

GAMBLING COMMISSION

Duties and responsibilities under the Proceeds of Crime Act 2002 Advice to operators (excluding casino operators)

September 2009

Contents

Overview	3
Part 1: Introduction	3
Who is this intended for?	3
The purpose of this advice	3
The role of the Commission	3
Part 2: The advice	4
1 What is meant by the proceeds of crime?	4
2 The Proceeds of Crime Act 2002	4
3 Offences under the Proceeds of Crime Act 2002	4
4 Risk-based approach	6
Introduction	6
Identifying and assessing the risks faced by the operator	7
5 Duties under the Proceeds of Crime Act 2002	8
Disclosure	8
Appointment of nominated officer	9
Role of nominated officer	10
Suspicious activities and reporting	10
What is meant by knowledge and suspicion?	11
What constitutes suspicious activity?	12
Suspicious activity reports	13
Appropriate consent	14
Applying for appropriate consent	16
6 Failing to report	18
7 After a report has been made	19
8 Prejudicing an investigation	19
9 Training	20
Annex A – Applicable licence types	22
Annex B – Glossary of terms	23

Overview

- i All gambling operators have a legal obligation to be alert to attempts by customers to gamble money acquired unlawfully, either to obtain 'clean' money in return or simply as a leisure activity. They must report any suspicion or knowledge they or their employees have of such attempts to the Serious Organised Crime Agency (SOCA) and, if circumstances permit, wait for clearance to deal with the customer or until a set period has elapsed.
- ii This advice explains how operators can make sure they and their employees comply with their legal obligations under the Proceeds of Crime Act 2002 (POCA). The advice is inevitably detailed and aimed primarily at operators with a number of employees. Operators with few or no employees may find the quick guide published separately on the Commission's website helpful although it remains the operator's responsibility to understand and comply with the requirements of POCA.

Part 1: Introduction

Who is this intended for?

- iii This advice is directed at all gambling operating licence holders (see Annex A for a complete list), excluding holders of casino licences, who can find guidance on our website.

The purpose of this advice

- iv This advice document sets out duties and obligations under POCA.
- v The document covers a number of topics operators need to be aware of. It should help operators to comply with their responsibilities under POCA.
- vi Operators should devise their own policies and procedures in order to meet their duties and responsibilities under POCA.

The role of the Commission

- vii The Gambling Commission (the Commission) licenses operators and one of the Commission's licensing objectives is to keep crime out of gambling. This advice document is an important tool in meeting that objective. Whilst potential breaches of POCA will normally be reported to SOCA and fall to the Police to investigate, the Commission has a duty to help operators meet their duties and responsibilities under POCA.
- viii Should operators regularly and consistently ignore their duties and responsibilities under POCA, the Commission will consider reviewing the suitability of the operator to carry on the licensed activities. This could result in the suspension or revocation of the operator's licence under sections 118 and 119 of the Gambling Act 2005.
- ix The Commission has the powers of accredited financial investigators under POCA in England and Wales.¹ This means, amongst other things, that 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.

¹ See Statutory Instrument No. 2009/975.

Part 2: The advice

1 What is meant by the proceeds of crime?

- 1.1 Broadly, the term 'proceeds of crime' 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.

2 The Proceeds of Crime Act 2002

- 2.1 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 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.²

- 2.2 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.³

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.

- 2.3 A person benefits from criminal conduct if he or she 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 gained by a person if he or she obtains an interest in it. This would mean that he or she has obtained benefit from the property.⁴ Property is 'criminal property' if it is a benefit from criminal conduct, either directly or indirectly, as long as the alleged offender knows or suspects that it is such.

- 2.4 If a person gains a pecuniary advantage as a result of, or in connection, with criminal conduct, he or she is to be taken to have obtained a sum of money equal to the value of the pecuniary advantage.⁵

- 2.5 The three 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.

3 Offences under the Proceeds of Crime Act 2002

- 3.1 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

² Section 340(3) and (4) of the Proceeds of Crime Act 2002.

³ Section 340(2) of the Proceeds of Crime Act 2002.

⁴ Section 340(5) to (9) of the Proceeds of Crime Act 2002.

⁵ Section 340(6) of the Proceeds of Crime Act 2002.

consolidated, updated and reformed the criminal law relating to money laundering to cover all criminal offences including any dealing in criminal property.

3.2 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.

3.3 POCA creates three 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 the proceeds of crime.⁶ These offences relate to the concealing, arrangement and acquisition of criminal property. In respect of the gambling industry, this generally could involve the taking of cash, cheque, debit or credit card payments from persons in the form of a bet or wager, or holding money on account for a customer for the purposes of gambling.

3.4 Section 327 of POCA provides that a person commits an offence if he or she:

- conceals criminal property (for example, by depositing funds obtained through criminal activity in a gambling account)
- disguises criminal property (for example, by placing funds obtained through criminal activity in 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 company)
- removes criminal property from the United Kingdom (for example, by taking his or her 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.

3.5 Section 328 of POCA provides that a person commits an offence if he or she enters into or becomes concerned in an arrangement which he or she 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.

3.6 Section 329 of POCA provides that a person commits an offence if he or she:

- acquires criminal property
- or uses criminal property
- or has possession of criminal property (for example, via stakes).

However, a person does not commit an offence if he or she acquired or used or had possession of the property for *adequate* consideration. What this means is that, if a person buys or exchanges something which is clearly below market value (inadequate consideration), then they will be committing an offence if the money or property is criminal property. If the person buys or exchanges something at its current market

⁶ Sections 327, 328 and 329 of the Proceeds of Crime Act 2002.

value (adequate consideration), then they will *not* be committing an offence if the money or property is criminal property. This defence protects operators who may be paid for a bet in the normal way with funds that appear to be suspicious, provided they report this suspicion (explained in paragraphs 5.17 to 5.20 below).

- 3.7** These are wide offences that can be committed by anyone, including employees of an operator, who have actual knowledge or suspicion that a customer is using the proceeds of crime. This means that the person must know or suspect that the property is the proceeds of crime in order to have committed the offence in section 329 of POCA.
- 3.8** 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 conduct occurred outside the United Kingdom and the conduct was not criminal in the country where it took place.
- 3.9** While POCA places responsibilities on operators, the legislation also gives them protection if they report suspicious activity. It is a defence to the offences listed above for a person to show that he or she made an authorised disclosure under section 338 of POCA. Disclosure of suspicious activity will be discussed later in this document.
- 3.10** 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.

4 Risk-based approach

Introduction

- 4.1** 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.
- 4.2** The possibility of gambling being used by criminals to assist in spending the proceeds of their criminal activity poses many risks for operators. These include criminal and regulatory sanctions for operators, civil action against the operator and damage to the reputation of the operator, leading to a loss of business.
- 4.3** Operators need to identify, assess and prevent these risks, just like any other business risk. Operators should assess the level of money laundering risk applicable to their business and implement reasonable and considered controls to minimise the risks posed to their business by money launderers. This 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.

- 4.4** Most operators already manage their affairs with regard to the risks inherent in their business, and measure the effectiveness of the policies and procedures they have put in place to manage these risks. A similar approach is appropriate to manage the risks of the operator's business being used for money laundering purposes, including the spending of the proceeds of crime by customers. Existing risk management systems should address money laundering risks. The detail and complexity of these systems will depend on the operator's size and the complexity of their business.
- 4.5** Even though operators outside the regulated sector (clarified in paragraph 3.2 above) are not obliged to have systems and procedures in place, POCA, nonetheless, imposes requirements on all operators that must be satisfied, as a breach can constitute a criminal offence⁷. Systems and procedures can assist operators in complying with their obligations, particularly in relation to reporting suspicious transactions.
- 4.6** In order to detect customer activity that may be suspicious, it is necessary to monitor 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.
- 4.7** Where a customer is assessed as presenting a higher risk it would be advisable to seek additional information in respect of that customer. This will help the operator to judge whether the higher risk that the customer is perceived to present is likely to materialise. Such additional information may include an understanding of where the customer's funds and wealth have come from. The need to 'know your customer' 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.
- 4.8** Deciding that a customer presents a higher risk of money laundering does not automatically mean that he or she 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 spending the proceeds of crime. Operators, therefore, need to remain vigilant and use their experience and common sense in applying their risk-based criteria and rules.
- 4.9** 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 their methods of compliance.
- 4.10** A risk-based approach requires the full commitment and support of senior management, and the active co-operation of all employees. The risk-based approach should be reflected in an operator's policies and procedures. 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.

Identifying and assessing the risks faced by the operator

- 4.11** The operator should assess its risks in the context of how it is most likely to be involved in money laundering and the spending of the proceeds of crime. Assessment

⁷ Sections 327 to 332 of the Proceeds of Crime Act 2002.

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?
- 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 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?

4.12 An example of the risk to operators from exposure to criminal spend is a case where a known criminal, with a previous conviction for money laundering, was released from prison, claimed state benefits, but then spent millions of pounds in gambling establishments. Another case is that of a grandmother with no known gambling history, on a state pension, who began to make weekly bets of about £100. Investigations later revealed that the grandmother was placing the bets on behalf of her grandson, a known criminal, and that the money spent was the proceeds of his criminal activity.

4.13 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).

4.14 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 the spending of the proceeds of crime, are kept under regular review.

5 Duties under the Proceeds of Crime Act 2002

- 5.1** 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.

Disclosure

5.2 If a person carries out any action falling under the principal offences discussed in paragraphs 3.3 to 3.6 above, then failure to make a disclosure to SOCA prior to carrying out the action can result in a criminal offence which can be committed by any employee of the operator. The employee does not commit any of these offences if a proper disclosure is made and, where applicable, appropriate consent is obtained from SOCA.⁸

⁸ Sections 327(2), 328(2) and 329(2) of the Proceeds of Crime Act.

- 5.3** SOCA was established by the Serious Organised Crime and Police Act 2005 and came into being on 1 April 2006. The functions of the UK Financial Intelligence Unit (UKFIU) are now placed within the Proceeds of Crime Department of SOCA. In addition, the Serious Crime Act 2007 provided for the merging of the Asset Recovery Agency and SOCA. This means that, with effect from 1 April 2008, SOCA also undertakes civil recovery and tax investigations in England, Wales and Northern Ireland. SOCA is an intelligence-led agency with law enforcement powers and harm-reduction responsibilities, where harm, in this context, is the damage caused to people and communities by serious organised crime.
- 5.4** The disclosure regime for money laundering is run by the UKFIU within SOCA. It receives and analyses suspicious activity reports (SARs) concerning instances of suspected spending of the proceeds of crime in order to counter money laundering, and makes those SARs available to law enforcement and taxation agencies so they can take the appropriate action.
- 5.5** In all instances where customers' funds are known or suspected of having criminal origins, a disclosure must be made to SOCA at the earliest opportunity using the methods set out on the SOCA website: www.soca.gov.uk.
- 5.6** 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 SOCA
 - resources which can be used to resolve difficult issues regarding a disclosure
 - how and when a disclosure is to be made to SOCA
 - 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

- 5.7** Whilst it is only incumbent upon those companies in the regulated sector (which, in the gambling sector, only includes non-remote and remote casinos) to appoint nominated officers, operators in the non-regulated sector should also consider appointing a nominated officer, as this can help them meet their obligations under POCA more effectively. This can particularly assist in the reporting of suspicious activity to SOCA, 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 paragraphs 5.38 and 5.40 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 cannot be prosecuted for the principal offences under POCA, as the decision whether to report or not to report to SOCA and request appropriate consent is the sole responsibility of the nominated officer.
- 5.8** The nominated officer should be of sufficient seniority to make decisions on reporting, which will have an impact on the operator's business relationship with its customers and its exposure to criminal, civil, regulatory and disciplinary sanctions. The nominated officer should also have sufficient responsibility to be allowed access to customer information and the operator's business information to enable informed decisions on suspicious activity to be made.
- 5.9** The nominated officer should receive all disclosures from employees and review them with a view to making a decision on whether to make a disclosure. Where necessary,

the nominated officer must make the required disclosure to SOCA as soon as practicable after the information has come to him or her.

- 5.10** It is important to note, however, that the position of a nominated officer brings with it responsibilities and associated offences, if he or she 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 POCA⁹.
- 5.11** Operators with chains of outlets may have an employee who holds a Personal Management Licence issued by the Commission, who would be suitable to appoint as the nominated officer for that chain. In the case of small or solo operators, a person of reasonable standing in the business can act as the nominated officer.
- 5.12** Where the operator does 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.

Role of the nominated officer

- 5.13** 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 SOCA. 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 SOCA 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.
- 5.14** Where an operator has appointed a nominated officer, he or she will:
- receive internal disclosures under Part 7 of POCA
 - decide whether these disclosures should be reported to SOCA
 - if appropriate, make such external reports to SOCA
 - ensure that appropriate consent is applied for as necessary.
- 5.15** The nominated officer should be able to monitor the day-to-day operation of the operator's anti-money laundering (AML) policies in general, including policies to deal with the spending of the proceeds of crime by customers, and respond promptly to any reasonable request for information made by the Commission or law enforcement bodies.
- 5.16** Where AML tasks are delegated by an operator's nominated officer to another employee, the nominated officer is still expected to take ultimate managerial responsibility for AML issues and he or she 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

- 5.17** Operators in the non-regulated sector are required to make a report in respect of

⁹ www.opsi.gov.uk/acts/acts2002/ukpga_20020029_en_22#pt7

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 the spending of the proceeds of crime.

5.18 Operators will only need to consider making a disclosure if they have actual knowledge or subjective suspicion.

5.19 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.

5.20 If the nominated officer or manager determines that a report warrants the submission of a SAR, he or she must report the matter to SOCA. Under POCA, the nominated officer or manager is required to make a report to SOCA as soon as is practicable if he or she 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?

5.21 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.¹⁰

5.22 Suspicion is more subjective and falls short of proof based on firm evidence. Suspicion has been defined by the courts as being beyond mere speculation and based on some foundation. As a judge put it: "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 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 speculation.¹¹

5.23 The test to decide whether you hold a suspicion is a subjective one. If you think a transaction is suspicious, you are not expected 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

¹⁰ http://www.opsi.gov.uk/acts/acts2002/ukpga_20020029_en_22#pt7

¹¹ Longmore LJ, *R v Da Silva* [1996] EWCA Crim 1654.

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 and how easy it is to make enquiries.

5.24 Unusual patterns of gambling, including gambling involving particularly 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 SOCA. 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 cash amount to spend.

5.25 In order for a disclosure 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.

What constitutes suspicious activity?

5.26 There are numerous things that can make someone either know or suspect that they are dealing with the proceeds of crime. Some common 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 or she 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 disclosure 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. 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 an unusual 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 the proceeds of crime.
- Operators are advised that instances of high spend by customers that lead to commercial risk for the operator may also indicate suspicious activity.

Suspicious activity reports (SARs)

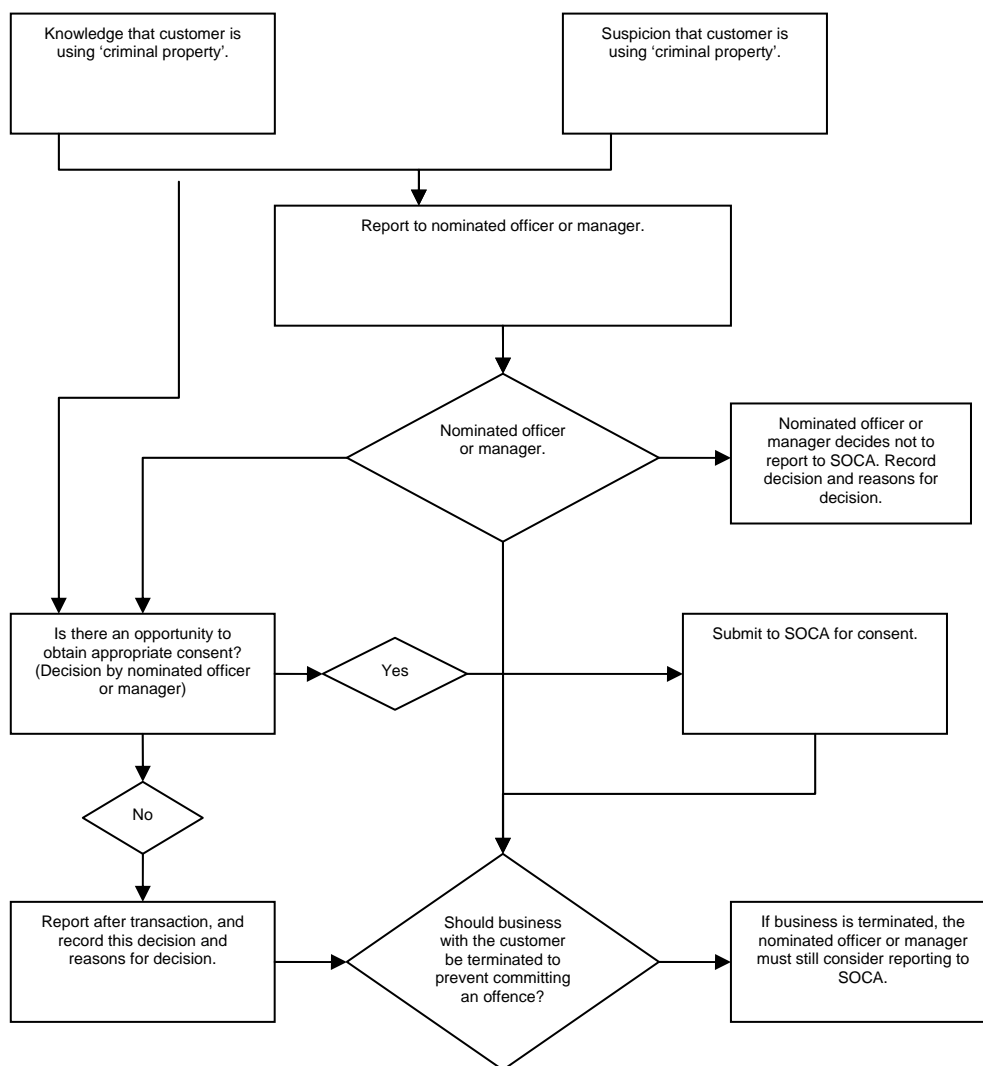
- 5.27** Disclosures under POCA of known or suspected money laundering activity must be made in the prescribed manner and form.¹² In this regard, the operator or operator's nominated officer (where one has been appointed) must disclose to SOCA any transaction or activity that, after his or her evaluation, he or she knows or suspects may be linked to money laundering. The prescribed form for the making of a disclosure to SOCA is a SAR. Such reports must be made as soon as is reasonably practicable after the information comes to the operator or nominated officer.
- 5.28** SOCA's preferred method for operators to submit their SARs is the 'SOCA Suspicious Activity Report Form'¹³, which can be found on the SOCA website at www.soca.gov.uk/financialIntel/suspectActivity.html#forms. Guidance on completing the form can be found at www.soca.gov.uk/financialIntel/formsGuide.html. SOCA prefers these forms to be submitted electronically using SAR Online, SOCA's web based reporting mechanism. SAR Online can be used by anyone with access to the internet and can be found at <https://www.ukciu.gov.uk/saronline.aspx>
- 5.29** Any reporter choosing not to use one of the electronic reporting methods is advised to obtain a copy of the SOCA preferred form. This form can be downloaded from the SOCA website and be completed by the person making the report on their own computer. However, in cases where it is not possible to complete the form on a computer, hard copy versions of the forms can be completed by hand. After completion, all forms should be posted to: UKFIU, PO Box 8000, London SE11 5EN. They can also be faxed to 0207 238 8286.
- 5.30** Operators should include in each SAR as much relevant information about the customer, transaction or activity that it has in its records. SOCA's website contains guidance on completing SARs in a way that gives most assistance to law enforcement (www.soca.gov.uk/financialIntel/formsGuide.html). In particular, SOCA has published a glossary of terms which they prefer operators to use when completing SARs (www.soca.gov.uk/financialIntel/SARglossary.html). This will also speed up consideration of the report by SOCA.
- 5.31** The bulk submission of SARs or those made through the SAR Online system will receive an acknowledgment of receipt, which will include an automatically generated ELMER (the SOCA database of SARs) reference number.
- 5.32** SOCA will not acknowledge receipt of any SARs sent by post or fax.
- 5.33** SARs will generally be the normal method of reporting, but reports may also take the form of a limited intelligence value report (LIVR), which may be appropriate in cases where operators know that a law enforcement agency already has an interest in the matter. SOCA provides detailed information on when LIVRs should be used (www.soca.gov.uk/financialIntel/suspectActivity.html), but it is suggested that, where operators are in doubt, they complete a SAR form.
- 5.34** In order that an informed overview of the situation may be maintained, all contact between operators, SOCA and other 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). Where a nominated officer has not been appointed, it is suggested that contact should be through a senior manager in the operator's organisation.

¹² Section 339(1) of the Proceeds of Crime Act 2002.

¹³ Operators that already use 'Encrypted Bulk File' submission can continue to submit reports electronically by those means.

5.35 Should operators require assistance, the UK FIU postal address is: PO Box 8000, London, SE11 5EN. The Unit can also be contacted during office hours on: 020 7238 8282.

Figure 1: Knowledge or suspicion of spending of proceeds of crime (subjective test)



Appropriate consent

5.36 If operators handle any proceeds of crime, they may commit a principal money laundering offence. However, if the operator submits a SAR to SOCA, this can amount to a defence. The ‘reporting defence’ includes the statutory mechanism which allows SOCA either to agree to the transaction going ahead (this is called ‘appropriate consent’), or to prevent the suspected money laundering going ahead.¹⁴

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

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

¹⁴ Section 335 of the Proceeds of Crime Act 2002.

- 5.38** A nominated officer (where one has been appointed by the operator), police constable, SOCA employee or customs officer can give a person (which may include employees of the operator) actual 'appropriate consent' to a suspect transaction proceeding.¹⁵
- 5.39** 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' has expired and no restraint order is obtained by the authorities (where the moratorium period is 31 days starting with the day on which the person receives notice that consent to the doing of the act is refused).¹⁶
- 5.40** 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 SOCA and, either:
- the SOCA 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' has expired and no restraint order is obtained by the authorities (where the moratorium period is 31 days starting with the day on which the person receives notice that consent to the doing of the act is refused).¹⁷
- 5.41** Reporting suspicious activity before or reporting after the event are not equal options which an operator can choose between.
- 5.42** 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.¹⁸ Where a customer instruction is received prior to a transaction or activity taking place, or arrangements being put in place, 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 SOCA 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 SOCA gives consent.¹⁹
- 5.43** In the gambling industry, business is often conducted out of normal office hours. In addition, gambling transactions are 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 is often not 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.²⁰
- 5.44** 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

¹⁵ Section 335(1) of the Proceeds of Crime Act 2002.

¹⁶ Section 335(2) of the Proceeds of Crime Act 2002.

¹⁷ Section 336 of the Proceeds of Crime Act 2002.

¹⁸ Section 327(2)(b) of the Proceeds of Crime Act 2002.

¹⁹ Section 336(3) and (4) of the Proceeds of Crime Act 2002.

²⁰ Section 327(2)(b) of the Proceeds of Crime Act 2002.

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 will be advisable to report the matter to SOCA directly, where feasible.

- 5.45** Operators or nominated officers will need to think very carefully about whether or not they wish to continue to do business with the suspected customer. Relevant considerations should be the potential for criminal offences under POCA, as well as potential damage to business reputation and other commercial factors.
- 5.46** Operators should also note that the reporting defence is not intended to be used repeatedly in relation to the same customer. If patterns of gambling lead to a steadily increasing level of suspicion of money laundering or even 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 sensitively, there should be no risk of prejudicing an investigation. However, given that operators will have previously reported the customer to SOCA, they should normally liaise with the agency about the best approach to turning the customer away.
- 5.47** How suspected customers 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 occur in practice.
- 5.48** For example, the operator may consider one transaction to be suspicious and reports it to SOCA 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. 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

- 5.49** Operators should apply for appropriate consent using the SAR Online facility (<https://www.ukciu.gov.uk/saronline.aspx>) where they have no existing arrangements to use other electronic media (bulk submission). Operators should complete the standard SAR form and ensure that they tick the "consent required" option and tick the option to indicate that they are disclosing under POCA. The SAR Online process provides an automatic acknowledgement of the report and an ELMER reference number.
- 5.50** In circumstances where operators are unable to use SAR Online (<https://www.ukciu.gov.uk/saronline.aspx>), they should fax their disclosure requesting consent to 0207 238 8286. They should use SOCA's standard SAR form which can be downloaded from the SOCA website (www.soca.gov.uk). Persons submitting the reports should ensure that they tick the "consent required" option and tick the option to indicate that they are disclosing under POCA.
- 5.51** Operators are strongly discouraged from using the postal system to submit SARs requiring consent as this may delay the decision on consent being relayed back to the operator.
- 5.52** Where operators have submitted a consent disclosure electronically or via fax, they are not required to post a duplicate report.

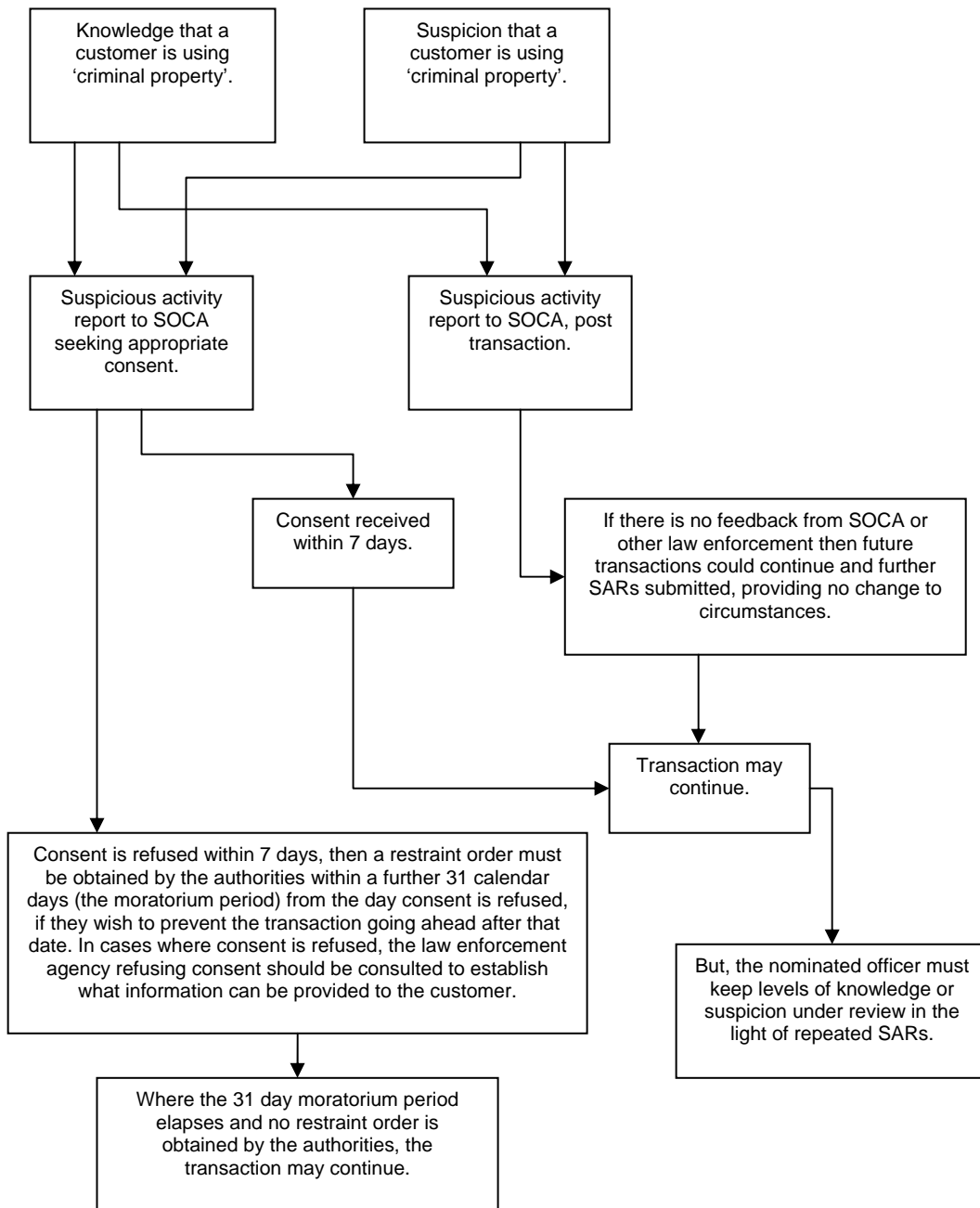
- 5.53** All requests for appropriate consent are treated as a priority within SOCA. The aim is to provide the quickest possible response to the person who has made the report. As soon as a decision has been made in relation to a request for consent it will be relayed to the person who has made the report without delay, but some consent decisions will take longer than others.
- 5.54** A consent decision will usually be communicated by telephone to the person who made the report in order to provide the quickest possible response. SOCA will also send a letter by post recording the decision, but there is no requirement to wait for this letter in order to proceed with the prohibited act if consent has already been granted verbally.
- 5.55** SOCA has indicated that it is mindful of the sensitivity of SARs, even within the same organisation, and endeavours to communicate only with persons whose details are verifiable by SOCA. The person who made the report may, therefore, wish to appoint a specified deputy to deal with decisions relating to the consent request in his or her absence, in order to avoid delays. Details of nominated officers, Money Laundering Reporting Officers or other persons responsible for making reports, and their deputies, including their direct contact telephone numbers, should be registered with SOCA. Registration is available through SAR Online (<https://www.ukciu.gov.uk/saronline.aspx>) or through forms available on the SOCA website (www.soca.gov.uk).
- 5.56** When consent is granted by SOCA or no response is received within seven working days, the operator is free to undertake the reported prohibited act(s) without committing a money laundering offence in relation to POCA. Operators should note that consent does not extend to any acts or criminal property not detailed in the initial disclosure or agreed with SOCA.
- 5.57** The seven day notice period commences on the day after a disclosure is made and excludes weekends and bank holidays. The purpose of the seven day notice period is to allow SOCA and its law enforcement partners sufficient time to assess the risk, and analyse, research and undertake further enquiries relating to the disclosed information, in order to determine the best response to the request for consent.
- 5.58** Where SOCA gives notice that consent to an act is refused, a further 31 day period (the 'moratorium') commences on the day that notice of refusal is given. The 31 days include weekends and bank holidays.²¹ It is an offence to undertake the act during this period as the participant would not have the appropriate consent. The moratorium period enables SOCA to further their investigation into the reported matter using the powers within POCA in relation to the criminal property (for example, by applying to the courts for a restraint order). If the moratorium period expires and no such action has been taken, the operator is free to proceed with the act(s) detailed in the initial disclosure.
- 5.59** On 5 December 2008, the Home Office published a circular on the so-called 'consent regime' in POCA.²² This circular contains guidance on the operation of the regime and was drawn up in consultation with SOCA, the Association of Chief Police Officers, the Association of Chief Police Officers (Scotland), the Crown Prosecution Service, HM Revenue and Customs, the Revenue and Prosecution Office and others. It was issued to ensure consistency of practice by law enforcement agencies in considering requests for consent. The circular sets out the principles by which the law enforcement agencies should make decisions on consent and how those principles should be applied. Law enforcement agencies are encouraged to recognise the potential, significant impact that each SAR and consent decision can have. This includes, for example, whether or not the proceeds of crime are recovered, crime is prevented,

²¹ Section 335 of the Proceeds of Crime Act 2002.

²² <http://www.homeoffice.gov.uk/about-us/publications/home-office-circulars/circulars-2008/029-2008/>

honest individuals and operators are exposed to financial loss or litigation, and the smooth running of commercial business is disrupted.

Figure 2: Appropriate consent



6 Failing to report

6.1 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 SOCA as soon as practicable after the information is received, they are open to criminal prosecution.²³ The criminal sanction under POCA is a prison term of up to five years and/or a fine.²⁴

²³ Section 332 of the Proceeds of Crime Act 2002.

²⁴ Section 334 of the Proceeds of Crime Act 2002.

- 6.2** For all failure to disclose offences it will be necessary to prove that the person nominated to receive disclosures 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.

- 6.3** Operators, therefore, are strongly advised to comply with the reporting requirements imposed on them by POCA.

7 After a report has been made

- 7.1** 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. This contact may also include seeking supplementary information or documentation from the operator and from other sources by way of a court order.

- 7.2** 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.

8 Prejudicing an investigation

- 8.1** Under section 342 of POCA a person commits an offence if he knows or suspects that a constable, customs officer or accredited financial investigator is acting (or proposing to act) in connection with a confiscation investigation, a civil recovery investigation or a money laundering investigation which is being or is about to be conducted and:
- he or she makes a disclosure which is likely to prejudice the investigation
 - or he or she 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.²⁵

- 8.2** 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 (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.

- 8.3** Those working in the gambling sector should be aware of the provisions in relation to this offence. There are a number of defences, including that the person did not know or suspect that the disclosure is likely to prejudice the investigation.

- 8.4** Once an internal disclosure has been made to the nominated officer (where one has been appointed) or an external SAR has been made to SOCA, it is a criminal offence for anyone to release information that is likely to prejudice an investigation.²⁶ Reasonable enquiries of a customer, conducted in a tactful manner, regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity is prudent practice and should not result in the offence of prejudicing an investigation.

- 8.5** 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

²⁵ Section 342(2) of the Proceeds of Crime Act 2002.

²⁶ Section 342(2)(a) of the Proceeds of Crime Act 2002.

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).²⁷ It is, however, a defence if the person does not know or suspect that disclosure of the information is likely to prejudice the investigation, or if the disclosure is made in compliance with other provisions of POCA, or similar enactments.²⁸

8.6 The offence of prejudicing an investigation can be committed before or after a disclosure has been made.

9 Training

9.1 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 SOCA. In the case of solo operators or operators without specific AML employees, advice is always available directly from SOCA.

9.2 One of the most important controls over the detection of the spending of the proceeds of crime and the 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.

9.3 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 anything that gives grounds for suspecting the spending of the proceeds of crime and money laundering activity.

9.4 Under POCA, individual employees face criminal penalties if they are involved in money laundering activity. If they do not make a report when required they may also face criminal sanctions. It is important, therefore, that employees are made aware of their legal obligations and are given training in how to correctly discharge them.

9.5 The content of any 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.

9.6 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 SOCA
- the potential effect of a breach of POCA on the operator and its employees.

²⁷ Section 342(1) of the Proceeds of Crime Act 2002.

²⁸ Section 342(3) of the Proceeds of Crime Act 2002.

- 9.7** Where a nominated officer has been appointed, he or she 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.
- 9.8** SOCA publishes a range of material at www.soca.gov.uk, such as threat assessments and risk profiles, of which operators may wish to make their employees aware. The information on the SOCA 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.

Annex A - Applicable licence types

Licence type	Licence category											
	A	B	C	D	E	F	G	H	I	J	K	L
non-remote bingo licence	✓	✓	✓	✓	✓							
general betting - standard licence	✓	✓	✓	✓	✓							
non-remote general betting - limited licence	✓	✓	✓									
non-remote pool betting licence	✓	✓	✓									
non-remote betting intermediary licence	✓	✓	✓									
gaming machine general AGC licence	✓	✓	✓	✓	✓							
gaming machine general FEC licence	✓	✓	✓	✓	✓							
non-remote external lottery manager licence	✓	✓	✓									
non-remote society lottery licence	✓	✓	✓									
remote bingo operating licence holder						✓	✓	✓	✓	✓	✓	✓
general betting - standard virtual events licence						✓	✓	✓	✓	✓	✓	✓
general betting - standard real events licence						✓	✓	✓	✓	✓	✓	✓
remote general betting - limited licence						✓						
remote pool betting licence						✓	✓	✓	✓	✓		
remote betting intermediary licence						✓	✓	✓	✓	✓		
remote betting intermediary (trading rooms) licence						✓	✓	✓				
remote external lottery manager licence						✓	✓	✓				
remote society lottery licence						✓	✓	✓				

Annex B - Glossary of terms

AML	Anti-money laundering.
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.
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 SOCA under POCA.
SOCA	The Serious Organised Crime Agency, which was established by the Serious Organised Crime and Police Act 2005 and came into being on 1 April 2006. SOCA is an intelligence-led agency with law enforcement powers and the responsibility to reduce the harm caused to people and communities by serious organised crime). SOCA is the organisation to which suspicious activity is reported.
UKFIU	The United Kingdom Financial Intelligence Unit, which is the unit within SOCA that operates the disclosure regime for money laundering.

Gambling Commission September 2009

Keeping gambling fair and safe for all

For further information or to register your interest in the Commission please visit our website at: www.gamblingcommission.gov.uk

Copies of this document are available in alternative formats on request.

Gambling Commission
Victoria Square House
Victoria Square
Birmingham B2 4BP

T 0121 230 6666
F 0121 230 6720
E info@gamblingcommission.gov.uk

ADV 09/10