-sars.

Completed forms should be posted to UKFIU, PO Box 8000, London, SE11 5EN. If using the form to request appropriate consent, it should be faxed immediately to 0207 238 8286, but it is not necessary to post and fax a consent request.

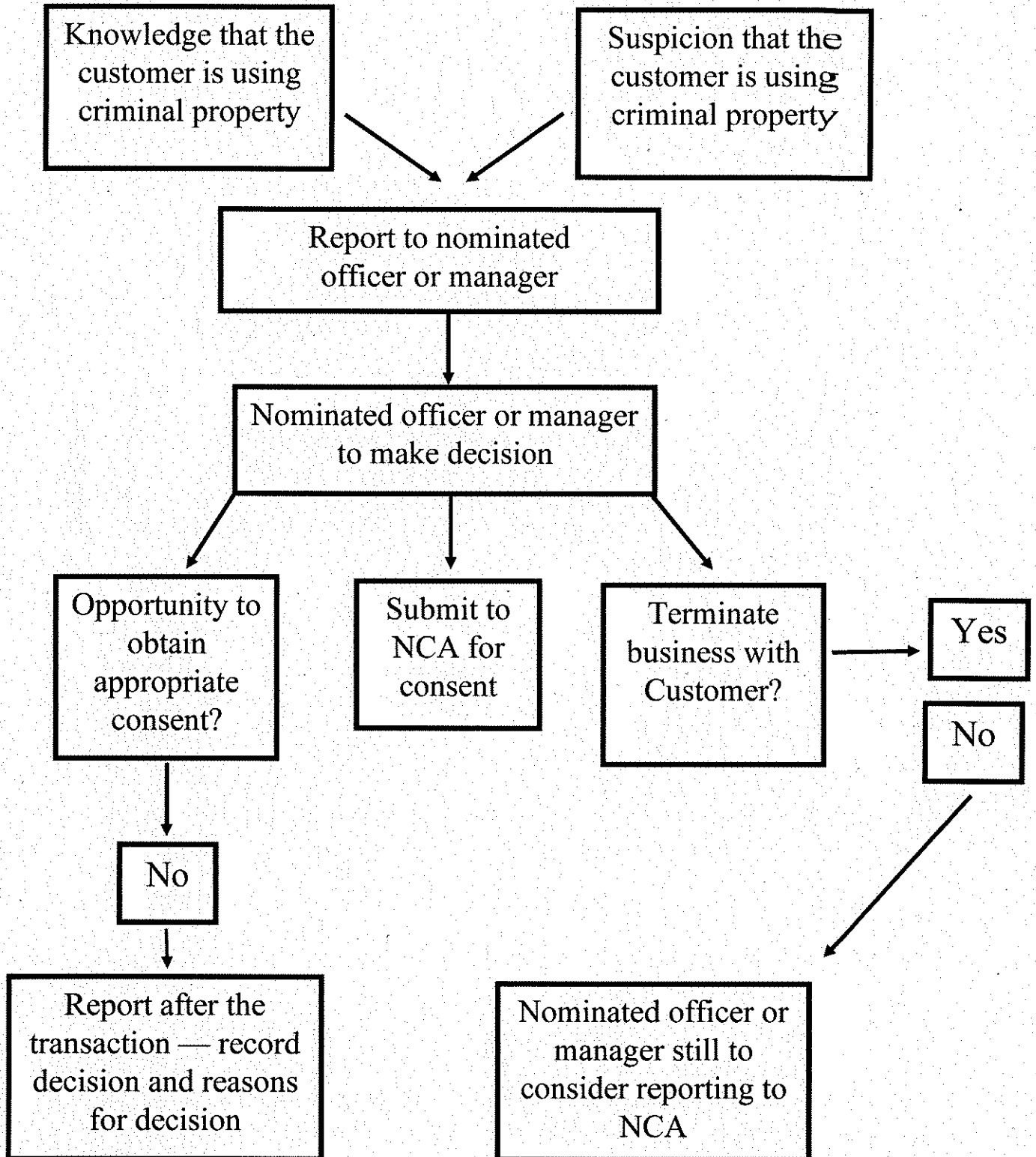
The paper based reporting system will not elicit an acknowledgment of receipt or an ELMER reference number for your records, and the SAR will take some time to reach investigators.

- 18.32 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 which they prefer operators to use when completing SARs (www.nationalcrimeagency.gov.uk/about-us/what-we-do/specialistcapabilities/ukfiu/howto-report-sars). This will assist in consideration of the report by the NCA.

- 18.33 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)?

18.34 In order that an informed overview of the situation may be maintained, all contact between operators 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.

Figure 1: Knowledge or suspicion of money laundering (subjective test)



Appropriate consent

- 18.35 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 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. This statutory mechanism is called 'appropriate consent'.
- 18.36 The decision whether or not to obtain appropriate consent will arise in the following scenarios:
- concealing, disguising, converting, transferring or removing criminal property
 - facilitating the acquisition, retention, use or control of criminal property by, or on behalf of, another person
 - acquisition, use or possession of criminal property These are referred to as "prohibited acts".
- 18.37 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 appropriate consent, they will not be committing an offence.
- 18.38 Operators will, therefore, need to consider how they will approach their reporting obligations and consider:
- the timing of the report(s) – particularly second or subsequent reports; and
 - whether the operator wishes to continue to do business with the customer while awaiting appropriate consent.
- 18.39 A nominated officer (where one has been appointed by the operator), police constable, employee of the NCA or customs officer can give a person (which may include employees of the operator) actual 'appropriate consent' to a suspect transaction proceeding. However, it should be noted that the NCA is the only body able to issue formal notification of consent by means of an official NCA letter, which can then be retained by the operator for their records.
- 18.40 Alternatively, such 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); or
 - 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.

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 appropriate consent. To avoid confusion requests for consent should be routed through the NCA. See paragraph 18.53 for more detail.

- 18.41 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 consented to the transaction; or
 - consent is not refused within seven working days (beginning with the day after the notice is given); or
 - 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.
- 18.42 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.²⁵ Where a customer instruction 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 consent sought to proceed with that transaction or activity. In such circumstances, it is an offence for a nominated officer to consent 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 gives consent.
- 18.43 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 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, it should be noted that the defence of 'reasonable excuse' when reporting after the transaction is currently untested by case law and should be considered on a case-by-case basis. Where the relationship with the customer is expected to have an element of duration and involve numerous transactions, it is advisable to seek consent prior to transacting with the customer.
- 18.44 Where there is knowledge or suspicion of money laundering, 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.
- 18.45 Operators or nominated officers will need to think very carefully about the risks if they decide 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.

- 18.46 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 a steadily increasing level of suspicion of money laundering or to actual knowledge of money laundering, operators will need to 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.
- 18.47 How customers suspected of money laundering will be dealt with is an important area of risk management for all operators. Operators should deal with the issue in their policies and procedures and, as all gambling operators are at risk of committing the principal offences, it is advisable for operators to consider these issues carefully before they arise in practice.
- 18.48 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 appropriate consent sought, where necessary. Where subsequent reports are also made after prohibited acts appear to have taken place, operators are encouraged to keep records about why reporting was delayed, and about why appropriate consent was not requested before the suspected money laundering took place.

Applying for appropriate consent

- 18.49 Where SAR Online is used and appropriate consent is needed, this can be done by checking the box requesting consent. Alternatively, requests can be faxed to the NCA UKFIU Consent Desk (see the NCA website www.nationalcrimeagency.gov.uk). You are advised to make it explicit in your report that you are seeking consent from the NCA.
- 18.50 The SAR requesting appropriate consent should set out:
- the information or other matter which provides the grounds for your knowledge, suspicion or belief
 - a description of the property that you know, suspect or believe is criminal property
 - a description of the prohibited act for which you are seeking consent to carry out.
- 18.51 The UKFIU Consent Desk will apply 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 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

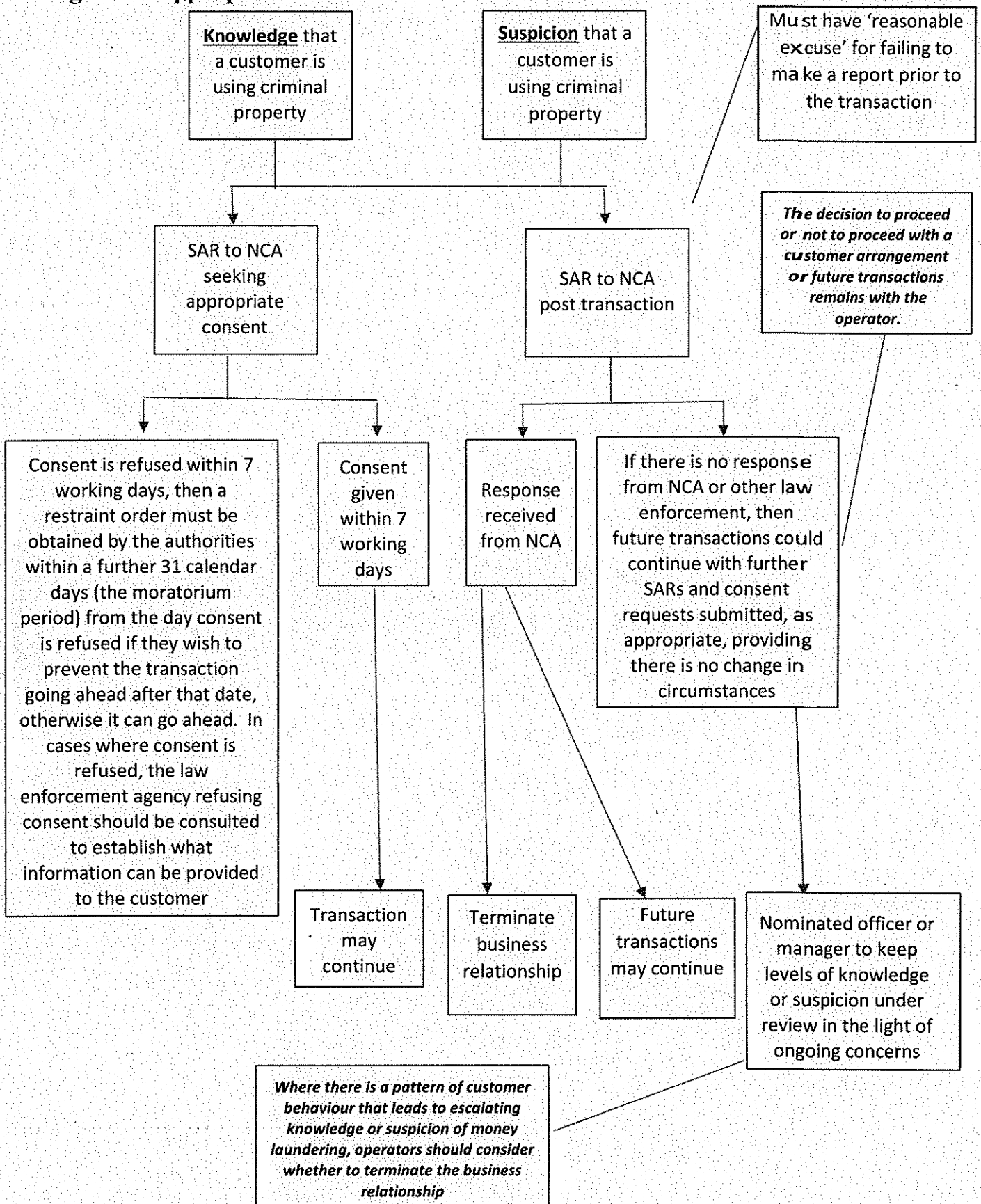
should be recorded, along with the operator's record of decisions made. A formal consent letter from the NCA will follow.

- 18.52 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 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.
- 18.53 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 consent. To avoid confusion those making requests for 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.
- 18.54 All requests for 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 consent request, however, in most cases the NCA is able to respond to requests for consent within three days. Operators should take this into account when deciding whether it is practical and reasonable to request consent prior to the transaction rather than making a report after the transaction or activity.
- 18.55 In the event that the NCA does not refuse 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 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 consent is refused.
- 18.56 Once a matter has been appropriately reported to the NCA, the decision to proceed or not with a transaction or arrangement remains with the operator. Even if consent is obtained from the NCA, the operator is not obliged to proceed with the transaction or arrangement.
- 18.57 Operators should note that consent only applies in relation to individual prohibited acts. Any subsequent activity will require separate consideration and, if necessary, separate consent 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) 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) of POCA.

- 18.58 The NCA's ability to grant 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.
- 18.59 The NCA cannot give advice to operators in relation to the specific circumstances where SARs should be submitted or the terms for requesting appropriate consent. Comprehensive guidance on consent requests is available on the NCA's website. Attention is drawn, in particular, to the following NCA publications: Obtaining consent from the NCA under Part 7 of the Proceeds of Crime Act (POCA) 2002 or under Part III of the Terrorism Act (TACT) 2000 and Seeking Consent for Repeated Transactions.

Figure 2: Appropriate consent



19. Failing to report (nominated officer)

19.1 POCA creates an offence of failing to report suspicious activity. 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. The criminal sanction under POCA is a prison term of up to five years and/or a fine.

19.2 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
- or believes the information on which the suspicion was based may assist in identifying the money launderer or the whereabouts of the laundered property.

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

20 After a report has been made

20.1 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 operator and from other sources by way of a court order.

20.2 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 the courts.

21 Prejudicing an investigation

21.1.1 Under section 342 of POCA, a person commits an offence if he:

- knows or suspects that an appropriate officer or, in Scotland, a proper person is acting or proposing to act) in connection with a confiscation investigation, a civil recovery investigation, a detained cash investigation or a money laundering investigation which is being or is about to be conducted, and
- he makes a disclosure which is likely to prejudice the investigation, or
- falsifies, conceals, destroys or otherwise disposes of, or causes or permits the falsification, concealment, destruction or disposal of, documents which are relevant to the investigation.

21.1.2 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 enactments, 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. The offence can be committed before or after a disclosure has been made.

21.2 Those working in the gambling sector should be aware of the provisions in relation to this offence. Reasonable enquiries of a customer, including social responsibility enquiries, 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, critically, make the enquiries in a way that it discloses those facts.

21.3 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.

Customer interaction

21.4 Normal customer enquiries will not, in our opinion, amount to prejudicing an investigation under POCA, unless you know or suspect 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/customer due diligence measures (and may be driven by social responsibility concerns) and should not give rise to the prejudicing of an investigation.

21.5 If patterns of gambling lead to a steadily 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 gaming 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 appropriate consent.

21.6 In circumstances where law enforcement agencies request operators 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, etc.), 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 consent if they decide to persist with a business relationship with such customers.

22 Training

- 22.1 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 always available on the NCA website.
- 22.2 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 and who are well trained in the identification of unusual activities or transactions which may prove 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.
- 22.3 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.
- 22.4 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.
- 22.5 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.
- 22.6 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.

- 22.7 Where a nominated officer has been appointed, he 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.
- 22.8 The NCA publishes a range of material at www.nationalcrimeagency.gov.uk, 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. In addition, the Association of British Bookmakers (www.abb.uk.com) has published useful guidelines on POCA and these can be obtained from them directly.
- 22.9 It is also recommended that operators consult the Commission's AML webpage, which has useful information and links to other AML resources. This can be found at: www.gamblingcommission.gov.uk/money_laundering

Appendix A - 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.
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.
Source of funds	Where the funds or wealth to finance the transaction come from.
The Commission	The Gambling Commission.

The NCA

The National Crime Agency, which became operational in October 2013. It 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.

UKFIU

The United Kingdom Financial Intelligence Unit, which is the unit within the NCA that operates the disclosure and consent regime for money laundering.

Appendix B - Example of a risk assessment model

Customer Base

It is accepted that the customer base in both AGCs and LicFECs is wide ranging, to a degree unpredictable and variable in demographic terms as to where a venue is located.

However, it is helpful to assess using operating experience, trends and averages.

‘A’ – Very Low Risk

‘B’ - Low Risk

‘C’ – Medium Risk

Business Profile		A	B	C
Factor	Risk Management/Mitigation			
What risk is posed by the business profile of customers using the gambling facilities?	Customers are efficiently monitored throughout the time they are on the premises to satisfy age restriction requirements, prevention of machine related crime, effective customer interaction, and the detection of self-excluders We apply the same approach in order to be alert to suspicious monetary transactions.	√		
What style(s) of gambling is provided to customers?	Solely confined to the provision of gaming machines.		√	
What categories of gambling products are provided to customers?	Categories D, C and B3		√	
Is the business high or low volume?	High volume		√	

Do gambling products pay out low or high stake prizes?	Low stake ranging from 10p to £2. An enhanced level of diligence is applied to monitoring customers gambling on B3 machines on £2 maximum stakes		√	
What risk is posed by transactions with business associates and suppliers?	The Company takes responsibility for third parties with whom it contracts for the provision of any aspect of the business as if they are bound by the same licence conditions and codes of practice.	√		
How is payment delivered to customers and in what form?	Category D and C machines operate solely using cash either in the form of coins or notes. Category B3 operate by the method of TITO with in-built software protection to identify suspicious activity and alert staff.		√	
Location of the gambling venue. Are there any local factors that might have a bearing on risk?	The venue is located in a typical high Street location where the level of crime is in line with national averages. The company maintains a good relationship with local police to keep abreast of current crime trends and perpetrators. The company is registered to receive crime bulletins from bacta		√	
Customers that might pose a risk				
Factor	Appropriate Risk Management/Mitigation	A	B	C
Do new customers stake large amounts of money over short periods of time?	This style of gambling is considered very unlikely to occur and certainly not in line with the gambling products we offer to customers. Should such activity be detected it would be the subject of reporting	√		

<p>Do the majority of customers live and/or work local to the venue?</p>	<p>This company provides a service predominantly to local residents and workers – it is assessed that 90% of our customers are well known to staff with new customers being subject to closer scrutiny</p>	<p>√</p>		
<p>Are any customers involved in a business that handles large amounts of cash?</p>	<p>Local traders operating legitimate businesses in the locality are an element of our customer base but activity does not suggest any heightened risk</p>	<p>√</p>		
<p>Are any customers known to have criminal backgrounds or association with the criminal fraternity?</p>	<p>Very occasionally, customer interaction will provide knowledge of criminal background and/or association leading to closer scrutiny and monitoring of such customers. Our business is not conducive to attracting the criminal fraternity outside of the norm experienced by other licensees.</p>		<p>√</p>	
<p>Reluctant to give you identification, or identification that isn't satisfactory?</p>	<p>Our staff are well versed in the practice of asking customers for satisfactory proof of ID in order to satisfy other requirements such as compliance with age restriction and self-exclusion. We would treat anyone reluctant in providing identification with suspicion that would trigger further investigation.</p>		<p>√</p>	
<p>Loading change machines or TITO machines with cash but gambling minimal amounts</p>	<p>Regarded as low risk and outside our operating experience. However, it is recognised that both facilities have risk potential. Customers using change machines are subject to the same degree of close scrutiny and TITO products operate under industry best practice with software identifying suspicious activity and alerting staff to interact with customers should instances be identified.</p>		<p>√</p>	
<p><i>Spare</i></p>				

Useful Links

National Crime Agency (NCA) - Suspicious Activity Reports (SARs):

<http://www.nationalcrimeagency.gov.uk/contact-us/reporting-suspicious-activity-sar>

National Crime Agency (NCA) – Suspicious Activity Report (SAR) Online System

[https://www.ukciu.gov.uk/\(ero0v5550ikzu355oj4qvbiz\)/saronline.aspx](https://www.ukciu.gov.uk/(ero0v5550ikzu355oj4qvbiz)/saronline.aspx)

National Crime Agency (NCA) - Guidance on submitting better quality Suspicious Activity Reports (SARs)

<http://nationalcrimeagency.gov.uk/publications/732-guidance-on-submitting-better-qualitysars/file>

UKFIU guidance of the revised glossary codes and the reporting routes

<http://www.nationalcrimeagency.gov.uk/publications/725-sar-glossary-code-and-reportingroutes/file>

Money Laundering Regulations: report suspicious activities:

<https://www.gov.uk/guidance/money-laundering-regulations-report-suspicious-activities>

Gambling Commission - latest anti-money laundering news:

<http://www.gamblingcommission.gov.uk/Gambling-sectors/AML/Latest-anti-money-laundering-news.aspx>

