GAMBLING COMMISSION

Proposed amendments to licence conditions and codes of practice (LCCP) for all operators in relation to the prevention of crime associated with gambling

Consultation
September 2015

Contents

1 Introduction

1.1 This consultation proposes a number of improvements to our *Licence conditions and codes of practice*[1] (LCCP) relating particularly to the prevention of crime associated with gambling. It also seeks views on other areas linked to crime.

1.2 The Gambling Commission (the Commission) has a duty to permit gambling so long as it thinks it reasonably consistent with the three licensing objectives set out in the Gambling Act 2005[2] (the Act). These objectives are:

- to keep gambling free from crime [and from being associated with crime]
- to ensure that gambling is fair and open
- to protect children and vulnerable people from being harmed or exploited by gambling.

1.3 The Commission's LCCP, together with the Act and associated regulations, statutory guidance to licensing authorities, and the Commission's formal statement of principles, form a central framework for regulating commercial gambling. The LCCP comprises licence conditions, which are mandatory obligations[3] on the holders of gambling operating licences. It also includes two types of code of practice provision – social responsibility provisions, which have the force of licence conditions, and ordinary code provisions, which, although not mandatory, set out good practice that we expect responsible operators to follow. In areas covered by ordinary code provision, licensees should adopt alternative approaches only where they can demonstrate that to do so would be equally effective in achieving the desired objective.

1.4 The LCCP is based on the principle that licensees are responsible for delivering the licensing objectives within the framework outlined above. The LCCP requires licensees to put in place effective policies and procedures for managing a range of risks to the licensing objectives, and to assure themselves that what they are doing is actually working. In most cases, the LCCP does not prescribe detailed rules, but describes the outcomes that we expect licensees to achieve within the framework. We consider that licensees themselves are best placed to decide how to secure those outcomes cost-effectively within their own particular circumstances with the minimum of regulatory prescription. This makes the LCCP more proportionate and less burdensome for licensees.

1.5 We first published the LCCP in 2007, to coincide with the Act, itself the first major reform of gambling regulation since the 1960s, coming into force. The first LCCP set out headline aspirations in many areas, expecting good practice and experience to develop over time. Since 2007, the Commission has reviewed various areas of the LCCP, refining and adding detail based on evidence and good practice from our casework and from operators. In incorporating further detail, however, we try to strike the right balance between giving licensees flexibility to find the most appropriate solutions and setting requirements sufficient to discourage the less responsible from undercutting the responsible by cutting corners or ignoring good practice.

1.6 This review of the LCCP focuses on the first licensing objective, keeping gambling free from crime and from being associated with crime. We and the gambling industry now have nearly ten years of experience in the operation of the Gambling Act 2005, in how crime manifests itself in relation to gambling in Great Britain, and how to manage the risks. While both we and the industry will of course continue to develop our understanding in these areas, the time is right to distil what we have learned collectively into what we hope and expect will be significant strengthening of the industry's defences against crime.

---

[1] Licence conditions and codes of practice (February 2015, updated April 2015)
[2] Gambling Act (2005) as amended by the Gambling (Licensing and Advertising) Act 2014.
[3] One mandatory obligation, imposed by licence condition 2, is that operators comply with the Commission's technical standards and requirements for the timing and procedure for testing. These include gaming machine technical standards and remote gambling and software technical standards, both of which therefore have the force of licence conditions.

1.7 We have looked at evidence from Commission casework and considered where we could improve our existing regulatory tools to support good operator practices, and to tackle poor practice more effectively, in order to better support this first objective.

1.8 In considering the crime related provisions of the LCCP, we have reflected our current approach to disorder (as opposed to crime) associated with gambling premises. While such disorder can be a source of considerable public concern, it tends to be limited to specific localities and therefore is best addressed through partnership between gambling businesses, licensing authorities and other local agencies. The Safebet Alliance[4] remains an excellent example of such a partnership. The Commission's revised statutory guidance to licensing authorities, currently subject to consultation, aims to strengthen local partnerships, encouraging gambling businesses and licensing authorities to work together to address issues of local concern, including disorder.

1.9 The review follows a detailed review of social responsibility elements in the LCCP in 2014. Some elements of the 2014 social responsibility review also linked to crime, eg, access to gambling by children and young people is an offence, but we addressed this in the last consultation. We do not propose to revisit any of the areas covered in the last consultation at this time.

1.10 This review comes at a time when work on implementing the 4th European Union Anti Money Laundering Directive (the Directive), adopted in June 2015, is well under way. However, it should not be seen as directly linked to or driven by that process. Through our work with operators on anti-money laundering it has become clear that the regulatory tools (as opposed to the criminal sanctions available through the Proceeds of Crime Act and the Money Laundering Regulations) available to the Commission require some development to become as effective as they should be. In most circumstances, the Commission's Statement of Principles commits us to pursuing regulatory rather than criminal avenues when dealing with those we license. However, the current LCCP provisions, drafted nearly ten years ago, do not yet give us or operators the full flexibility needed to deliver against that principle. This leaves operators at greater risk of criminal sanction when regulatory procedures would be more effective. We intend to use this review to address that risk.

1.11 Not all of the proposals in this consultation are for specific changes to the LCCP at this stage. We intend that some proposals should stimulate wider debate on emerging issues, for example, on the use of digital currencies in gambling. In this respect, the consultation seeks views on how we should develop our current position.

1.12 We are also using this opportunity to consult on an update to the Commission's guidance for remote and non-remote casinos, The Prevention of Money Laundering and Combating the Financing of Terrorism (third edition). This document is attached at Appendix A.

1.13 Gambling operators can contribute to this review of the LCCP and related areas by pooling their information and sharing their experiences to improve our understanding of risks relating to crime in gambling. The approach we have taken to date has been to encourage operators to work together and share best practice and learning where practical. There remains a question, however, about the extent to which regulation should be used to accelerate the pace of such sharing, and in particular encourage or mandate the sharing of data to develop new insights and tools.

1.14 The proposed amendments in this paper will be of interest to **all gambling operators**, to gambling customers and to bodies or individuals with an interest in the regulation of gambling.

[4] The Safe Bet Alliance sets out national guidelines to improve safety and security for staff and customers in high street betting shops. The guidelines were developed in partnership with the Metropolitan Police, Crimestoppers, the Institute of Conflict Management and Community Union.

1.15 Although the proposals are relevant to all sectors, in some areas of the consultation we have broken down the requirements for individual gambling sectors as with the existing LCCP.

1.16 Where changes are proposed to LCCP provisions we have shown additions in bold and deletions as strikethrough.

1.17 We hope that the gambling industry and wider interest groups will engage constructively with the questions raised in this consultation. Although we have posed some specific questions within this consultation, we are aware that respondents may have interests in some of the areas discussed that go beyond the questions posed. We are happy to accept other comments on areas discussed in the consultation.

1.18 We are seeking responses to this consultation by 30 December 2015. Further details on how to respond are included at Section 8 of this document.

1.19 Following completion of this consultation, and taking into account the responses received, we expect to introduce new and amended licence conditions and codes of practice. We may issue supplementary consultations where consultation responses require further consideration before making changes. We expect that new or amended provisions will come into force during 2016, following the three month period of notice required for any changes.

2 Provision of information to the Commission about gambling-related crime

2.1 Crime can relate to gambling operators in several different ways. In some cases, operators are the victims of crime but in other cases they might, usually unknowingly, benefit financially from crime. This is particularly the case where the proceeds of crime have been spent on gambling. Organised criminals may also seek to acquire gambling businesses for criminal purposes, including money laundering. This risk is addressed through the fit and proper checks undertaken at licensing stage.

2.2 The LCCP requires licensees to provide information about gambling-related crime to the Commission, and we give lower priority to crimes against licensees that do not impact on the licensing objectives or on other players. However, the limitations of our existing reporting requirements mean that operators do not always provide some information necessary for us to undertake our statutory functions effectively in terms of keeping gambling free from crime and from being associated with crime. We therefore propose to revisit these requirements in this section, and consider both an amendment to the LCCP and/ or whether licensees require more guidance on the types of reports we expect.

2.3 We acknowledge that this is a complicated area because of the range of ways in which crime and gambling can link, for example:

- Situations in which a customer commits an offence that involves the licensee, but in which the operator is not the victim (for example, the spending or “washing” of the proceeds of crime)
- Offences committed against a licensee, whether by a customer or not
- Offences committed by customers against other customers
- Offences committed by a licensee’s employees in collusion with customers
- Offences committed by employees against a licensee
- Offences committed by employees against customers.

2.4 Each of these categories has the potential to impact differently on the licensing objective of keeping crime out of gambling. We are therefore seeking views on the most effective and proportionate way of ensuring that we receive the information we need to carry out our duties effectively.

The current position

2.5 Licence conditions 15.1.1 (reporting suspicion of offences etc – non-betting licences) and 15.1.2 (reporting suspicion of offences etc - betting licences) both cover information that licensees must provide to the Commission in relation to criminal offences. However, both licence conditions refer only to offences under the Gambling Act 2005, or to licence breaches, rather than to broader criminal offences.

2.6 Although these conditions clearly set out the requirement for licensees to notify the Commission of offences under the Act, it may be less clear whether this is an absolute requirement or whether there is some discretion as to the scale of offence that licensees must report. Licensees report events through the Commission’s online reporting portal.

2.7 For example, a licensee should report underage gambling or underage entry into age restricted premises (section 48 and 49 offences) when it is certain that an offence has been committed. That is, when there is proof that someone is underage, rather than a suspicion that they may be, or a failure to prove otherwise. We do not have data on the completeness of reports we receive but we suspect that different licensees interpret the requirement differently, eg, some providing evidence of suspicion of underage entry. Therefore, we may need to provide clearer advice about which reports we expect to receive to get more consistent reporting.

2.8 Similarly, licensees should report cheating at gambling (a section 42 offence). Our evidence from reports appears to indicate that we receive information about higher value or otherwise more significant cases, but not about low level cheating identified and stopped through the proper supervision of gaming. Regardless of value, licensees should record all such occurrences. Again, it may be appropriate for the Commission to provide advice on when licensees should make reports.

2.9 Licence condition 15.2.1 (reporting key events) sets out a list of key events. Licensees must report any such to us as soon as reasonably practicable and in any event within five working days of the licensee becoming aware that the event has occurred. The definition of a key event is "an event that could have a significant impact on the nature or structure of a licensee's business".

2.10 Under 15.2.1, licensed operators are currently obliged to make the Commission aware of:

> "Any investigation by a professional, statutory, regulatory or government body (in whatever jurisdiction) into the licensee's activities, or the activities in relation to the licensed entity of a personal licence holder or a person occupying a qualifying position employed by them, where such an investigation could result in the imposition of a sanction or penalty which, if imposed, could reasonably be expected to raise doubts about the licensee's continued suitability to hold a Gambling Commission licence."

2.11 Where crime involves employees and does not relate to an offence under the Act or the LCCP, licensed operators may be required to make a report dependent upon whether or not the employee is a licensed individual. Licence condition 15.2.1 (reporting key events), item 22, requires a licensee to report if a licensed individual is subject to a disciplinary sanction for reasons of gross misconduct. Such reports are also likely to pick up non-gambling related crimes, eg, theft from the employer. However since the majority of employees in the gambling industry are not licensed there may be value in introducing a wider reporting requirement for crime against operators carried out by employees, where these impact on the licensing objectives or on players.

2.12 Current reporting requirements are therefore based upon two key factors: whether an offence under the Gambling Act 2005 has been committed; and whether any employees involved hold a personal management licence (PML) or personal functional licence (PFL), or whether they hold one of a number of qualifying positions listed in Licence condition 15.2.1. We are interested in views on whether further guidance in these areas would help licensees to make consistent reports to us.

Evidence

2.13 In recent years, we have devoted increasing attention and resources to investigating licensees for non-compliance. A number of those investigations have identified significant failings on the part of licensees in delivering the licensing objective of keeping crime out of gambling, particularly in the area of anti-money laundering.

2.14 Several of the cases only came to our attention as a result of media reports about gambling-related crime, through enquiries from law enforcement agencies or through intelligence sharing by other bodies. In the majority of cases, licensees themselves did not make the Commission aware of information about the gambling-related crime involved. At present, there is no clear requirement in LCCP for them to do so.

Example
A customer of a major gambling operator was recently prosecuted for offences under the Proceeds of Crime Act 2002, after spending a six-figure sum with the operator. Information provided by the operator played a key role in the trial by providing a clear record of the spending involved.

However, the Commission only became aware of the case due to a referral from a police force, following which the Commission made enquiries of the operator. Ultimately, this led to an investigation that revealed serious shortcomings in the operator's money laundering controls.

Had the police force in question not made the referral to the Commission, it is unlikely that we would have become aware of the case in any other way.

2.15 We are aware that in many cases licensees offer valuable assistance to the police and other law enforcement agencies investigating and preventing crime. There will of course be many situations where a crime is committed which relates to a licensee, but which does not demonstrate any shortcomings in the licensee's efforts in pursuit of the licensing objective of keeping gambling free from crime and from being associated with crime. For example, there may be instances when a customer causes criminal damage to a licensee's property, or threatens to assault or actually assaults a staff member. Licensees should report these incidents to the proper authorities, but are not required to report them to us, where they are not linked to the first licensing objective (although licensees must take appropriate action and record such situations if they are linked to a customer who is or appears to be at risk of harm from gambling, in line with their social responsibility requirements). We are, of course, interested in learning about continued incidents that might impact on an operator's ability to provide gambling facilities. However, as previously stated, we give lower priority to incidents that do not affect the licensing objectives or other players, and would expect such matters to be dealt with through a review of a premises licence.

2.16 We are also aware of several cases in which offences were committed against operators, either by customers or by employees. For example, in casinos, where dealers can influence the outcome of the gaming, there have been cases of dealers colluding with associates to pay out incorrect winnings at the expense of the licensee, or systematically defrauding their employer by stealing from the tables. Employees working in back office functions have also carried out non-gaming related thefts. As these cases impact on the first licensing objective, we have an interest in hearing about them.

Proposed changes to the licence conditions

2.17 The current reporting requirements are formulated in a way that means certain crimes that could raise concerns about whether licensees are meeting the licensing objectives do not have to be reported. On that basis, we are concerned that operators may have, but not be sharing with us, a lot of information about gambling-related crime. We consider that having clearer reporting requirements relating to information about crime would enable us to deliver our duties in this area more effectively and consistently.

2.18 The current system of reporting also means that there may actually be a disincentive for operators to share information about crime with us. Currently, if a licensee shares such information they may become subject to additional scrutiny and even the potential for formal regulatory action. In the absence of a specific licence condition that requires a licensee to share this information, keeping it from us could be tempting despite ordinary code provision 8.1 (information requirements), which informs licensees that they should be open with the Commission. A clearer requirement will help to level the playing field in this area and ensure that we gain a range of information that will help us to take consistent, proportionate and risk-based decisions.

2.19 That said, we are aware that any additional requirement to submit information has an impact on licensees. We are also aware that in the course of their business, licensees will encounter a large number of potential criminal offences and investigations, many of which will have little or no impact on the delivery of the licensing objectives. We do not consider it would be proportionate or helpful to oblige licensees to provide information about all the criminal offences or investigations by law enforcement agencies of which they become aware. We are therefore seeking views on the most proportionate and effective way to balance any requirement in this area with the potential regulatory burden.

Proposed addition to licence condition 15.2.1
Reporting key events
All operating licences

A key event is an event that could have a significant impact on the nature or structure of a licensee's business. Licensees must notify the Commission, or ensure the Commission is notified, in such form or manner as the Commission may from time to time specify, of the occurrence of any of the following key events as soon as reasonably practicable, and in any event within five working days of the event's occurrence.

29. Any criminal investigation by a law enforcement agency, including the police and the National Crime Agency, in which the licensee is involved in circumstances where the Commission could reasonably be expected to question whether the licensee had taken sufficient steps to keep crime out of gambling. This applies whether the investigation relates to crimes allegedly committed:

- **by or against the licensee**
- **by one or more employees of the licensee (whether or not the crime is committed against the licensee**
- **by a third party in circumstances involving the gambling facilities provided under the licence.**

Consultation questions

Q1. What are your views on the introduction of an additional key event obliging operators to provide information to the Commission about investigations of crimes committed against them, crimes committed by their staff or crimes committed using its gambling facilities (for example, spending or laundering the proceeds of crime)?

Q2. For operators, what information about gambling-related crime does your organisation already record centrally, and in what form?

Q3. What are your views on the most proportionate way to ensure that the Commission is provided with information about gambling-related crime in a way that strikes an effective balance between the need for this information and the regulatory burden that providing it would impose?

Q4. Do you consider the proposed wording above to be sufficiently clear on what kinds of gambling-related crimes the Commission would expect to be provided with information about? If not, what wording or additional guidance would be helpful?

3 Anti-money laundering

3.1 The first licensing objective requires licensees to keep gambling free from crime and from being associated with crime. Key to meeting this objective are effective controls to prevent gambling being used to launder money – whether that be concealment or conversion of criminal funds (washing), or simply the use of criminal funds for gambling, particularly where they contribute significantly to the bottom line or where theft etc has been committed to support a gambling habit. The Commission's engagement with the industry and the outcome of regulatory investigations has led us to consider how the industry might best improve its defences, and how the Commission might improve its existing regulatory tools for anti-money laundering to support good practice and to tackle poor practice more effectively.

3.2 Commission casework has shown that cases of crime involving gambling often highlight shortcomings in licensees' procedures. This is particularly true in cases relating to alleged money laundering offences in which the proceeds of crime are laundered or spent on gambling.

3.3 We therefore propose to introduce a number of new licence conditions and to make appropriate changes to others to make them more effective. We also seek views on a number of other proposals.

3.4 At the same time, we are taking this opportunity to seek views on a proposed new edition of our anti-money laundering guidance for non-remote and remote casino operators.

Assessing money laundering risk

3.5 We already expect licensees to manage regulatory risks, including money laundering risks, just as they manage their commercial risks. So, we expect them to manage their operations with regard to the risks posed to the licensing objectives in the Act, and to measure the effectiveness of the policies and procedures they have put in place to manage those risks. As part of this, licensees should manage any risks that their operations might be used for money laundering or terrorist financing in the same way that they manage all the risks to the licensing objectives.

3.6 In order to manage regulatory risks, including money laundering risks, licensees should have in place policies and procedures, and measure the effectiveness of these, just as they would for commercial risks. The starting point of any policy or procedure to manage and mitigate anti-money laundering risks is for licensees to have an effective assessment of what those risks are in relation to the licensee. This assessment will be relative to the size and scale of the licensee in question. We are mindful of additional burden particularly on smaller licensees, and are aware that they may need additional guidance, including potentially using or adapting standardised assessments of risk.

3.7 Further guidance about assessing risk is contained in our anti-money laundering guidance to casinos, which is also attached for consultation within this document at Appendix A. We are also currently amending the anti-money laundering information on our website where we also intend to provide more information that is useful for operators, including a section dealing with key AML risks.

3.8 Compliance and investigation activity undertaken by the Commission over recent years has demonstrated that there are weaknesses in the way that some operators assess their money laundering risks, and a failure to keep these assessments under regular review.

3.9 We therefore propose to introduce a licence condition that will require licensees to conduct, and regularly review, assessments of money laundering risks, and devise action plans to manage the identified risks. Licensees should use these assessments as a tool to manage money laundering risks for themselves. We would not expect licensees to submit assessments to us, except as part of normal compliance activity or when investigating cases.

Proposed new licence condition

All operating licences, except non-remote lottery, gaming machine technical and gambling software licences

1 Licensees must conduct an appropriate assessment of the risk of their business being used for money laundering. This risk assessment must be reviewed and revised as necessary at least annually in the light of any changes of circumstances including the introduction of new products or technology, new methods of payment by customers, changes in the customer demographic, or other material changes (including arrangements for master and sub customer accounts).

2 Following completion of the risk assessment, and any review of the assessment, licensees must devise an action plan to manage the risks, and mitigate them where possible. This action plan should include arrangements for licensees to submit suspicious activity reports to the National Crime Agency and to discontinue customer business relationships in appropriate circumstances.

3 A copy of the licensee's money laundering risk assessment and action plan must be provided to the Commission on demand.

Consultation questions

Q5. Do you agree that it should be a condition of an operator's licence that they undertake an assessment of money laundering risks?

Q6. If you are an operator, do you already undertake a money laundering risk assessment or would the proposed licence condition require significant additional work?

Q7. Do you have any comments on the draft addition of the licence condition requiring licensees to conduct and review money laundering risk assessments, and devise an action plan to mitigate the risks?

Due diligence checks on customers

3.10 In the same way that it is essential for licensees to assess money laundering risks in general, it is also critical that they determine the potential money laundering risks posed by individual customers, or categories of customer. This is particularly relevant where a licensee's initial assessment of a customer indicates that the customer presents a heightened money laundering risk.

3.11 In addition, where the licensee identifies that there is a heightened risk that a customer is using funds derived from his or others' criminal activity, it is vitally important to establish, as far as reasonably possible, that the customer is using legitimate funds in transactions with the licensee. Our guidance document, *The prevention of money laundering and combating the financing of terrorism – Guidance for remote and non-remote casinos* (3rd edition) (attached for consultation at Appendix A) provides further information on this area at paragraph 2.20).

3.12 Our compliance and investigation activity has demonstrated that licensees often do not make sufficient enquiries about the customers who transact with them and do not take adequate measures to establish the customer's source of funds. These are essential tools to prevent money laundering and to support the first licensing objective. We therefore propose to introduce a new licence condition requiring operators to take measures to identify and monitor customers who present a higher risk of money laundering.

Proposed new licence condition

All operating licences, except non-remote lottery, gaming machine technical and gambling software licences

1 Licensees must take reasonable steps, consistent with their assessment of the risk of their business being used for money laundering, to identify and monitor the gambling activities of customers who the licensee has identified present a heightened money laundering risk, and take appropriate steps to satisfy themselves that the funds used to finance the customer's transactions with the licensee are not the proceeds of crime.

Consultation questions

Q8. Do you agree that identifying customers is an important measure to manage heightened money laundering risks presented by specific customers?

Q9. Do you have any comments on the draft addition of the licence condition requiring licensees to identify customers where there is a heighted risk or money laundering and to satisfy themselves about the legitimacy of the customers' funds?

Customer monitoring across products and platforms

3.13 Commission casework has demonstrated that licensees have found it hard to recognise and link information relating to the same customer carrying out gambling activity in different parts of the business, such as across different gambling platforms, both remote and non-remote, and gambling products.

3.14 Although this is a challenging area, monitoring and linking information relating to customer activity across the entire business and linking the customer across platforms and products will provide the licensee with a more comprehensive picture of the money laundering risks to which it is exposed.

3.15 Despite the challenges we have seen good examples of licensees collecting information and sharing it not only within their own operations, but wider to other licensees. We encourage licensees to consider where they may be able to apply similar practices in their businesses.

Good practice example
There are further complications when a criminal spreads business between different operators, as this makes it harder for an individual licensee to detect untoward practices.

One licensee has written to other operators within the area to inform them when a customer relationship has been discontinued and the Commission has been alerted, in order to provide as much joined-up information as possible.

3.16 Licensees are already required to collect and analyse customer information to meet social responsibility obligations. Under social responsibility code provision 3.4.1 (Customer interaction), licensees are required to make use of all relevant sources of information to identify customers at risk of harm from gambling, including by reference to information related to time and money spent gambling. Social responsibility code provision 3.9.1 (Identification of individual customers) requires remote licence holders to have effective policies and procedures in place designed to identify separate accounts held by the same individual. It is a logical step to collect and use this information, much of which may be identical to that needed for social responsibility purposes, to support anti-money laundering policies.

3.17 We therefore propose to introduce a new ordinary code provision that will provide that operators monitor customers and their accounts across all outlets, platforms and products.

Proposed new ordinary code provision

All operating licences, except non-remote lottery, gaming machine technical and gambling software licences

1 In order to fully assess the money laundering risks to which they are exposed, licensees should take reasonable steps to monitor the gambling activity of customers and the accounts they hold (for example, by tracking and linking transactions) across the licensee's entire gambling portfolio.

Consultation questions

Q10. Do you agree that, in order to have a comprehensive picture of customer risk, it is necessary to monitor customers across all the operator's outlets, platforms and products?

Q11. Do you think that an ordinary code provision is necessary to address this need?

Other reportable events – discontinuing a business relationship with a customer as a result of money laundering concerns

3.18 There will be circumstances in which a licensee decides that a particular customer is either engaged in money laundering or that, by continuing the business relationship with the customer, there is a risk that the licensee will commit money laundering offences under the Proceeds of Crime Act 2002. The licensee may therefore decide to discontinue the business relationship with the customer. Non-remote and remote casino operators also have a statutory obligation to terminate any business relationship with a customer where they cannot complete customer due diligence measures in respect of that customer.

3.19 Information regarding customers with whom a licensee has discontinued a business relationship is useful to the Commission as it assists in developing a clearer understanding of money laundering threats and trends in the gambling industry, and in measuring the industry's commitment to the first licensing objective.

3.20 We therefore propose to require licensees to report on the number of cases where they discontinue a customer relationship having decided that there is a risk that the licensee will commit money laundering offences. This will entail an appropriate addition to Licence condition 15.2 (Reporting key events and other reportable events). We invite views on this proposed new licence condition.

Proposed new licence condition

Licence condition 15.2.3
Other reportable events
All operating licences, except non-remote lottery, gaming machine technical and gambling software licences

1 Licensees must notify the Commission in such form or manner as the Commission may from time to time specify, or ensure that the Commission is so notified, as soon as reasonably practicable of the number of instances where the licensee has discontinued a business relationship with a customer as a result of a decision by the licensee that there was a risk that money laundering offences might otherwise be committed.

Consultation questions

Q12. Do you have any comments on the proposal which will require operators to report on the number of customers where they have ended the business relationship due to money laundering concerns?

Q13. How far would such a requirement add to the regulatory burden on operators?

Anti-money laundering measures for operators based in foreign jurisdictions

3.21 Non-remote and remote casinos in Great Britain are required to comply with the Money Laundering Regulations 2007. This requires them to apply customer due diligence measures, provide anti-money laundering training to employees, keep records and appoint a nominated officer, among other things.

3.22 At the time that the Gambling (Licensing and Advertising) Act 2014 came into force, the Commission considered it necessary to attach an individual condition to the licences of remote casino operators who are licensed by the Commission but have remote gambling equipment located outside of Great Britain. This was to ensure that those licensees put in place the anti-money laundering measures articulated in the Money Laundering Regulations 2007. We have since attached this individual licence condition to all remote casino licences issued by the Commission in circumstances where the remote gambling equipment is based in a foreign jurisdiction.

3.23 We now propose to introduce formally a licence condition for remote casino licensees with remote gambling equipment located outside Great Britain. This will ensure consistency and transparency across all new licence applications.

Proposed new licence condition

All remote casino operating licences

1 Licensees must comply with Parts 2 and 3 of the Money Laundering Regulations 2007 (UK Statutory Instrument No. 2157 of 2007) as amended by the Money Laundering (Amendment) Regulations 2007 (UK Statutory Instrument No. 3299 of 2007), or the equivalent requirements of any UK Statutory Instrument by which those regulations are amended or superseded insofar as they relate to casinos (the MLR) whether or not the MLR otherwise apply to their business.

Consultation question

Q14. Do you have any comments on the draft new licence condition for remote casino operators who have remote gambling equipment located outside of Great Britain?

Cash and cash equivalents

3.24 One of the central regulatory tools available to the Commission to hold licensees to account for managing the risks of money laundering is licence condition 5.1.1, which relates to cash handling. Our extensive casework experience has demonstrated a clear theme of shortcomings in this area across a wide range of operators: across the industry, there are numerous incidents where licensees have failed to implement and monitor effectively their policies and procedures for handling cash and cash equivalents.

3.25 However, the condition as drafted has proved somewhat ineffective in terms of both encouraging robust defences on the part of the industry and providing fast, agile regulatory options for the Commission. A literal reading of the licence condition 5.1.1 suggests that a licensee would be in breach if it did not have policies and procedures in place for handling cash and equivalents, but not if those policies and procedures were ineffective or inappropriate. We therefore consider that the current wording does not provide us with the necessary tool to allow regulation of licensees in a fair, consistent and proportionate way. In particular, it may prevent us from imposing a financial penalty if we discover ineffective policies.

3.26 For example, in a recent case, although there were gross failures on the part of the licensee to implement its policies and procedures, we could not prove conclusively that it had breached the licence condition. This was because the licensee had policies in place, but these were not very effective.

3.27 We therefore propose to update this licence condition to remove the ambiguity and so that the intention of the condition is clearer. We have also taken the opportunity to correct a technical error with this licence condition and current licence condition 5.1.2 (Payment services).

Proposed amended licence conditions

5 Cash ~~handling~~ and cash equivalents, and payment methods and services

5.1 ~~Payment services~~ Cash and cash equivalents

Licence condition 5.1.1
Cash ~~handling~~ and cash equivalents
All operating licences except gaming machine technical and gambling software licences

1 Licensees, as part of their internal controls and financial accounting systems, must have and ~~put into effect~~ **implement** appropriate policies and procedures concerning the ~~handling~~ **usage** of cash, and cash equivalents (~~ie~~ **eg** bankers drafts, cheques and debit cards **and digital currencies**) **by customers,** designed to minimise the risk of crimes such as money laundering, to avoid the giving of illicit credit **to customers** and to provide assurance that ~~gambling activities are being conducted fairly~~ **gambling activities are being conducted in a manner which promotes the licensing objectives.**

5.2 Payment methods and services

Licence condition ~~5.1.2~~ 5.2.1
Payment methods and services
All remote casino, bingo and betting operating licences, except ancillary and remote betting intermediary (trading room only) licences

1 Licensees should only accept payment from customers using their gambling facilities in Great Britain by a method which involves the provision of payment services as defined in Schedule 1 Part 1 of the Payment Services Regulations 2009 (SI 2009 No 209)**, ~~if~~** if the provider of those services is a 'payment service provider' within the definition of that term in regulation 2 of those Regulations.

Consultation questions

Q15. Do you agree that licence condition 5.1.1 should apply to remote gambling operators and that it should be amended to make it clear that operators must have effective policies and procedures for the handling of both cash and cash equivalents?

Q16. Do you have any views on the licence condition as redrafted?

Linking means of payment of stake to payment of winnings

3.28 The financial and gambling markets are diverse and rapidly evolving. Against this background, the means by which customers pay for services and the manner in which they request operators to pay their winnings or return their deposits is of ever-increasing importance from the perspective of anti-money laundering. The Financial Action Task Force has identified new payment methods as a risk that all operators should consider.

3.29 The act of money laundering is normally characterised as involving three stages:

- **placement** of funds in the retail market or financial system
- **layering** – passing funds through different legitimate activities, usually by moving monies in and out of various accounts and using electronic fund transfers
- **integration** – assimilating funds with legitimate economic and financial activity.

While this is not a comprehensive model for all types of gambling, it usefully characterises the cycle of activity in which criminal money is given the appearance of being clean.

3.30 There is a risk that customers will place and layer criminal proceeds through gambling transactions. One way of mitigating this risk is to link the payout of winnings with the means by which a customer pays for gambling transactions. We acknowledge that this will not eliminate the risk, but returning winnings in the same form, eg, in cash or back to the same bank account, limits the opportunity for a money launderer to layer the proceeds of criminal activity.

Example
Money launderers may hold cash derived from criminal activity that they want to move to a particular bank account as part of the money laundering cycle. They may use the cash to bet on an event with a high likelihood of success, but with a potentially low return.

If the winnings are then paid to the particular bank account that they have selected, they will have effectively placed and layered the transactions through one relatively low risk transaction.

3.31 We are interested in views on managing risk in this area. This might include introducing a licence condition requiring operators to link the means by which a customer pays for a gambling service to the means by which any winnings or refunded deposits are paid out to the customer. The condition could also require licensees to have controls in place to manage the risk of money laundering where it is not feasible to return funds to the source or in the same form. There may also be other ways of managing the risks, and we welcome your opinions.

Consultation questions

Q17. Do you have any views whether we should introduce a licence condition to cover this risk, and what it should contain?

Q18. Do you think that this requirement should be limited to cash stakes only?

Q19. Do you have any other views on how to manage risk in this area?

Current ordinary code provisions for anti-money laundering

3.32 The current ordinary code provisions that address anti-money laundering in the LCCP are as follows:

Ordinary code provision 2.1.1
Anti-money laundering - casino
All remote and non-remote casino licences

1 In order to help prevent activities related to money laundering and terrorist financing, licensees should act in accordance with the Commission's guidance on anti-money laundering, *The Prevention of Money Laundering and Combating the Financing of Terrorism - Guidance for remote and non-remote casinos*.

Ordinary code provision 2.1.2
Anti-money laundering – other than casino
All licences except casino licences

1 As part of their procedures for compliance with the requirements in respect of the prevention and detection of money laundering in the Proceeds of Crime Act 2002 and the Terrorism Act 2000, licensees should take into account the Commission's advice on the Proceeds of Crime Act 2002, *Duties and responsibilities under the Proceeds of Crime Act 2002 - Advice for operators (excluding casino operators).*

3.33 These ordinary code provisions encourage operators to adopt a risk-based approach to managing money laundering risks. The documents to which the code provisions refer contain a mixture of legal requirements and best and good practice in preventing money laundering.

3.34 The Commission is not proposing to revise these ordinary code provisions at this stage, although amendments may be later required depending on the outcomes of this consultation. We are nonetheless seeking views on whether to change the status of these ordinary code provisions, with appropriate adjustments to wording, to make them licence conditions, which are mandatory.

Consultation question

Q20. Do you have any views on whether the Commission should change the status of these ordinary code provisions to make them licence conditions, requiring all operators to comply with the anti-money laundering guidance or advice issued by the Commission?

Revised guidance for non-remote and remote casinos on preventing money laundering and combating the financing of terrorism

3.35 The Commission is the supervisory authority for casinos in terms of the Money Laundering Regulations 2007 (the Regulations). Amongst other things, this means that the Commission should publish guidance to casinos on anti-money laundering.

3.36 We published the first edition of this guidance in December 2007 to coincide with the Money Laundering Regulations 2007 coming into effect. The second edition was published in December 2011 (and underwent some subsequent minor revisions). HM Treasury requires all supervisory authorities to review regularly the anti-money laundering guidance that they issue to the businesses that they supervise.

3.37 In order to help prevent activities related to money laundering and terrorist financing, ordinary code provisions 2.1.1 and 2.1.2 provide that remote and non-remote casino licensees should act in accordance with our guidance on anti-money laundering, *The Prevention of Money Laundering and Combating the Financing of Terrorism - Guidance for remote and non-remote casinos*.

3.38 We propose to publish a third edition of the guidance on *The Prevention of Money Laundering and Combating the Financing of Terrorism* for remote and non-remote casinos. The purpose of this edition is to:

- incorporate learning from our anti-money laundering case work
- provide new guidance and update existing guidance in critical areas identified in our compliance and investigation activity
- update references to the Serious Organised Crime Agency (SOCA) to the National Crime Agency (the NCA), its successor
- meet the requirements of HM Treasury to review regularly any guidance issued.

3.39 We have also reviewed the guidance in support of the proposals contained in the *anti-money laundering* chapter of this consultation document. We intend that licensees will use the updated guidance in conjunction with any anti-money laundering licence conditions that we may introduce as a result of the consultation. If we do not adopt the changes after the consultation, then the guidance will remain in use as part of the code.

3.40 We intend this edition to be the final edition of the guidance before the EU 4th Money Laundering Directive is transposed into UK legislation. We expect that new regulations will come into force in mid 2017, at which time we will need to publish new or updated guidance for gambling operators.

3.41 *Appendix A* is the proposed third edition of the guidance with the changes from the second edition marked up for ease of reference. We seek your comments on the proposed changes.

3.42 We do not propose to update our advice on the Proceeds of Crime Act 2002, *Duties and responsibilities under the Proceeds of Crime Act 2002 - Advice for operators (excluding casino operators)* at this time, as this was last revised in September 2014.

Consultation questions

Q21. Do you have any comments on the revised sections of the guidance document?

Q22. Do you have any comments on the new sections of the guidance document?

Q23. Are there any other areas which you think should be covered in the guidance?

4 Responsible placing of digital adverts

4.1 The UK's creative industries, which includes the film, television and music industries, are now worth £76.9 billion per year to the UK economy[5]. However, in recent years these industries have come under increased threat from the piracy of their copyrighted works online. Some websites are promoting and engaging in illegal activity and making significant financial gain by placing adverts for well-known brands.

4.2 A 2014 report by the Digital Citizens Alliance[6] estimated that in 2013, piracy websites generated $227 million from advertising. Brands that advertise on these sites risk funding online criminals and providing seed money for other illegal activity. Disrupting the money unlawful websites make from advertising is therefore critical in tackling online criminal activity.

4.3 Operation Creative is a multi-agency initiative designed to disrupt and prevent websites from providing unauthorised access to copyrighted content. The initiative is led by the City of London's Police Intellectual Property Crime Unit (PIPCU) in partnership with the creative and advertising industries, including the Federation Against Copyright Theft (FACT) and the British Recorded Music Industry Ltd (BPI).

4.4 Operation Creative hosts an Infringing Website List (IWL), which is verified by the City of London Police. Access to the IWL enables advertisers to take action to ensure that their brand does not appear on sites contained in the list.

4.5 We are aware from work undertaken by Operation Creative that adverts for mainstream, licensed gambling operators are appearing on these sites. Therefore, it appears that some licensees are inadvertently providing a source of revenue for online crime.

4.6 We are committed to supporting Operation Creative. During the period March to June 2015 our involvement in brokering contact between PIPCU and Marketing PML holders has resulted in a 36% decrease in adverts from licensed gambling operators appearing on the IWL. However, a significant number of adverts still appear.

4.7 A gambling industry brand advert appearing on a website under police investigation for criminal copyright infringement could lead to significant reputational risk for both the licensee in question and for the Commission. It also risks legitimising illegal sites that undermine the creative industries and that can harm the consumer (via risk of malware, etc).

4.8 Social Responsibility code provisions 1.1.2 and 1.1.3 (Responsibility for third parties) do require licensees to take responsibility for third parties with whom they contract. Despite this, we continue to see adverts appearing on illicit websites, and it remains a significant issue. The existing conditions do not refer to this specific area. Given the ongoing problem, we are concerned that the existing conditions may not give sufficient prominence to this issue, and that we may need additional conditions in order to address it.

4.9 Our work with Operation Creative is reactive. The progress we have achieved is through Operation Creative partners identifying the offending adverts, following which the Commission brokers contact with the licensee concerned. However, this reactive approach is not sustainable long term, and nor should it be. We believe it is very important to move from our current law enforcement and regulator-led approach to a more proactive approach led by licensees.

4.10 We would expect licensees to take more responsibility for ensuring that adverts placed by themselves or others do not appear on illegal websites in the first instance. Ideally, they could do this by using commercial content verification software and by requiring their affiliates or other contractors to do the same.

[5] Creative Industries worth £8.8 million an hour to UK economy
[6] Digital Thieves and the Hijacking of the Online Ad Business

4.11 We are therefore seeking views on the following questions:

Consultation questions

Q24. What are your views on introducing a requirement, potentially via a Social Responsibility code provision, for licensees to take all reasonable measures to ensure that digital adverts placed by themselves, or third parties, do not appear on copyright infringing websites?

Q25.What are your views on introducing an ordinary code provision on measures licensees should consider taking to prevent adverts appearing on illegal sites, such as the use of commercial content verification software?

Q26. What other steps or measures do you think could be considered?

5 Misuse of insider information by industry personnel

5.1 There is potential for a conflict of interest if a licensee's employees, particularly if employed in the trading function, encounter information that might indicate suspicious betting activity. This conflict of interest may arise if an employee sees an emerging suspicious trend in betting markets, and uses this information to place bets in their own interest.

5.2 The betting integrity regulatory system relies on operators reporting information about suspicious betting patterns to the Commission and the relevant Sports Governing Body (SGB) under LCCP licence condition 15.1.2 (Betting licences). If, instead of, or in addition to making such a report, an individual chooses to use that information in their own interests by placing bets, the LCCP system, and confidence in it, may be undermined. Regardless of whether they have also made a report, an employee should not use such information for personal gain.

5.3 We recognise that people employed in the betting industry often have a deep interest in betting; indeed, that is the source of much of their value as employees. We know that it is custom and practice in the industry for traders to place their own wagers with rival operators in furthering that interest. However, licensees may be at risk of accepting bets based on advantageous commercial intelligence that is in the possession of employees of other operators.

5.4 We consider that these risks can be mitigated by two measures. These build on the 2010 Report of the Sports Betting Integrity panel (also known as the Parry recommendation),[7] 1.11, which called on operators to "*vary betting terms and conditions to make the contravention of sports or other professional or employer rules on betting a breach of the operator's own [betting] terms and conditions".* The ABB circulated a model condition in this area in 2010, but unfortunately that condition did not extend beyond sports rules (ie, did not cover professional or employer rules). This is an important opportunity to fill this gap.

5.5 To underpin the effectiveness of the Parry recommendation, we also recommend that betting operators provide mutual assurance among themselves that effective employment terms and conditions are in place, requiring employees to act primarily in the interests of their employers.

5.6 We have previously recommended these measures to a number of trade bodies in the gambling industry. We now propose to include these measures as ordinary code provisions in the LCCP as a way for the industry to address this vulnerability both to the licensing objectives and to its own commercial interests.

Proposed new ordinary code provision 7.2.1
Gambling staff
All betting operating licences

1. Licensees should have employment terms and conditions that:

- **Require employees to report any indicators of suspicious betting to their employer; and**
- **Prohibit their employees from using information related to suspicious betting for the purpose of placing their own wagers, either with their employer or with other operators.**

[7] Report of the Sports Betting Integrity Panel

Proposed new ordinary code provision 7.2.2
Gambling staff
All betting operating licences

1. Licensees should ensure that a condition of their accepting bets is that customers are not in breach of any rules about betting from a sports governing body, other professional body of which they are a member, or their employers.

Consultation questions

Q27. What are your views on the introduction of new ordinary code provisions advising betting operators that they should put in place new employment terms and conditions to require employees to report indicators of suspicious betting and impose restrictions?

Q28. What are your views on the introduction of a new ordinary code provision to advise betting operators that they should include a clause to state that breaches of sports or other rules will also constitute a breach of the operator's customer betting terms and conditions?

6 Digital currencies (often referred to as virtual currencies or cryptocurrencies eg, Bitcoin)

Background

6. 1 In this consultation, we have adopted a definition of digital currencies similar to that set out by HM Treasury in their 2014 Call for information[8] and subsequent response. A digital currency scheme incorporates both a 'decentralised payment system and a related currency where transactions achieve consensus through a variety of means such as proof-of-work'[9]. They are often referred to as virtual currencies, cryptocurrencies and electronic money (e-money)

6. 2 Digital currencies (eg, Bitcoin, a peer-to-peer payment system introduced in 2009) have been subject to increasing public, industry and government interest over the past twelve months. This increased interest, and a number of misconceptions about digital currencies, has driven further consideration of their use within the domestic and international economy, how they might be regulated, and whether they could be associated with crime.

6.3 In the UK, the regulatory position of digital currencies continues to evolve. In 2015, HM Treasury's response[10] to the previously mentioned 'call for information' set out a series of measures that will apply a degree of regulation to the digital currencies industry. As these measures will take time to implement, the interim position encourages the digital currency industry to self regulate. The Bank of England, European Central Bank and the Financial Action Task Force (FATF) have also published their analyses of digital currencies.

6.4 There appears to be strong interest in using digital currencies as a means of payment within the gambling industry across the world. At the time of writing no licensees have reported to us that they allow the use of digital currencies in gambling. We have, however, received a number of enquiries regarding use of digital currencies (in particular, Bitcoin).

6.5 Currently, adoption of digital currencies for the purchase of goods and services remains small in comparison to other means of payments. There is little evidence of digital currencies being used for money laundering/terrorist financing.

The Commission's view

6.6 We are aware that there have been misconceptions about digital currencies, and whether their use constitutes gambling. We view digital currencies under the Gambling Act 2005 as 'money or money's worth', and therefore their use in gambling does constitute real money gambling. Any operator wishing to offer gambling facilities[11] to consumers in Great Britain, including use of digital currencies for real money gambling, must hold an Operating Licence obtained from us. Licensees are also currently required to inform the Commission of any use of digital currencies as covered by the current LCCP licence condition 15.2.1 section 17 (Reporting key events). In addition, in this consultation we also propose to introduce a new licence condition requiring licensees to conduct an effective assessment of the risk or their business being used for money laundering, including new methods of payments by customers (see paragraphs 3.5-3.8).

6.7 All licensed operators, whether using digital currencies or not, have a responsibility to keep crime, including money laundering, out of gambling. Additionally, casino operators must also comply with the Money Laundering Regulations 2007. The Commission also expects all operators to comply with the Commission's *Licence Conditions and Codes of Practice (LCCP),* and the Commission's guidance and advice on anti-money laundering.

[8] Digital currencies call for information
[9] Put simply, proof-of-work is when a piece of data must satisfy certain requirements before it is able to produce the final 'product'.
[10] Digital currencies response to call for information
[11] As specified under the Gambling Act 2005.

6.8 Digital currencies therefore fall within the Commission's current Anti-Money Laundering (AML) framework. Operators must satisfy themselves and the Commission that they have effective policies and procedures in place to mitigate any AML risks including those associated with digital currencies.

6.9 This means that any licensee wishing to use digital currencies as a means of payment for gambling must be able to apply and take appropriate action regarding their Know Your Customer (KYC) policies, source of funds and any additional risks associated with this form of payment to their transactions.

6.10 Any operators using a payment intermediary such as a Bitcoin exchange and/or payment services provider may need to take additional steps to ensure the funds came from a legitimate source, regardless of the currency used as a means of payment or means to gamble.

Challenges with digital currencies

6. 11 There are a number of challenges around the use of digital currencies, some of which may make them attractive to illicit use. For example:

- There is increasing scope to use digital currencies, which, coupled with some of the misconceptions surrounding them, eg, whether their use does constitute gambling, may increase the challenges if gambling operators do not fully understand them
- The degree of anonymity associated with digital currencies may be attractive to individuals who want to conceal their identity and the source of their funds[12]
- Coupled with other tools[13] to conceal identity, the ownership and source of funds can be effectively concealed from law enforcement or operator enquiries
- There is an absence of specific AML regulation surrounding digital currencies in the UK at present[14]
- The decentralised nature of digital currencies means there is no central authority that supports its value and can assist law enforcement
- Digital currencies such as Bitcoin have had a history of large price fluctuations. Operators would need to appropriately consider and mitigate against any risk to their financial security following possible currency fluctuations as well as being open with players as to those risks.

6.12 A licensee's policies to mitigate against the risk of money laundering would require them to put in place KYC requirements and be satisfied that a customer is not using the proceeds of crime. Given that this is likely to be more challenging with digital currencies, it begs the question why a licensee would wish to allow their use, and how they may overcome the AML challenges associated with them.

6.13 We recognise that there may be potential benefits in using digital currencies, not least the potential for reduced payment costs. However, our evidence about licensee compliance with the current AML framework presents concerns about how well licensees will be able to implement effective AML controls to manage risks associated with digital currencies.

6.14 We therefore ask for your views on any benefits of using digital currency within the British gambling industry, on the challenges that we have described, and on potential means of mitigating those.

[12] The Commission is aware that digital currencies could be considered 'pseudonymous' as transactions are recorded on a public ledger.
[13] For example, Virtual Private Networks (VPNs) and the Onion Router.
[14] Implementing regulation of digital currency exchanges will take time therefore present use of digital currencies is unregulated.

Consultation questions

Q29. Looking at the challenges in the use of digital currencies listed above, do you see any omissions or oversights? What are your views on the validity of those challenges?

Q30. How might these and any other challenges that you have identified, especially those associated with AML, be mitigated?

Q31. Given the potential difficulty in identifying customers and managing AML risks, what would be the potential benefits in the use of digital currencies compared to the extra compliance work involved?

Q32. Do you see the business drivers to use digital currencies increasing or diminishing, and to what extent?

Q33. What additional AML measures might be needed when accepting deposits from a payment intermediary where their source is digital currencies?

7 Areas of future and ongoing work

7.1 This consultation covers the amendments that the Commission is proposing for implementation in 2016. As already noted, some areas included are intended to stimulate debate on wider issues, where work is ongoing. As a result, responses to some areas in this consultation may lead to further consultation as we take note of your input.

7.2 The Commission is also currently developing some other areas of work, linked to preventing crime in gambling, but not included in this consultation. These are:

- An assessment of whether the current controls for peer to peer poker contained in the Remote Gambling and Software Technical Standards are effective enough at minimising risks to the licensing objectives. We are currently gathering further evidence to assess the need for improvements and ensure any new requirements both provide the required level of information to consumers and deter would-be cheaters. The information we collect from operators will be used to identify common themes or areas requiring improvement. We expect to complete this work by the end of 2015.
- An assessment of our regulatory tools against the Council of Europe Convention on the Manipulation of Sports Competitions[15] (the Convention). The Convention is the first legally binding international tool to fight match fixing. It aims to detect and punish the manipulation of sports competitions and to support cooperation between public authorities, sports organisations and sports betting operators. The UK has not yet signed up to the Convention, and the process of ratification is still ongoing. However the Commission intends to review how the articles in the Convention relate to the current regulatory framework, and whether improvements are required to the latter. This work will commence within the next six months.

[15] Council of Europe Convention on the Manipulation of Sports Competitions

8 Responding to this consultation

8.1 The Commission is committed to full and open consultation and we welcome comments on any aspect of this document. A response template is available on our website. The Commission would prefer respondents to complete the response template provided and send it by email to: consultation@gamblingcommission.gov.uk

8.2 Alternatively, responses can be sent by post to:
Consultation
Gambling Commission
Victoria Square House
Victoria Square
Birmingham
B2 4BP

8.3 The deadline for responses to this paper is **end of day 30 December 2015**. Respondents are of course welcome to comment on only one or some of the topics addressed by this consultation.

8.4 When responding, please state whether you are responding as an individual or representing the views of an organisation. If responding on behalf of an organisation, please make clear who that organisation represents. If responding as an individual, please mention your own interest.

8.5 Please note that responses may be made public or published in a summary of responses to the consultation unless you state clearly that you wish your response or name to be treated confidentially. Confidential responses will be included in any statistical summary of numbers of comments received. If you are replying by email or via the website, unless you specifically include a request to the contrary in the main text of your submission, the Commission will assume your consent overrides any confidentiality disclaimer that is generated by your organisation's IT system.

8.6 Any information or material sent to us and which we record may be subject to the Freedom of Information Act 2000 (FOIA). The Commission's policy on release of information is available on request or by reference to our website at www.gamblingcommission.gov.uk. The Commission will treat information marked confidential accordingly and will only disclose that information to people outside the Commission where it is necessary to do so in order to carry out the Commission's functions or where the Commission is required by law to disclose the information. As a public authority the Commission must comply with the requirements of FOIA and must consider requests for information made under the Act on a case-by-case basis. Therefore when providing information, if you think that certain information may be exempt from disclosure under FOIA, please annotate the response accordingly so that we may take your comments into account.

8.7 All information provided to the Commission will be processed in accordance with the Data Protection Act 1998. However, it may be disclosed to government departments or agencies, local authorities and other bodies when it is necessary to do so in order to carry out the functions of the Commission and where the Commission is legally required to do so.

GAMBLING COMMISSION

Appendix A

The prevention of money laundering and combating the financing of terrorism

Guidance for remote and non-remote casinos

Third edition

Consultation
September 2015

This document contains proposed amendments to *The prevention of money laundering and combating the financing of terrorism: Guidance for remote and non-remote casinos*.

Please see the *Licence conditions and codes of practice* consultation document published alongside this draft guidance document to see an explanation for the proposed amendments, and for information on how to respond to the consultation.

Proposed additions to the text of the document are marked in **black and bold**, and proposed deletions are marked in ~~strikethrough~~.

Contents

Figures

Annex A – Glossary of terms

Part 1 – Summary of the guidance

Principles to be followed

i All casinos (both premises based and remote) must have appropriate systems and processes to ~~forestall and~~ prevent money laundering and terrorist financing. To achieve this they should:

- develop systems and controls that are appropriate for their businesses;
- adopt a risk-based approach that is flexible, effective, proportionate and cost-effective;
- have full commitment from, and responsibility resting with, senior management;
- regularly assess the adequacy of their systems and controls;
- maintain, where necessary, records of customers and transactions that meet the needs of law enforcement investigations tackling money laundering and terrorist financing;
- provide initial and ongoing training for all relevant employees;
- support their nominated officers with resources and authority to operate objectively and independently;
- engage with law enforcement bodies and the Gambling Commission (the Commission) **in relation to** ~~by reporting~~ suspicious activity; and
- participate in feedback and best practice forums.

Risk-based approach

ii The Money Laundering Regulations ~~2007~~ (the Regulations)[16] require operators to have a policy and procedure in relation to risk assessment and management. The risk-based approach involves a number of discrete steps in assessing the most proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the operator. These steps require the operator to:

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

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

iv The risk-based approach is discussed in section 2 of this guidance.

Senior management responsibility

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

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

[16] The Money Laundering Regulations 2007

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

- customer due diligence (CDD) measures and ongoing monitoring;
- reporting;
- record keeping;
- internal control;
- risk assessment and management;
- training; and
- the monitoring and management of compliance with, and the internal communication of, such policies and procedures.

viii Senior management responsibility is discussed in section **4**~~3~~ of this guidance.

Nominated officer

ix Nominated officers have responsibility for:

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

x They must have the authority to act independently in carrying out their responsibilities, and have access to sufficient resources to carry out their duties.

xi Casinos must have contingency arrangements in place for circumstances where no nominated officer is in post, for example, if on annual leave, long-term sick leave or if the nominated officer leaves the employ of the casino.

xii The responsibilities of the nominated officer are discussed in section **5**~~4~~ of this guidance.

Casino employees

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

xiv Employees must follow casino policies and procedures for:

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

xv The duties of casino employees are discussed throughout sections ~~4, 5, 6 and 7~~ **5, 6, 7 and 8** of this guidance.

Customer due diligence

xvi A key requirement in the Regulations is the requirement to make checks on customers - CDD. Casino operators can use one of two approaches; identifying and verifying the identity of all customers on entry to the casino's licensed premises (the on entry approach) or undertaking identification and verification when a customer approaches the threshold set out in the Regulations (the threshold approach).

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

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

xix **CDD** ~~Customer due diligence~~ is discussed in section ~~5~~**6** of this guidance.

Record keeping

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

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

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

xxii Record keeping is discussed in section **7**~~6~~ of this guidance.

Suspicious activity reports

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

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

that a person is engaged in money laundering or terrorist financing.

xxiv Operators must ensure that any employee reports to the nominated officer where they have grounds for knowledge or suspicion that a person or customer is engaged in money laundering or terrorist financing. The operator's nominated officer must consider each report, and determine whether it gives grounds for knowledge or suspicion.

xxv If the nominated officer determines that a report does give rise to grounds for knowledge or suspicion, he must report the matter to the **NCA** ~~SOCA~~. Under POCA, the nominated officer is required to make a report to the **NCA** ~~SOCA~~ as soon as is practicable if he has grounds for suspicion that another person, whether or not a customer, is engaged in money laundering. Under the Terrorism Act, similar conditions apply in relation to disclosure where there are grounds for suspicion of terrorist financing.

xxvi Suspicious activities and reporting requirements are discussed in section **8**~~7~~ of this guidance.

Offences

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

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

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

xxx The offences are discussed in section **8**~~7~~ of this guidance.

Part 2 – The guidance

1 Introduction

1.1 The law concerning money laundering is based on the general and wide ranging prevention and detection of the use of any proceeds of crime, the prevention and detection of terrorist financing, and for some businesses (including casinos) the more specific requirements of the business and its employees to have policies and procedures in place covering the risks it faces from money laundering.

~~1.2 Money laundering is a term that is often misunderstood. It is defined in section 340 of POCA and covers wide ranging circumstances involving any activity concerning the proceeds of any crime. This includes:~~

~~a) trying to turn money raised through criminal activity into 'clean' money (that is, classic money laundering);~~
~~b) possessing or transferring the benefit of acquisitive crimes such as theft and fraud, and funds generated from crimes like tax evasion;~~
~~c) possessing or transferring stolen goods;~~
~~d) being directly involved with any criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property; and~~
~~e) criminals investing the proceeds of their crimes in the whole range of financial products.~~

1.2~~3~~ Using money in casinos, regardless of the amount, that is the proceeds of any crime can amount to money laundering if the person using or taking the money knows or suspects that it is the proceeds of crime. Money laundering offences can be committed by both the customer and casino employees, depending on respective levels of knowledge or suspicion.

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

1.3 **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.**

1.4~~2~~ **Money laundering is a term that is often misunderstood. It is defined in section 340 of POCA[17] and covers wide ranging circumstances involving any activity concerning the proceeds of any crime. This includes:**

- **trying to turn money raised through criminal activity into 'clean' money (that is, classic money laundering);**
- **possessing or transferring the benefit of acquisitive crimes such as theft and fraud, and funds generated from crimes like tax evasion (this includes the possession by an offender of the proceeds of his own criminal activity);**
- **possessing or transferring stolen goods;**
- **being directly involved with any criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property; and**
- **criminals investing the proceeds of their crimes in the whole range of financial products.**

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

- **placement**
- **layering**
- **integration.**

[17] Section 340 of POCA

1.6 **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.**

1.7 **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.**

1.8 **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 or obtained.**

1.9 **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 always easy to determine. Although the remote gambling industry might appear less vulnerable as electronic transfers are required for placements, identify theft and identify fraud can enable the money launderer to move criminal proceeds with anonymity. Furthermore, the use of multiple internet transactions can facilitate the layering stage of money laundering.**

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

Legal background

~~**1.4** The Regulations came into effect on 15 December 2007 and replaced the Money Laundering Regulations 2003 (the 2003 Regulations). Both remote and non-remote casinos licensed by the Commission are covered by the Regulations.~~

The FATF Recommendations and EU Directive

~~**1.5** The Regulations are generated from the Third European Union Directive (2005) that was adopted in October 2005. This directive represents Europe's ongoing commitment to tackle the international problem of money laundering and terrorist financing by implementing the global standards produced by the Financial Action Task Force (FATF) in 2003.~~

~~**1.6** The FATF recommendations that set the global standards single out the business sectors where there are believed to be the highest risks of money laundering and terrorist financing. This includes remote and non-remote casinos~~.

1.11 **The Financial Action Task Force (FATF), which is an international intergovernmental body, issues recommendations on AML and CTF. The recommendations set out a framework of measures which member countries should implement in order to combat money laundering and terrorist financing. They are endorsed by over 180 countries and are recognised as the international standard for AML/CTF.**

1.12 **The FATF Recommendations[18] set out the essential measures that countries should have in place to:**

- **identify the risks, develop policies and provide domestic coordination**
- **pursue money laundering, terrorist financing and the financing of proliferation**
- **apply preventative measures for the financial and other designated sectors**
- **establish powers and responsibilities for competent authorities and implement other institutional measures**
- **enhance the transparency and availability of beneficial ownership information of legal persons and arrangements**
- **facilitate international cooperation.**

1.13 **The European Union (EU) is an economic and political union of member states which are located primarily in Europe. The EU operates through a system of supranational independent institutions and intergovernmental decisions negotiated by the EU member states.**

1.14 **The Fourth EU Anti-Money Laundering Directive (the EU Directive)[19] sets out a framework which is designed to protect the European financial system against the risks of money laundering and terrorist financing and is, to a large extent, based on the international standards adopted by FATF. It requires EU member states to prohibit money laundering and to oblige the financial sector, comprising credit institutions and a wide range of other financial institutions (including casinos), to identify their customers, keep appropriate records, establish internal procedures to train staff and guard against money laundering, and to report any indications of money laundering to the competent authorities.**

The Proceeds of Crime Act

1.15~~7~~ Criminal offences of money laundering were first introduced in the United Kingdom (UK) 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 include any dealing in 'criminal property', which is defined widely as the proceeds of any type of crime, however small the amount. ~~POCA created three principal offences that between them criminalise any involvement in the proceeds of any crime if the person knows or suspects that the property is the proceeds of crime.~~[20]

1.16 **POCA establishes a number of money laundering offences including:**

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

1.17~~8~~ **The principal offences criminalise any involvement in the proceeds of any crime if the person knows or suspects that the property is criminal property.[21] 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.**

[18] The latest Recommendations
[19] Directive (EU) 2015/849
[20] ~~Sections 327, 328 and 329 of POCA.~~
[21] Sections 327, 328 and 329 of POCA.

1.18 **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.

1.19 **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.**

1.20 **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.

1.21 The~~se~~ **principal money laundering offences** are wide ~~offences that~~ **and** can be committed by any person, including a casino employee, who has actual knowledge or suspicion that a customer is using the proceeds of crime, or has possession of the proceeds of criminal activity.

1.22 **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.[22]**

1.23 **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.[23]**

---

[22] Section 327(2A) of POCA

[23] Operators should note that, following the decision in relation to *R v Anwoir* [2008] 2 Cr. App. R. 36, the Courts no longer need to *prove* that the criminal property derives from specific criminal conduct, but can instead rely on *the circumstances in which the property was handled*, from which an "irresistible inference" can be drawn that the property could only be derived from crime.

1.24 **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.**[24]

The Terrorism Act

1.25 **The Terrorism Act 2000 establishes several offences about engaging in or facilitating terrorism, as well as raising or possessing funds for terrorist purposes. It establishes a list of proscribed organisations that are believed to be involved in terrorism. In December 2007, tipping off offences and defences to the principal terrorist property offences were introduced.**

1.269 **The Terrorism Act applies to all persons and includes** ~~Specific~~ obligations to report suspected terrorist financing ~~were included in the Terrorism Act, as amended by the Anti Terrorism Crime and Security Act 2001. This legislation creates criminal offences, most of which can be committed by anyone in the UK~~. ~~Some of t~~**The** offences **of failing to disclose and tipping off** are specific to people working in firms covered by the Regulations, and who are therefore in the regulated sector, which includes casinos.

The Money Laundering Regulations

1.27 **The Regulations are generated from and implement the EU Directive.**[25] **They set requirements for the AML regime within the regulated sector and outline the scope of CDD, in particular. The Regulations cover a range of businesses and professions, including remote and non-remote casinos licensed by the Commission.**

1.28 **The Regulations impose additional requirements on the regulated sector. These include written policies and procedures, CDD, record keeping and training.**

1.2910 ~~The Regulations cover a range of businesses and professions, including remote and non-remote casinos licensed by the Commission~~. This guidance sets out how casino operators can and must comply with the law **governing money laundering**, ~~which at times is complex and demanding~~. The law places responsibilities on the Commission as the supervisory authority for casinos. The Commission should produce guidance that helps casino operators to meet the requirements of the law, is workable in the remote and non-remote casino environments and is approved by HM Treasury. This guidance, **therefore,** covers the full requirements of the UK law as it affects casinos.

~~**1.11** The purpose of this guidance is to:~~

- ~~outline the legal framework for AML and CTF requirements and systems across the remote and non-remote casino sector;~~
- ~~summarise the requirements of the relevant law and regulations, and how they may be implemented in practice;~~
- ~~indicate good industry practice in AML/CTF procedures through a proportionate risk-based approach;~~
- ~~assist operators to design and implement the policies and procedures necessary to mitigate the risks of being used in connection with money laundering and the financing of terrorism.~~

[24] Section 304 of POCA

[25] The current regulations (the Money Laundering Regulations 2007) came into effect on 15 December 2007 and implement the 3rd EU Anti-Money Laundering Directive. New regulations which will implement the 4th EU Anti-Money Laundering Directive are likely to come into effect by June 2017.

~~1.12 This guidance sets out what will be expected of casino operators and their employees in relation to the prevention of money laundering and terrorist financing, but allows them some discretion as to how they apply the requirements of the AML/CTF regime in the particular circumstances of their business.~~

~~1.13 This guidance will be of direct relevance to senior management and nominated officers in remote and non-remote casinos.~~

The role of gambling operators

1.30 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.

1.31 As described in the preceding paragraphs, 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).**

1.32 Operators should report instances of money laundering or attempts by customers to launder money to 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.

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

The role of the Commission

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

1.35 Under the Regulations[26], the Commission is designated as the supervisory authority for casinos. The Regulations[27] stipulate that a supervisory authority must:

- **effectively monitor the relevant persons for whom it is the supervisory authority and take necessary measures for the purpose of securing compliance by such persons with the requirements of the Regulations**
- **inform the NCA of instances where, in the course of carrying out its functions under the Regulations, it knows or suspects that a person is or has engaged in money laundering or terrorist financing.**

[26] Paragraph 23(1)(e)
[27] Paragraph 24(1)

1.36 **The Commission adopts a risk-based approach to its role and we, therefore, focus our 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, the Regulations and the Terrorism Act, 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.**

1.37 **Where operators fail to uphold the licensing objectives, for example by being ineffective in applying AML/CTF controls or ignoring their responsibilities under POCA, the Regulations and the Terrorism Act, 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.**

Purpose of the guidance

1.38 **All gambling operators have a responsibility to keep financial crime out of gambling. 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.**

1.39 **The purpose of this guidance is to:**

- **outline the legal framework for AML and CTF requirements and systems across the remote and non-remote casino sector;**
- **summarise the requirements of the relevant law and regulations, and how they may be implemented in practice;**
- **indicate good industry practice in AML/CTF procedures through a proportionate risk-based approach;**
- **assist operators to design and implement the policies and procedures necessary to mitigate the risks of being used in connection with money laundering and the financing of terrorism.**

1.40 **This guidance sets out what will be expected of casino operators and their employees in relation to the prevention of money laundering and terrorist financing, but allows them some discretion as to how they apply the requirements of the AML/CTF regime in the particular circumstances of their business. It will be of direct relevance to senior management and nominated officers in remote and non-remote casinos.**

1.41 **While the guidance focuses primarily on the relationship between operators and their customers, and the money laundering risks presented by transactions with customers, operators should also give due consideration to the money laundering risks posed by their business-to-business relationships, including any third parties they contract with.**

How should the guidance be used?

1.42~~14~~ The purpose is to give guidance to those who set operators' risk management policies and procedures for preventing money laundering and terrorist financing. This guidance aims to assist operators with detail about how to comply with the Regulations and the wider legal requirements, and is intended to allow operators flexibility as to how they comply. Operators will need to establish ~~their own,~~ more detailed and more specific internal arrangements directed by senior management and nominated officers to reflect the risk profile of their business.

~~1.15 When provisions of the statutory requirements or the Commission's regulatory requirements are directly described in the text of the guidance and are obligatory, the guidance uses the term 'must', indicating that these provisions are mandatory. Where the guidance is merely advisory, the term 'should' is adopted. References to 'must' and 'should' in the text should therefore be construed accordingly.~~

1.43~~16~~ This guidance is not intended to be a substitute for legal advice or operators' individual risk management plans. Operators should refer to the Regulations and associated legislation in making decisions in relation to the Regulations.

Content of the guidance

1.44 **In this guidance, the word 'must' denotes a legal obligation, while the word 'should' is a recommendation of good practice, and is the standard that the Commission expects operators to adopt and evidence. The Commission will expect operators to be able to explain the reasons for any departures from that standard.**

1.45~~17~~ This guidance emphasises the responsibility of senior management to manage the operator's money laundering and terrorist financing risks, and how this should be carried out on a risk-based approach. It sets out a standard approach to the identification of customers and verification of their identities, separating out basic identity from other measures relating to **CDD** ~~customer due diligence~~, including the obligation to monitor customer activity.

1.46~~18~~ It is accepted that a proportionate risk-based approach has to meet a variety of scenarios and, as such, has to be based on an understanding of how the business is designed to operate. There is, therefore, a need for ongoing and repeated assessments of risk to meet changing circumstances.

1.47~~19~~ The guidance contains the following sections:

- the importance of adopting a risk-based approach
- the importance of senior management taking responsibility for effectively managing the money laundering and terrorist financing risks faced by the operator's businesses
- the role and responsibilities of the nominated officer
- the proper carrying out of the CDD obligations, including monitoring customer transactions and activity
- record keeping
- the identification and reporting of suspicious activity.

Status of the guidance

1.48~~20~~ POCA requires a court to take account of industry guidance, such as this, that has been approved by a Treasury minister when considering whether a person within the regulated sector has committed the offence of failing to report. Similarly the Terrorism Act requires a court to take account of such approved industry guidance when considering whether a person has failed to report under that Act. The Regulations state that a court must consider whether someone has followed this guidance if they are prosecuted for failing to comply with the Regulations.[28] The first edition of this guidance was approved by HM Treasury on 27 July 2010.

1.49~~21~~ Operators must be able to demonstrate that they have taken all reasonable steps to comply with all the AML requirements. If they can demonstrate to a court and/or the Commission that they have followed this guidance then the court or the Commission is obliged to take that into account.

[28] Sections 330 and 331 of POCA and Regulation 45

1.5022 The Commission is not a 'designated authority' under the Regulations and therefore has no powers to take action against operators that breach the Regulations.[29] However, an ordinary code provision within the Licence Conditions and Codes of Practice requires casino operators to act in accordance with this guidance. Should operators not follow the code provision, the Commission may 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 (the Act).

1.5123 The Commission also has employees who have the powers of accredited financial investigators under POCA in England and Wales.[30] This means 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.

1.5224 The guidance provides a sound basis for operators to meet their legislative and regulatory obligations when tailored by operators to their particular business risk profile. Departures from this guidance, and the grounds for doing so, should be documented and may have to be justified~~, for example,~~ to, **amongst others,** the Commission.

2 Risk-based approach

Introduction

2.1 The Regulations impose compulsory compliance requirements and a breach can constitute a criminal offence.[31] However, within this legal framework of requirements, casinos have flexibility to devise policies and procedures which best suit their assessment of the money laundering and terrorist financing risks faced by their business. The Regulations require a policy and procedure in relation to risk assessment and management.[32]

2.2 Operators are already expected to manage their operations with regard to the risks posed to the licensing objectives in the Act, and measure the effectiveness of the policies and procedures they have put in place to manage those risks. The approach to managing the risks of the operator being used for money laundering or terrorist financing is consistent with the existing regulatory requirements.

2.3 **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.**

[29] Regulation 42
[30] ~~See Statutory Instrument No 2009/975.~~See The Proceeds of Crime Act 2002 (References to Financial Investigators) Order 2009 (Statutory Instrument No. 2009/975) and The Proceeds of Crime Act 2002 (References to Financial Investigators) (Amendment) Order 2009
[31] Regulation 45
[32] Regulation 20(1)(e)

2.~~43~~ The risk-based approach involves a number of discrete steps in assessing the most proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the operator. These steps require the operator to:

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

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

2.~~64~~ A risk-based approach will serve to balance the burden placed on operators and their customers with a realistic assessment of the threat of the operator being misused in connection with money laundering or terrorist financing. It focuses the effort where it is most needed and will have 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.

2.~~75~~ A risk-based approach requires the full commitment and support of senior management, and the active co-operation of all employees. **It** ~~Senior management~~ should ~~ensure that the risk-based approach is~~ **be** part of the operator's philosophy and **be** reflected in **the operator's** ~~its~~ policies, ~~and~~ procedures **and controls**. There needs to be a clear communication of the policies and procedures **to all employees** ~~across the operator~~, 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 risk.**

Identifying and assessing the risks faced by the operator

2.~~86~~ The operator should assess its risks in the context of how it is most likely be involved in money laundering, **criminal spend** or terrorist financing. Assessment of risk is based on a number of questions, including:

- What risk is posed by the business profile and customers using the casino?
- **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, perhaps who use and operate within their cheque cashing facilities?
- Is the business a mixed portfolio? Are customers 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 **to** 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 cheque or debit cards?
- Are customers likely to be individuals who hold public positions in other countries, that is, PEPs?
- 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?
- Are there likely to be situations where the customer's purchase or exchange of chips is irrational or not linked with gaming?

- Is the majority of business conducted in the context of business relationships?
- **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)?**
- **In relation to remote gaming, does the customer use shared internet protocol addresses, dormant accounts or virtual private network (VPN) connections?**

Risk assessments

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

2.10 **Risk, therefore, is a function of the three factors mentioned above:**

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

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

- **identification**
- **analysis**
- **evaluation**.

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

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

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

2.15 **Money laundering and terrorist financing risks may be measured using a number of factors. Application of risk categories to customers and situations can provide a strategy for managing potential risks by enabling operators to subject customers to proportionate controls and monitoring. The standard risk categories used by FATF for casinos are as follows:**

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

2.16 **The risk categories used by the Commission in its risk assessment are: customer risks (which includes country/geographic risks); means of payment risks (which forms part of the transaction risks); and product risks (these are the risks associated with particular gambling products).**

Country/geographic risk

2.17 **Some countries pose an inherently higher money laundering and terrorist financing risk than others. In addition to considering their own experiences, operators should take into account a variety of sources of information as identified by credible sources identifying countries with risk factors that may result in a determination that a country and customers from that country pose a higher risk. Operators may wish to assess information available from non-governmental organisations which can provide a useful guide to perceptions relating to corruption in the majority of countries.**

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

2.19 **The country/geographic risk can also be considered together with the customer risk.**

Customer risk

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

- **customers who are PEPs**
- **high spenders – the level of spending which will be considered to be high for an individual customer will vary among operators, and among casinos managed by the same operator**
- **disproportionate spenders – operators should obtain information about customers' financial resources so that they can determine whether customers' spending is disproportionate to their income or wealth**
- **casual customers – this includes tourists and participants in junkets, but can also include regular customers, particularly where their spending pattern changes**
- **improper use of third parties – criminals may use third parties or agents to avoid CDD undertaken at the threshold or to buy chips, or they may be used to gamble so as to break up large amounts of cash**
- **junkets – junket operators can pose a heightened money laundering risk**

- **multiple player accounts – some customers will open multiple player accounts under different names to hide their spending levels or to avoid breaching the CDD threshold**
- **unknown or anonymous customers – these customers may purchase large amounts of chips with cash at casino tables, and then redeem the chips for large denomination notes after minimal or no play.**

Transaction risk (including means of payment)

2.21 **Casinos should consider operational aspects (products, services, games, accounts and account activities) that can be used to facilitate money laundering and terrorist financing. In addition, land-based and remote casinos have the following potential transaction risks:**

- **proceeds of crime – there is a risk that the money used by a customer has arisen from criminal activities, so greater monitoring of high spenders will help to mitigate the risk**
- **cash – customers may use non-remote casinos to exchange large amounts of criminal proceeds, or may deposit criminal proceeds into an internet gambling account at a non-remote casino**
- **transfers between customers – customers may transfer money between themselves or may borrow money from unconventional sources, including other customers, which can offer criminals an opportunity to introduce criminal proceeds into the legitimate financial system through the casino**
- **use of casino deposit accounts – criminals may use accounts to deposit criminal proceeds and then withdraw funds with little or no play**
- **redemption of chips, tickets or tokens for cash or cheque, particularly after minimal or no play**
- **particularly in remote casinos:**
    - **multiple gambling accounts or wallets – customers may open multiple accounts or wallets with an operator in order to obscure their spending levels or to avoid CDD threshold checks**
    - **changes to bank accounts – customers may hold a number of bank accounts and regularly change the bank account they use for the remote operator**
    - **identity fraud – details of bank accounts may be stolen and used on remote gambling websites, or stolen identities may be used to open bank accounts or remote gambling accounts**
    - **pre-paid cards – these cards pose the same risks as cash, as remote operators normally cannot perform the same level of checks on the cards as they can on bank accounts**
    - **e-wallets – some e-wallets accept cash on deposit, which poses a higher risk, and some customers may use e-wallets to disguise their gambling**
    - **games involving multiple operators – for example, poker games often take place on platforms shared by a number of remote gambling operators, which can facilitate money laundering by customers, such as chip dumping.**

Product risk

2.22 **Product risk includes the consideration of the vulnerabilities associated with the particular products offered by the operator. In non-remote casinos there are a number of gambling opportunities that offer the potential for a money launderer to place funds and generate a winning cheque or similar with minimal play. Also, a number of gambling activities take place in remote and non-remote casinos where customers effectively play against each other. This offers the money launderer a means to transfer value by deliberately losing to the individual to whom they want to transfer the funds.**

2.23 **Products which may pose a money laundering risk for the operator therefore include:**

- **peer to peer gaming**
- **gaming where two or more persons place opposite, equivalent stakes on even, or close to even, stakes (for example, the same stake on red and on black in a game of roulette, including electronic roulette)**
- **gaming machines, which can be used to launder stained or fraudulent bank notes.**

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

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

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

- **whether the operator's business model is focused on:**
  - **attracting a large number of customers who gamble relatively small amounts, or**
  - **attracting a small number of customers who gamble relatively large amounts**
- **speed and volume of business**
- **for non-remote casinos, the size of the premises**
- **the customer profile, for example whether:**
  - **the majority of customers are regular visitors or are members**
  - **the casino relies on passing trade, including tourists or those who are part of junkets (for non-remote casinos)**
- **for non-remote casinos, whether the casino has VIP rooms or other facilities for high rollers**
- **types of financial services offered to customers**
- **types of customer payments and payment methods**
- **types of gambling products offered**
- **the customers' gambling habits**
- **staffing levels, and staff experience and turnover**
- **the type and effectiveness of existing gambling supervision measures and mechanisms**
- **whether the operator:**
  - **owns or manages other non-remote and remote casinos**
  - **offers different types of gambling**
  - **has other internet gambling websites**
- **whether the casino is standalone or integrated with other leisure facilities**
- **whether the operator is based in one country or has a gambling presence in multiple countries.**

2.27~~7~~ Deciding that a customer ~~is~~ present~~sing~~ a higher risk of money laundering or terrorist financing does not automatically mean that **t**he **person** is a **criminal,** money launderer or ~~a~~ financier of terrorism. Similarly, identifying a customer as presenting a low risk of money laundering or terrorist financing does not mean that the customer is definitely not ~~money~~ laundering **money or engaging in criminal spend**. Employees therefore need to remain vigilant and use their experience and common sense in applying the operator's risk-based criteria and rules, seeking guidance from their nominated officer as appropriate.

2.28~~8~~ Many customers carry a lower money laundering or terrorist financing risk. 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).

2.29 **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.**
- **A customer spent a large volume of cash at a casino, including a significant quantity of Northern Irish and Scottish banknotes. The customer told staff that the cash came from restaurants and takeaway food establishments that he ran around the United Kingdom. This explanation was accepted at face value by the staff, however, in reality the customer did not own any legitimate businesses and was later convicted of money laundering offences arising from criminal activity.**

2.309 Where a customer is assessed as presenting higher risk it ~~will~~ **would** be **expected that** ~~necessary to seek~~ additional information in respect of ~~the~~ **that** customer **is collected**. This will help the operator judge whether the higher risk that the customer is perceived to present is likely to materialise**, and provide grounds for proportionate and recorded decisions.** Such additional information **should** ~~may~~ include an understanding of where the customer's funds and wealth have come from. **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.**

2.3110 If casinos adopt the threshold approach to CDD, part of the risk-based approach will involve making decisions about whether or when verification should take place electronically. Operators must determine the extent of their CDD measures, over and above the minimum requirements, on a risk-sensitive basis depending on the risk posed by the customer and their level of gambling.

2.3211 In order to be able to detect customer activity that may be suspicious, it is necessary to monitor **all** transactions or activity.[33] **The** ~~M~~**m**onitoring **of** customer activity should be carried out using the risk-based approach. ~~with h~~**H**igher risk customers **should be** subjected to a ~~an appropriate~~ frequency and depth of scrutiny, ~~which is likely to be~~ greater than may be appropriate for lower risk customers. **This should not be confused with customers who are of** either **high or low commercial value to the operator**.

2.33 **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.**

Risk management is dynamic

2.3412 A money laundering/terrorist financing risk assessment is not a one-off exercise. Operators must therefore ensure that their policies and procedures for managing money laundering and terrorist financing 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.**

2.35 **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**.

Enhanced due diligence

2.36 **Operators are required to apply, on a risk-sensitive basis, enhanced customer due diligence measures and enhanced ongoing monitoring (commonly referred to as enhanced due diligence) in any situation which, by its nature, can present a higher risk of money laundering or terrorist financing.[34]**

[33] Regulation 8
[34] Regulation 14(1)

Politically exposed persons

2.37 **Enhanced due diligence measures must be applied in respect of PEPs. In particular, this means that an operator who proposes to allow a PEP to be a customer must:**

- **have approval from its senior management for establishing a business relationship with that person;**
- **take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship; and**
- **where a business relationship is entered into, conduct enhanced ongoing monitoring of the relationship.**

2.38 **PEPs are more fully discussed in section 6 of this guidance.**

~~Remote casinos – enhanced due diligence~~ Remote casinos

2.39~~13~~ The Regulations view situations where a customer is not physically present for identification purposes **(as in the case of remote casinos)** as higher risk for money laundering and require an operator to **undert**ake **enhanced due diligence** ~~specific and adequate measures to compensate for the higher risk (referred to as enhanced customer due diligence and ongoing monitoring in the Regulations)~~, for example, by applying one or more of the following measures:[35]

(a) ensuring that the customer's identity is established by additional documents, data or information;

(b) supplementary measures to verify or certify the documents supplied, or confirmatory certification by a credit or financial institution which is subject to the money laundering directive[36]; or

(c) ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution.

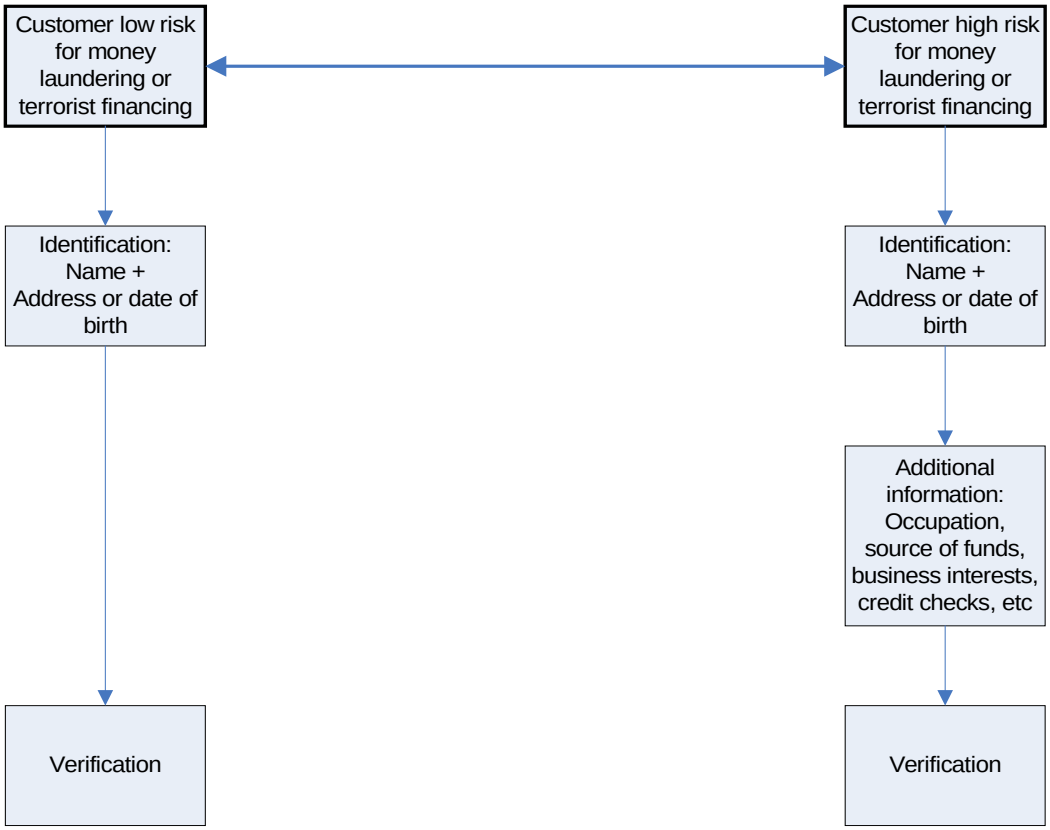
2.40~~14~~ These measures should be applied regardless of the threshold approach for CDD and should be tailored to the risk posed.[37] Option (c) above will fit with remote casinos' business methods where it is necessary for a customer to have a bank or credit card account, which must be in **the customer's** ~~his~~ name.

~~**2.15**~~ Remote operators also have the benefit of being able to withhold payment of winnings or remaining deposits until satisfied that CDD is satisfactorily done.

2.41~~16~~ Remote operators should include in their policies how they will manage, on a risk-sensitive basis, the higher risks presented by customers not being physically present for identification purposes.

[35] Regulation 14(2)
[36] This refers to any credit or financial institution in the EU which is subject to EU Money Laundering Directive.
[37] The EU 4th Money Laundering Directive alters the requirements for enhanced customer due diligence. Under the new Directive, enhanced customer due diligence is likely to be required for non face-to- face business relationships or transactions *where there are no safeguards* (such as electronic signatures). However, until the provisions of the Directive are transposed into UK legislation, operators should continue to apply the requirements under the Regulations. Transposition into UK legislation is likely to occur in 2017.

Figure 1: Risk-based approach



Note:
Casino operators should undertake risk assessments of each premises and each remote site and:
(a) look at the average drop/win per customer, and
(b) risk assess each customer.
See paragraphs 2.1 to 2.16 of this guidance for more detail on assessing risk.

3 Customer relationships

3.1 **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.**

3.2 **Operators are subject to both certain provisions of POCA, the Regulations 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.**

3.3 **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.**

3.4 **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.**

3.5 **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. Operators may find it helpful to provide their customers with a leaflet which explains why they are being asked questions about their game play.**

3.6 **The Commission recognises that some operators may find their obligations under POCA and the Regulations 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 Regulations (and the Act and the relevant licence conditions and codes of practice), in particular in relation to CDD, the reporting of money laundering activity by customers and obtaining appropriate consent where necessary.**

3.7 **Customer relationships for AML purposes consist of three aspects:**

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

3.8 **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

3.9 **The establishment of a business relationship with a customer will occur when either:**

- **the casino starts tracking a customer's drop/win figures**
- **a customer opens an account with the operator or joins a membership scheme**
- **a customer obtains a cheque cashing facility with the operator.**

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

- **the potential risk posed by the customer**
- **appropriate due diligence checks on the customer**
- **whether it is known or suspected that the customer may launder money, including criminal spend.**

3.11 **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.**

3.12 **There is further discussion of business relationships in paragraphs 7.5 to 7.8.**

Customer monitoring

3.13 **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.**

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

3.15 **Once knowledge or suspicion of criminal spend is linked to a customer in one area of the business (for example, gaming machine play), operators should monitor the customer's activity in other areas of the business (for example, table games).**

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

3.17 **Customer monitoring forms part of ongoing monitoring, which is discussed in paragraphs 6.8, 6.9, 7.7 and 7.8.**

Termination of business relationship

3.18 **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 an increasing level of suspicion, or actual knowledge of, money laundering,**

otherwise they may potentially commit one of the principal money laundering offences.

3.19 **Additionally, where the operator cannot complete CDD measures, the business relationship with the customer *must* be terminated and the operator should consider submitting a suspicious activity report to the NCA.**[38]

3.20 **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 from the NCA before paying out any winnings or returning funds to the customer**.

~~3~~4 Senior management responsibility

Introduction

~~3~~4.1 Senior management must be fully engaged in the processes around an operator's assessment of risks for money laundering and terrorist financing, and must be involved at every level of the decision making to develop the operator's policies and processes to comply with the Regulations. Disregard for the legal requirements, for example, turning a blind eye to customers spending criminal proceeds, may result in criminal or regulatory action.

~~3~~4.2 It is considered best practice, and is explicit in parts of the Regulations, that a risk-based approach should be taken to tackling money laundering and terrorist financing.

~~3~~4.3 Operators, using a risk-based approach, should start from the ~~premise~~ **principle** that most customers are not money launderers or terrorist financiers. However, operators should have policies and procedures in place to highlight those customers who, according to criteria established by the operator, may present a higher risk. The policies and procedures should be proportionate to the risks involved.

[38] Regulation 11

Obligations on all operators

~~3~~4.4 An officer of a licensed operator which is subject to the Regulations (that is, a director, manager, secretary, chief executive, member of the management committee, or a person purporting to act in such a capacity) who consents to, or connives in, the commission of offences under the Regulations, or where the commission of any such offence is attributable to any neglect on his part, will be individually liable for the offence.[39]

~~3~~4.5 **Senior management should require that** ~~T~~**t**he nominated officer **provide** ~~should compile~~ an annual report covering the operation and effectiveness of the operator's **systems** ~~policies~~ and **controls** ~~procedures~~ to combat money laundering, **and take any action necessary to remedy deficiencies identified by the report in a timely manner**. In practice, senior management should determine the depth and frequency of information **provided by the nominated officer that** they feel is necessary to discharge their responsibilities. The nominated officer may also wish to report to senior management more frequently than annually, as circumstances dictate. The nominated officer may not need to provide the names of suspected persons in any report.

Policies and procedures

~~3~~4.6 Operators must establish and maintain appropriate written risk-based policies and procedures relating to:

- CDD measures and ongoing monitoring**, including enhanced measures for high risk customers;**
- reporting;
- record keeping;
- internal control;
- risk assessment and management;
- training; and
- the monitoring and management of compliance with, and the internal communication of, such policies and procedures.[40]

~~3~~4.7 The operator's policies and procedures should cover:

- the arrangements for nominated officer reports to senior management;
- the systems for customer identification and verification, including enhanced arrangements for high risk customers, which includes PEPs;
- the circumstances in which additional information in respect of customers will be sought in the light of their activity;
- the procedures for handling SARs, covering both reporting by employees and transmission to **the NCA** ~~SOCA~~;
- the mechanisms for contact between the nominated officer and law enforcement or **the NCA** ~~SOCA~~, including the circumstances in which appropriate consent should be sought;
- the arrangements for recording information not acted upon by the nominated officer, with reasoning why no further action was taken;
- the monitoring and management of compliance with internal policies and procedures;
- the communication of such policies and procedures, including details of how compliance is monitored by the nominated officer, and the arrangements for communicating the policies and procedures to all relevant employees;
- employee training records; and
- supporting records in respect of business relationships, and the retention period for the records.

[39] Regulation 47
[40] Regulation 20

Training

~~34~~.8 The Regulations require that all relevant employees of casinos must be trained on the prescribed AML and CTF topics. Operators must ensure that their employees understand the Regulations and apply the operator's policies and procedures, including the requirements for CDD, record keeping and SARs.

~~34~~.9 One of the most important controls over the prevention and detection of money laundering is to have employees who are alert to the risks of money laundering and terrorist financing, and who are well trained in the identification of unusual activities or transactions which appear to be suspicious. The effective application of even the best designed control systems can be quickly compromised if the employees applying the systems are not adequately trained. The effectiveness of the training will therefore be important to the success of the operator's AML/CTF strategy.

~~34~~.10 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 the prevention of money laundering and terrorist financing, and for providing them with regular training in the identification and reporting of anything that gives grounds for suspicion of money laundering or terrorist financing. **Operators should also monitor the effectiveness of such training, to ensure that all employees are trained in an appropriate and timely manner, and that the training is fit for purpose.**

~~34~~.11 Under POCA and the Terrorism Act, individual employees face criminal penalties if they are involved in money laundering or terrorist financing. If they do not make an internal report to their nominated officer when necessary they may also face criminal sanctions. It is important, therefore, that employees are made aware of their legal obligations, and are given training in how to discharge them.

~~34~~.12 The Regulations require operators to take appropriate measures so that all relevant employees are:

- made aware of the law relating to money laundering and terrorist financing; and
- regularly given training in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing.[41]

~~34~~.13 'Relevant employees' includes the holders of personal management licences and personal functional licences issued by the Commission as well as employees responsible for completing CDD measures. It does not include any ancillary employees such as catering and bar staff.

~~34~~.14 The content of any training, the regularity of training and the assessment of competence following training are matters for each operator to assess and decide in light of the money laundering risks they identify. The Commission will expect such issues to be covered in each operator's policies and procedures. This should make provision for the attainment of an appropriate competence level by the relevant employees identified in paragraph ~~34~~.13, prior to them undertaking the duties for which they will be responsible. This may, for example, be achieved by the attainment of an appropriate pass rate in a competency test following training.

~~34~~.15 Operators should also ensure that relevant employees are aware of and understand:

- their responsibilities under the operator's policies and procedures for the prevention of money laundering and terrorist financing;
- the money laundering and terrorist financing risks faced by an operator and each of its casino premises;
- the operator's procedures for managing those risks;
- the identity, role and responsibilities of the nominated officer, and what should be done in his absence;

[41] Regulation 21.

- the potential effect of a breach upon the operator and upon its employees;
- how the casino will undertake CDD;
- how the casino will track customers when CDD is not undertaken on entry to the casino; and
- how PEPs will be identified.

~~3~~4.16 There is no single solution when determining how to deliver training and a mix of training methods may, therefore, be appropriate. On-line training systems can provide a solution for many employees, but this approach may not be suitable for all employees. Classroom training can be more effective in these circumstances.

~~3~~4.17 Procedure manuals, whether paper or electronic, are useful in raising employee awareness and can supplement more dedicated forms of training, but their main purpose is generally to provide ongoing reference rather than being written as training material.

~~3~~4.18 Ongoing training **must** ~~should~~ be given to all relevant employees at appropriate intervals. Records should be maintained to monitor who has been trained, when they received the training, the nature of the training and the effectiveness of the training.

~~3~~4.19 The nominated officer should be heavily involved in devising and managing the delivery of such training, taking particular care to ensure that systems are in place to cover all part-time or casual employees.

~~3~~4.20 **The NCA** ~~SOCA~~ publishes a range of material at www.nationalcrimeagency~~soca~~.gov.uk, such as threat assessments and risk profiles, of which operators may wish to make their employees aware. The information on this website could usefully be incorporated into operators' training materials.

4.21 **It is also recommended that operators consult the Commission's AML webpage, which has useful information (including statements regarding AML controls) and links to other AML resources.**

~~4~~5 Nominated officer

~~4~~5.1 Licensed casino operators must appoint a nominated officer, who is responsible for:[42]

- receiving internal disclosures under Part 7 of POCA and Part III of the Terrorism Act;
- deciding whether these should be reported to **the NCA** ~~SOCA~~;
- if appropriate, making such external reports; and
- ensuring that appropriate consent is applied **for** as necessary.

5.2 **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.**

~~4.2~~5.3 ~~A~~**The** nominated officer should be able to monitor the ~~effectiveness of the~~ day-to-day operation of the operator's AML/CTF policies, 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.**

~~4.3~~5.4 The term 'nominated officer' is used and defined in the Regulations.

[42] Regulation 20(2)(d)

Standing of the nominated officer

~~4.4~~5.5 The nominated officer is responsible for the oversight of all aspects of the operator's AML/CTF activities at all premises. They are the focal point for all activity within the operator relating to AML. The individual appointed as nominated officer must have a sufficient level of seniority. The nominated officer must hold a personal management licence (PML) issued by the Commission. The job description of the nominated officer should clearly set out the extent of the responsibilities given to him and his objectives. The nominated officer will need to be involved in establishing the basis on which a risk-based approach to the prevention of money laundering and terrorist financing is put into practice.

~~4.5~~5.6 The nominated officer must:

- have the authority to act independently in carrying out his responsibilities
- be free to have direct access to the Commission and appropriate law enforcement agencies, including **the NCA** ~~SOCA~~
- be free to liaise with **the NCA** ~~SOCA~~ on any question of whether to proceed with a transaction in the circumstances, that is, in relation to appropriate consent.

5.7 **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.**

5.8 **The Commission recognises that some 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.**

~~4.6~~5.9 Senior management of the operator must ensure that the nominated officer has sufficient resources available to him, including appropriate employees and technology. This should include arrangements that apply in his temporary absence.

~~4.7~~5.10 Where a nominated officer is temporarily unavailable, another PML holder may deputise. Operators should consider the appointment of a permanent deputy nominated officer.

~~4.8~~5.11 Where AML/CTF tasks are delegated by an operator's nominated officer **to another employee**, ~~the Commission will expect~~ the nominated officer **remains responsible for AML issues** ~~to take ultimate managerial responsibility~~ and **is** ~~they are~~ likely to remain liable for the commission of any criminal offences relating to POCA, the Terrorism Act or the Regulations. The Commission strongly recommends that in such circumstances:

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

Internal and external reports

~~4.9~~5.12 An operator must require that anyone working for the operator, to whom information or other matter comes in the course of business, as a result of which they know or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing must make an internal report to their nominated officer.

Whilst disclosure to another of the fact that a person may be engaged in money laundering is generally an offence, such disclosures to a nominated officer are specifically protected, where they are made as soon as is practicable and in the course of the discloser's employment.[43] It is recommended that employees be made aware that they have a legal defence to prosecution if they make an internal report to the nominated officer as soon as is reasonably practicable after the information or other matter comes to their attention.

~~4.10~~5.13 Any internal report should be considered by the nominated officer, in the light of all other relevant information, to determine whether or not the information contained in the report leads them to form knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of money laundering or terrorist financing.

~~4.11~~5.14 The nominated officer should consider any information held about the customer's personal circumstances that might be available to the operator; and review other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship and identification records held.

~~4.12~~5.15 The nominated officer must be fully conversant with his legal obligations to make external reports to **the NCA** SO~~CA~~.

~~4.13~~5.16 Many of the records required by the Regulations relate to work done, or decisions made, by the nominated officer, including records of why reports have not been made to **the NCA** ~~SOCA~~.

~~5~~6 Customer due diligence

Introduction

~~5~~6.1 A key requirement in the Regulations is the requirement to make checks on customers, known as customer due diligence or CDD.[44] Casino operators may take one of two approaches; identifying and verifying the identity of all customers on entry to the casino's licensed premises or undertaking identification and verification when a customer approaches the threshold set out in the Regulations.

~~5~~6.2 This requirement applies to customers of both remote and non-remote casinos. Aside from these checks being a statutory requirement in the Regulations, they also make sense in terms of helping operators avoid the commission of criminal offences under POCA.

~~5~~6.3 The Regulations define casino as 'the holder of a casino operating licence'.[45] CDD therefore may be conducted just once by the holder of an operating licence and does not need to be repeated each time a customer visits another casino operated by that licensee. CDD records held by a casino operator will need to be available across the operator's different casino premises and the policies and procedures must include details of how the operator will manage this. Operators should note that CDD is ongoing and may need updating for changes in the customer's circumstances and personal details.

6.4 **The Regulations require land-based casinos to establish and verify the identity of all customers:**

- **before entry to any premises where such facilities are provided; or**
- **who, in the course of any period of 24 hours –**
  - **purchase from, or exchange with, the casino, chips with a total value of €2,000 or more;**
  - **pay the casino €2,000 or more for the use of gaming machines.[46]**

[43] Section 337 of POCA
[44] Regulation 10
[45] Regulation 3(13)
[46] Regulation 10(1)

6.5 **The Regulations also require remote casinos to establish and verify the identity of all customers:**

- **before access is given to such facilities; or**
- **who, in the course of any period of 24 hours pay to, or stake with, the remote casino €2,000 or more in connection with facilities for remote gaming.[47]**

6.6 **The casino must verify the identity of each customer before or immediately after such purchase, exchange, payment or stake takes place.[48]**

6.7 **Operators should satisfy themselves that the sources of information employed to carry out CDD 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. However, operators should ensure that they are not placing an overreliance on one source of information to conduct these checks.**

Ongoing monitoring

6.8 **The Regulations require operators to conduct ongoing monitoring of a business relationship. This entails the following:**

- **scrutiny of transactions undertaken throughout the course of the relationship (including,**
  where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, his business and risk profile; and
- **keeping the documents, data or information obtained for the purpose of applying CDD measures up-to-date.**

6.9 **Casinos are expected to approach this requirement on a risk basis. Dependent on how frequently a casino forms business relationships it may be good practice to apply ongoing monitoring more widely. Regular players should be the subject of closer scrutiny and their level of play should be assessed with reference to the information already known about them, and where necessary, additional information must be collected and retained about the source of their funds.**

Threshold approach

5.46.10 **As discussed in paragraphs 6.4 and 6.5, the** ~~The~~ Regulations set out thresholds which, if customer transactions approach this level, require the casino operator to verify the identity of the customer. These limits are:

- in non-remote casinos the 'threshold approach for chips' – identification and verification is required when a customer purchases from or exchanges with the casino chips with a total value of €2,000 or more during any period of 24 hours;
- in non-remote casinos the 'threshold approach for gaming machines' – identification and verification is required when a customer pays €2,000 or more into the gaming machines during any period of 24 hours. This threshold amount does not include any winnings; or
- in remote casinos the 'threshold approach for remote gaming' – identification and verification is required when a customer pays to, or stakes with, the casino €2,000 during any period of 24 hours **(but see paragraph 6.16 below).**

5.56.11 The gaming machine limits only apply in premises based casinos. By separating the purchase or exchange of chips from the payment to use gaming machines there is the potential for customers to spend up to €2,000 in the machines in addition to the purchase

[47] **Regulation 10(1).**
[48] **Regulation 10(2)**

or exchange of chips up to €2,000. It should be noted that for the purpose of this guidance 'gaming machine' and 'stake' have the same meaning as that in the Act.

~~5.66~~.12 In premises based casinos automated and semi-automated table games such as touch-bet roulette are not defined as gaming machines and therefore the take in these games should be counted towards the threshold approach for chips.

6.13 The threshold test in relation to remote casinos refers to money being 'paid' or 'staked'. Regulation 10(3) of the Regulations states that 'stake' has the meaning given by section 353(1) of the Act. Section 353(1) of the Act provides that 'stake' means an amount paid or risked in connection with gambling and which either –

- **is used in calculating the amount of the winnings or the value of the prize that the person making the stake receives if successful, or**
- **is used in calculating the total amount of winnings or value of prizes in respect of the gambling in which the person making the stake participates.**

6.14 The Act draws a distinction between amounts paid and amounts risked, however, both are a 'stake'. 'Amounts paid' is interpreted as including (but not limited to) the payment of new funding. 'Amounts risked' is a wider concept and is interpreted as including recycled winnings. Thus 'stake' includes the recycling of previous winnings, as well as newly introduced sums of money.

6.15 This interpretation is made equally clear in the Regulations, where a similar distinction is drawn (in relation to the threshold test for remote casinos), namely pay to or stake with €2000 or more. Here, 'stake' has the same meaning as described above. 'Pay to' is a phrase which has been deliberately included in the test and is interpreted as meaning the payment of new funding. 'Stake', as indicated above, includes recycled winnings.

6.16 Remote casino operators should therefore include recycled winnings (or "turnover") where they use the threshold approach to determine when CDD is required under regulation 10 of the Regulations. It should also be noted that, under the Regulations, withdrawals from a remote gambling account are not included for threshold purposes.

6.17 Remote casino operators adopting the threshold approach should also consider the requirements for enhanced customer due diligence discussed in paragraphs 2.33 to 2.38.

~~5.76~~.18 If casinos wish to adopt the threshold approach, the following two conditions must be satisfied:

- it must verify the identity of each customer before, or immediately after, the customer purchases, exchanges, pays or stakes €2,000 or more; and
- the Commission must be satisfied that the casino operator has appropriate procedures in place to monitor and record the total value of chips purchased from or exchanged with the casino, the total money paid for the use of gaming machines, or the total money paid or staked in connection with facilities for remote gaming by each customer.

~~5.86~~.19 Casino operators will have to satisfy the Commission that they have the mechanisms in place that are appropriate for the spend profile in each premises. For example, a casino with a customer drop/win average considerably below the threshold will need mechanisms in place to monitor customer transactions to be sure that any customer reaching either of the threshold levels is picked up in good time to allow CDD to be completed. Where the operator has a number of premises, the Commission will consider the use of the threshold approaches for each casino premises rather than for an operator.

~~5.9~~6.20 Casinos adopting the threshold approach should think carefully about whether they wish to defer both identification and verification until the threshold is reached, or whether identification will be conducted on entry but verification deferred until the threshold is reached. For example, a premises based casino may operate a membership scheme where customers are identified on admission but verification only occurs once the threshold is approached. Similarly, remote casinos may require customers to identify themselves (and undertake age verification) on registering with the casino but only require verification of identity if the threshold is approached. **This is sometimes called the hybrid approach.**

~~5.10~~6.21 There may be significant advantages in asking customers for their identification on entry, even if verification of this information is deferred until the threshold is reached, for example, identifying customers on entry means it will not be necessary to interrupt the customer's gambling once the threshold is reached, and verification becomes necessary.

~~5.11~~6.22 Casinos **must** ~~have to~~ monitor both **the** purchase and exchange of chips. If either hits the threshold, CDD will be necessary.

~~5.12~~6.23 A key challenge for casinos wishing to adopt the threshold approach is keeping track of the level of all an individual customer's purchases and exchanges of chips, and spend on the gaming machines. However, it **may be** ~~is~~ appropriate to do so in light of the known spend patterns in each premises.

~~5.24~~6.24 Should casino operators choose to adopt the threshold approach, they must satisfy the Commission, on a premises-by-premises basis, that they have the appropriate procedures in place to manage the threshold in light of the assessed money laundering risk and spending profile at each premises.

6.25 Some remote casinos operate a 'wallet' system which allows customers to use the money in their wallet in different parts of the operator's site. An operator's site may include some casino games as well as other games. It is only when a customer first enters the casino part of an operator's website and stakes money or chips that the CDD requirements apply. The Regulations do not apply to people 'window shopping' in a remote casino's website, it applies only when money is staked. Where an operator is unsure of what the funds in the wallet will be used for (for example, casino or sports betting) they should consider applying these controls to all customers.

6.26 Casinos using the 'threshold approach' must be sure that they are able to end transactions with a customer who reaches the threshold if they are unable to comply with the CDD requirements.

6.27 The Commission has not determined the start of a 24 hour period for the purposes of the Regulations. Casino operators are free to choose the start time of their 24 hour period (previously referred to as the 'business day) to meet the demands of their business.

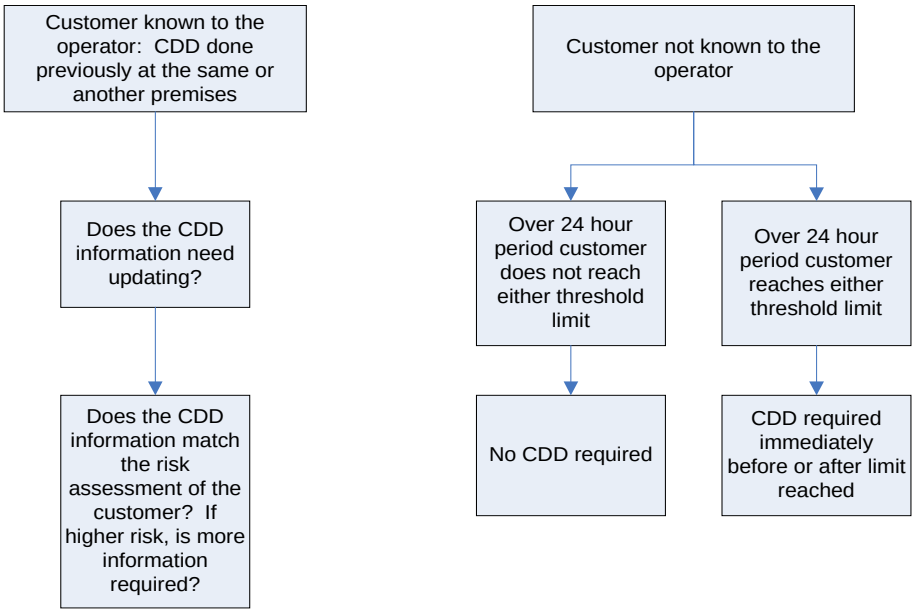
Identification and verification on entry

6.28 The on entry approach requires casinos to identify and verify the identity of the customer before entry to any premises where gaming facilities are provided, or before access is given to remote gaming. Once the customer's identity is verified he may commence gaming.

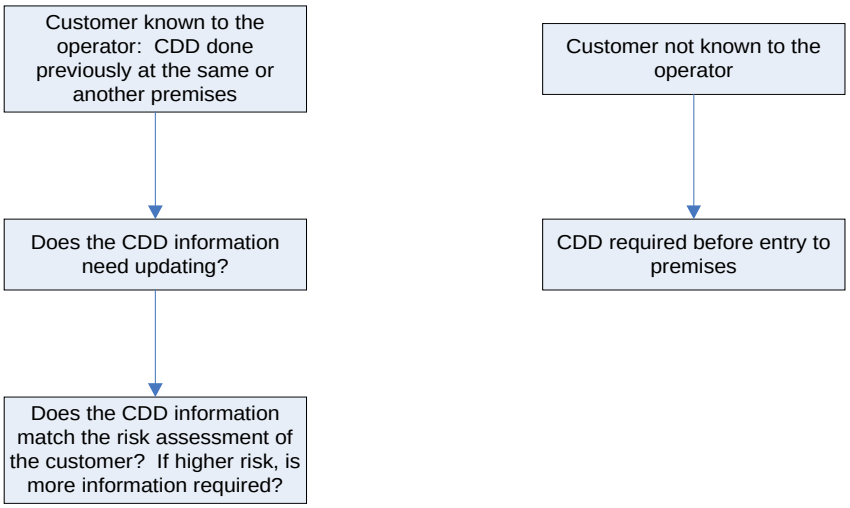
6.29 If a casino using the on entry approach to CDD is unable to complete the appropriate CDD they must not allow the customer access to the premises or to the remote gaming. In non-remote casinos this does not allow guests of known customers a single entry without undertaking CDD. However, operators should consider using variations of the threshold CDD approach for guests of casino members.

Figure 2: Customer due diligence

Threshold model

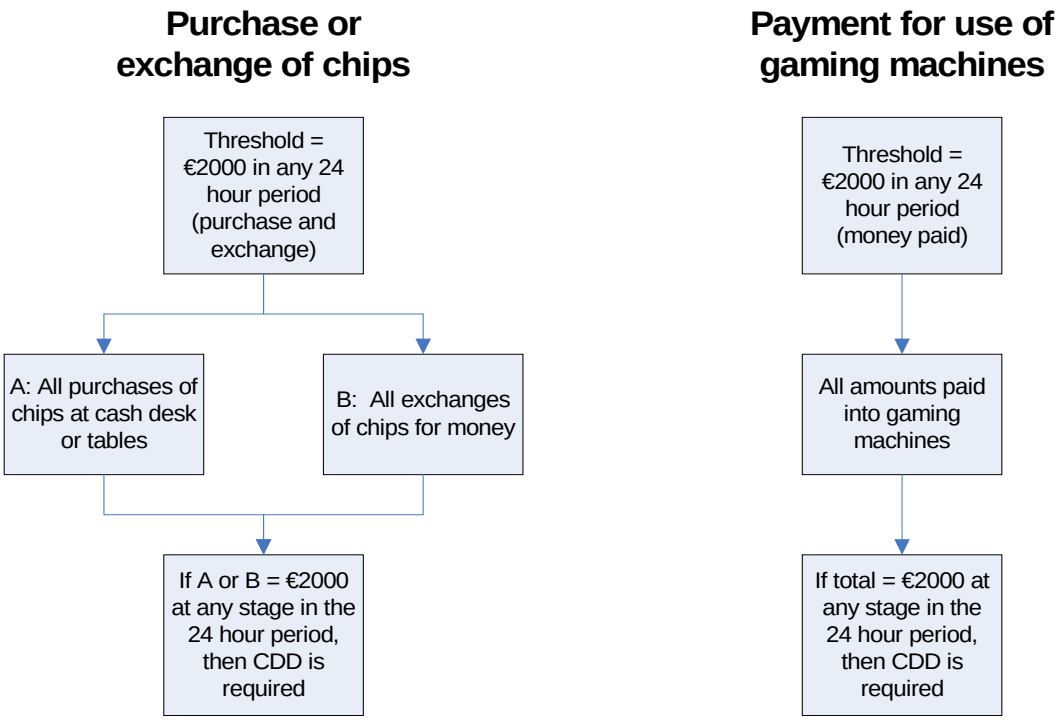


On entry model



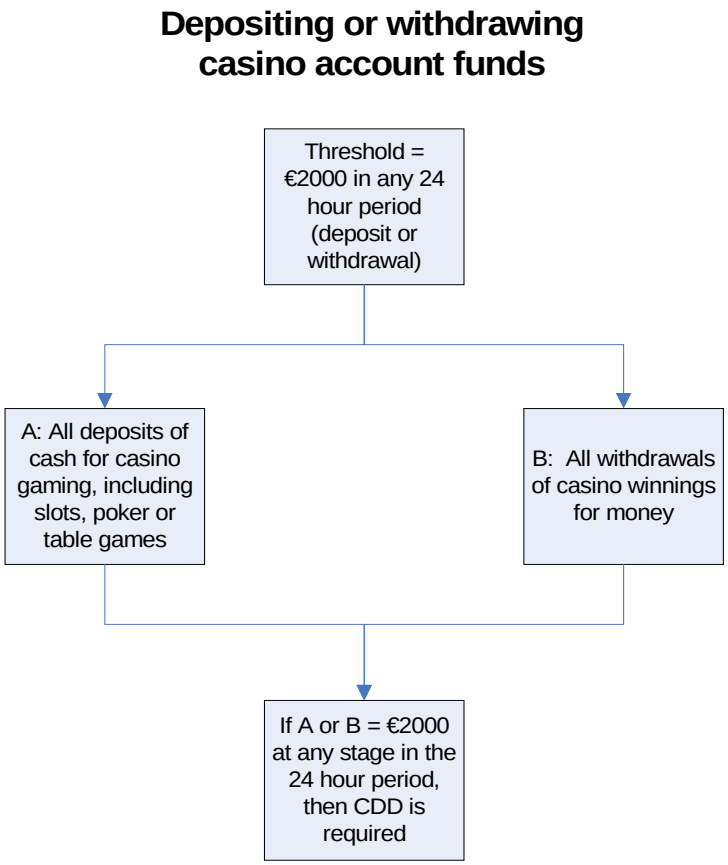
Notes:
1. Operator to be reasonably satisfied that the customer is who they claim to be.
2. The requirement applies to an operator, not to each premises.
3. Identification: Name, plus residential address or date of birth.
4. Verification: Documents or electronically.
5. Records of CDD to be kept for five years from the end of the business relationship or last visit to the premises run by the operator.

Figure 3: Determining when the threshold is reached (non-remote casinos) – chips and gaming machines



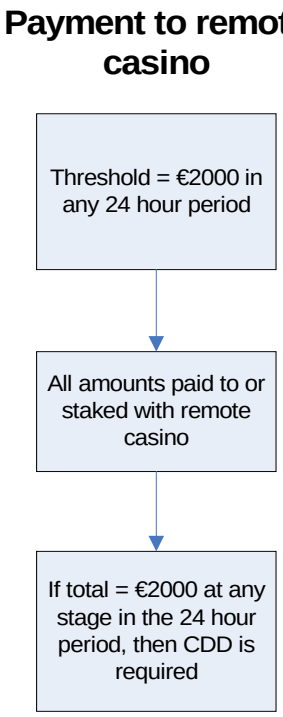
Notes:
1. The casino can set its own 24 hour period, for example the same hours as the business day, as appropriate to its business model.
2. A customer could spend €1800 on chips and a further €1800 in a gaming machine and not reach the threshold (see paragraph 5.5 of this guidance).
3. Risk-based approach – operator analysis of spending behaviours at each premises and an objective assessment made of the likelihood of customers reaching either threshold. Measures then put in place need to capture all customers likely to hit either threshold.

Figure 4: Determining when the threshold is reached (non-remote casinos) – casino account



Notes:
1. The casino can set its own 24 hour period, for example the same hours as the business day, as appropriate to its business model.
2. Risk-based approach – operator analysis of spending behaviours at each premises and an objective assessment made of the likelihood of customers reaching the threshold. Measures then put in place need to capture all customers likely to hit the threshold.

Figure 5: Determining when the threshold is reached (remote casinos)



Notes:
1. The casino can set its own 24 hour period, for example the same hours as the business day, as appropriate to its business model.
2. "Stake" has the meaning in the Gambling Act 2005.
3. Risk-based approach – operator analysis of spending behaviours and an objective assessment made of the likelihood of customers reaching the threshold. Measures then put in place need to capture all customers likely to hit the threshold.

~~5.14 Some remote casinos operate a 'wallet' system which allows customers to use the money in their wallet in different parts of the operator's site. An operator's site may include some casino games as well as other games. It is only when a customer first enters the casino part of an operator's website and stakes money or chips that the CDD requirements apply. The Regulations do not apply to people 'window shopping' in a remote casino's website, it applies only when money is staked. Where an operator is unsure of what the funds in the wallet will be used for (for example, casino or sports betting) they should consider applying these controls to all customers.~~

~~5.15 Casinos using the 'threshold approach' must be sure that they are able to end transactions with a customer who reaches the threshold if they are unable to comply with the CDD requirements.~~

~~5.16 The Commission has not determined the start of a 24 hour period for the purposes of the Regulations. Casino operators are free to choose the start time of their 24 hour period (previously referred to as the 'business day) to meet the demands of their business.~~

~~Identification and verification on entry~~

~~5.17 The 'on entry' approach requires casinos to identify and verify the identity of the customer before entry to any premises where gaming facilities are provided, or before access is given to remote gaming. Once the customer's identity is verified he may commence gaming.~~

~~5.18 If a casino using the 'on entry' approach to CDD is unable to complete the appropriate CDD they must not allow the customer access to the premises or to the remote gaming. This puts a stop, in non-remote casinos, to the current practice of allowing guests of known customers a single entry without undertaking CDD. However, operators should consider using variations of the threshold CDD approach for guests of casino members.~~

Identification and verification

~~5.19~~6.30 Applying CDD measures involves several steps. The operator is required to identify customers and then verify their identities, either upon entry or when reaching the threshold. Identification of a customer is being told or coming to know of the customer's identifying details, such as their name and address. Verification is obtaining some evidence which supports this claim of identity. The operator *identifies* the customer by obtaining a range of information about him. The *verification* of the identity consists of the operator verifying some of this information against documents, data or information obtained from a reliable and independent source.

Identification

~~5.20~~6.31 Identification of customers consists of a number of aspects, including the customer's name, current and past addresses, date of birth, place of birth, physical appearance, employment and financial history, and family circumstances.

~~5.21~~6.32 Casino operators ~~may~~ **should** identify their customers ~~simply~~ by asking them for personal information, including name, home address and date of birth**, or by using** ~~O~~**o**ther sources of identity, **including** ~~can include~~:

- identity documents, such as passports and photocard driving licences presented by customers
- other forms of confirmation, including assurances from persons within the regulated sector (for example, banks) or employees within the same casino or casino group who have dealt with the customer for some time.

6.33 ~~Some or all of this information will need to be verified.~~ It may also be helpful to obtain information on customers' source of funds and level of legitimate income, for example **their**

occupation. This information may assist casinos with their assessments about whether a customer's level of gambling is in profile for their approximate income, or whether it is suspicious.

Verification

~~5.22~~6.34 Information about customer identity must then be verified through documents, data and information which come from a reliable and independent source. There are a number of ways that a person's identity can be verified, including:

- obtaining or viewing original documents
- conducting electronic verification
- obtaining information from another person in the regulated sector (for example, banks).

No method of verification, either documentary or electronic, can conclusively prove that the customer definitely is who they claim to be. However, the Commission expects casinos to be reasonably satisfied, following appropriate inquiry, that customers are who they claim to be. **Where confirmation of a customer's identity is obtained from employees in the same casino group, the Regulations still require operators to verify this identity using an independent source. This is particularly relevant where the casino providing the confirmation is located in another jurisdiction.**

~~5.23~~6.35 It is generally considered good practice to require either:

- one government document which verifies either name and address, or name and date of birth
- a government document which verifies the customer's full name and another supporting document which verifies their name and either their address or date of birth.

~~5.24~~6.36 Some casinos have adopted the practice of allowing celebrities who are household names to by-pass the identification procedures agreed under the 2003 Regulations. Identification under these circumstances is not an issue. Verification may not be an issue owing to the easy availability of open source data and public knowledge that can be relied on as 'information from an independent and reliable source'. If such circumstances apply then the casino must keep records of the celebrity's presence at the casino, how their identity has been verified and where necessary the supporting records of their gaming. CDD using a customer's celebrity status is a subjective decision and must be supported by adequate records.

Electronic verification

~~5.25~~6.37 Increasingly casinos use reliable electronic systems to help with verification. Some of these systems also have the advantage of assisting in the identification of PEPs. The amount of electronic information available about individuals will vary, depending on the extent of their electronic 'footprint'.

~~5.26~~6.38 Electronic data sources can provide a wide range of confirmatory material without necessarily requiring the customer to produce documents. Electronic sources can be a convenient method of verification. They can be used either as the sole method of verification, or in combination with traditional document checks, on a risk basis. For an electronic check to provide satisfactory evidence of identity on its own it must use data from multiple sources, and across time, or incorporate qualitative checks that assess the strength of the information supplied. An electronic check that accesses data from a single source (for example, a single check against the electoral roll) is not enough on its own to verify identity.

~~5.27~~6.39 Where such sources are used for a credit check, the customer's permission is required under the Data Protection Act 1998 (the Data Protection Act). Credit checks can provide inexpensive information on which to assess a customer's access to funds and to obtain a

credit profile to match against spending patterns. For example, a criminal spending large amounts of criminal property would most likely not match his or her credit profile. A search for identity verification for AML/CTF purposes, however, leaves a different footprint on the customer's electronic ~~file~~ **record**, and the customer's permission is not required, but they must be informed that this check is to take place. There are systems available that give typical financial and lifestyle profiles of people in a given postcode, such systems do not amount to credit check and do not require the use of personal information but can provide helpful indicators of someone's expected financial profile.

~~5.28~~6.40 Some external electronic databases are accessible directly by casinos but it more likely they will be purchased from an independent third party organisation. The size of the electronic 'footprint' in relation to the depth, breadth and quality of data, and the degree of corroboration of the data supplied by the customer may provide a useful basis for an assessment of the degree of confidence in the product.

~~5.29~~6.41 A number of commercial agencies which access many data sources are accessible online by operators, and may provide operators with a composite and comprehensive level of electronic verification through a single interface. Such agencies use databases of both positive and negative information, and many also access high-risk alerts that utilise specific data sources to identify high-risk conditions, for example, known identity frauds or inclusion on a sanctions list.

~~5.30~~6.42 Positive information (relating to full name, current address, date of birth) can prove that an individual exists, but some can offer a higher degree of confidence than others. Such information should include data from more robust sources – where an individual has to prove their identity, or address, in some way in order to be included, as opposed to others, where no such proof is required.

~~5.31~~6.43 Negative information includes consideration of lists of individuals known to have committed fraud, including identity fraud, and registers of deceased persons. Checking against such information may be appropriate where other factors suggest an increased risk of impersonation fraud.

Criteria for use of an electronic data provider

~~5.32~~6.44 Before using a commercial agency for electronic verification, operators should be satisfied that information supplied by the data provider is considered to be sufficiently extensive, reliable and accurate. This judgement may be assisted by considering whether the provider meets all the following criteria:

- it is recognised, through registration with the Information Commissioner's Office, to store personal data;
- it uses a range of positive information sources that can be called upon to link an applicant to both current and previous circumstances;
- it accesses negative information sources, such as databases relating to identity fraud and deceased persons;
- it accesses a wide range of alert data sources; and
- it has transparent processes that enable the operator to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject.

~~5.33~~6.45 In addition, a commercial agency should have processes that allow the enquirer to capture and store the information they used to verify identity.

~~5.34~~6.46 It is important that the process of electronic verification meets a standard level of confirmation before it can be relied on. The standard level of confirmation, in circumstances that do not give rise to concern or uncertainty, is:

- one match on an individual's full name and current address, and
- a second match on an individual's full name and either his current address or his date of birth.

~~5.35~~6.47 Commercial agencies that provide electronic verification use various methods of displaying results – for example, by the number of documents checked, or through scoring mechanisms. Operators should ensure that they understand the basis of the system they use, in order to be satisfied that the sources of the underlying data meet the required standard.

Documentary evidence

~~5.36~~6.48 If verification is undertaken using documents, casino operators should usually rely upon documents issued by government departments.

~~5.37~~6.49 Original documents should be examined so that, as far as reasonably practicable, forgeries are not accepted. Casino operators should recognise that some documents are more easily forged than others. If suspicions are raised in relation to any document offered, operators should take whatever practical and proportionate steps are available to establish whether the document offered is a forgery or has been reported as lost or stolen. While the presentation of false documents does not, in itself, amount to money laundering, it may constitute an offence under the Fraud Act 2006 or Identity Cards Act 2006 and should, in appropriate circumstances, be reported to the police or the ~~SOCA~~ **NCA**. Casino operators should also be aware that even if documents appear to be legitimate and issued by a government department they may be false, for example, the European ~~d~~**D**riving ~~p~~**P**ermit**, International Drivers License and National Identity Card, which are** ~~that is~~ freely available through the internet **but are fake**. Commercial software is available that checks the algorithms used to generate passport numbers. This can be used to check the validity of passports of any country that issues machine-readable passports.

~~5.38~~6.50 If documents are in a foreign language appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity, for example, a translation of the relevant sections.

~~5.39~~6.51 Documentation purporting to offer evidence of identity may emanate from a number of sources. These documents differ in their integrity, reliability and independence. Some are issued after CDD on the holder of the document is carried out by the issuing authority. There is a broad hierarchy of documents.

~~5.40~~6.52 Documents issued by government departments and agencies that contain a photograph may be considered reliable. In practical terms, for face-to-face verification conducted by non-remote casinos, production of a valid passport or photocard driving licence should enable most individuals to meet the identification requirement for AML/CTF purposes. These documents will also confirm either residential address or date of birth.

~~5.41~~6.53 Alternatively government issued documents without a photograph may be used which incorporates the customer's full name, supported by a second document, which is ideally also government issued, or issued by a public sector body or authority. This second document must also include the customer's full name and either his residential address or his date of birth.

~~5.42~~6.54 The following sources may, therefore, be useful for verification of UK-based customers:

- current signed passport
- birth certificate
- current photocard driving licence
- current EEA member state identity card
- current identity card issued by the Electoral Office for Northern Ireland
- residence permit issued by the Home Office
- firearms certificate or shotgun licence
- benefit book or original notification letter from the Department of Works and Pensions confirming the right to benefits
- council tax bill

- utility bill or statement (but not ones printed off the internet), or a certificate from a utilities supplier confirming an arrangement to pay services on pre-payment terms
- bank, building society or credit union statement or passbook containing current address (but not statements printed off the internet) - bank or credit cards alone will not be sufficient as these do not provide either residential address or date of birth
- confirmation from an electoral register that a person of that name lives at that address
- recent original mortgage statement from a recognised lender
- solicitor's letter confirming recent house purchase or land registry confirmation of address
- local council or housing association rent card or tenancy agreement
- HM Revenue and Customs (HMRC) self-assessment statement or tax demand
- house or motor insurance certificate.

~~5.43~~6.55 Customers who are not resident in the UK should be asked to produce their passport, national identity card or photocard driving licence. If the casino has concerns that the identity document presented by a customer is not genuine, they should contact the relevant embassy or consulate. Confirmation of the customer's address can be obtained from:

- an official overseas government source
- a reputable directory of addresses
- a person regulated for money laundering purposes in the country where the customer is resident (for example, a casino or bank) who confirms that the customer is known to them and lives or works at the overseas address supplied.

~~5.44~~6.56 Non-remote casinos have adopted the practice of photographing new customers on their first visit to the casino as part of the CDD records. Doing so assists with casino security issues and with customer tracking. It is a matter for each casino operator, but the Commission views the use of customer photographs as good practice in the casino environment that contributes to the prevention and detection of money laundering and terrorist financing.

Politically exposed persons

Definition

~~5.45~~6.57 A PEP is a person who is or has, at any time in the preceding year, been entrusted with prominent public functions by a state outside the UK, a Community institution (for example, the European Parliament) or an international body (for example, the United Nations), including the following persons:

- heads of state, heads of government, ministers and deputy or assistant ministers
- members of parliament
- members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exception circumstances
- members of courts of auditors or of the boards of central banks
- ambassadors, charge d'affairs and high ranking officers in armed forces
- members of the administrative, management or supervisory bodies of state-owned enterprises.[49]

The following persons are also regarded as PEPs by virtue of their relationship or association with the persons listed above:

- family members of the persons listed above, including spouse, partner, children and their spouses or partners, and parents
- known close associates of the persons listed above, including persons with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relationships, or who is a sole beneficial owner of a legal entity or arrangement set up by the PEP with whom they are associated.

[49] Regulation 14(5) and Schedule 2

PEP status itself does not incriminate individuals or entities. It does, however, put a customer into a higher risk category.

Risk-based approach to PEPs

~~5.46~~6.58 The nature and scope of a particular casino's business will help to determine the likelihood of PEPs in their customer base, and whether the operator needs to consider screening all customers for this purpose.

~~5.47~~6.59 Establishing whether individuals are PEPs is not always straightforward and can present difficulties. Where operators need to carry out specific checks, they may be able to rely on an internet search~~engine,~~ or consult relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations. Resources such as the Transparency International Corruption Perceptions Index, which ranks approximately 150 countries according to their perceived level of corruption, may be helpful in assessing the risk. This can be found at www.transparency.org/policy_research/surveys_indices/cpi. **Another useful source of information is** www.knowyourcountry.com**.** If there is a need to conduct more thorough checks, or if there is a high likelihood of an operator having PEPs for customers, subscription to a specialist PEP database may be a valuable tool in assessing the risk.

~~5.48~~6.60 New and existing customers may not initially meet the definition of a PEP, but that position may change over time. Equally, individuals who are initially identified as PEPs may cease to be PEPs, for example, a year after they change their job or retire. The operator should, as far as practicable, be alert to public information relating to possible changes in the status of its customers with regard to political exposure. Casino operators should be alert to situations which suggest that the customer is a PEP. These situations include:

- receiving funds from a government account
- correspondence on an official letterhead from the customer or a related person
- general conversation with the customer or related person linking the person to a PEP
- news reports suggesting that **the** ~~your~~ **customer** ~~client~~ is a PEP or is linked to one.

~~5.49~~6.61 Although under the definition of a PEP an individual ceases to be so regarded after he has left office for one year, operators are encouraged to apply a risk-based approach in determining whether or when they should cease carrying out appropriately enhanced monitoring of transactions. In many cases, a longer period might be appropriate, in order to ensure that the higher risks associated with the individual's previous position have adequately abated.

~~5.50~~6.62 Each operator's policies and procedures should cover when and how customers will be checked for PEP status.

PEPs requirements

~~5.31~~6.63 An operator who proposes to allow a PEP to be a customer must:

- have approval from its senior management for establishing a business relationship with that person;
- take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship; and
- where a business relation is entered into, conduct enhanced ongoing monitoring of the relationship.

~~5.52~~6.64 Each operator's policies and procedures should cover how and when senior management approval will be sought and provided, and deal with how the customer will be dealt with if there is any delay to approval being provided.

Failure to complete CDD checks

~~5.53~~6.65 Where a casino operator is unable to comply with the required CDD measures in relation to a customer, the operator:

- must not carry out a transaction with or for the customer through a bank account;
- must not establish a business relationship or carry out an occasional transaction with the customer;
- must terminate any existing business relationship with the customer; and
- must consider making a report to **the** ~~SOCA~~ **NCA**.[50]

~~5.54~~6.66 Casinos must therefore have clear policies in place on how they will manage situations where they are unable to comply with the CDD measures.

Requirements for remote casinos

~~5.55~~6.67 In the light of the requirements imposed by regulation 11, where remote casinos use the threshold approach to CDD, they should adopt the following procedure:

- at the point **where the threshold** ~~that verification~~ is **reached** ~~triggered~~, operators should put all monies owed to the customer into an account (or equivalent) from which no withdrawals can be made
- further deposits can be made to that account as long as they too are locked into it until CDD is completed
- bets can be made from the account, again providing any winnings are locked until CDD is completed
- once CDD is completed, the account can be unlocked and business continue as normal
- if it cannot be completed, then the operator must proceed in line with regulation 11(1) and terminate the business relationship with the customer
- if monies are to be repaid, then the amount repaid should consist of all monies owed to the customer at the point that the **threshold** ~~verification procedure~~ was **reached** ~~triggered~~, plus all deposits made at that point and thereafter
- money should be refunded back to the originating account, and:
    - there should be appropriate risk mitigation
    - where appropriate, operators should submit SARs or seek appropriate consent
- if the refund is to be completed back to another account (whether partially or completely):
    - risk assessment must be done that should take into account information such as:
        - multiple destinations – is the customer requesting that the money be sent to several bank accounts?
        - high risk destination – is the customer requesting that the money be returned to a country where there is a significant money laundering concern?
        - above €2000 – is the amount above the threshold for CDD?
    - there should be appropriate risk mitigation
    - where appropriate, operators should submit SARs or seek appropriate consent
- there should be ongoing monitoring of the account and, if necessary, reporting of findings via services such as CIFAS (the UK's Fraud Prevention Service).

~~5.56~~6.68 The customer should be made fully aware of the procedures adopted by the operator when they first register so that there is no misunderstanding at a later stage.

6.69 Remote casino operators should also consider the requirements for enhanced customer due diligence discussed in paragraphs 2.36 to 2.41.

[50] Regulation 11.

~~Existing customers~~

~~5.57 Where the identity of an existing customer has already been established to the standards agreed following the 2003 Regulations then there is no need to undertake CDD to the new standards until the customer enters a casino again, or reaches a CDD threshold, depending on the CDD model in use by the operator.~~

List of persons subject to financial sanctions

~~5.58~~6.70 The UK operates financial sanctions on persons and entities following their designation at the United Nations and/or European Union. The UK also operates a domestic counter-terrorism regime, where the Government decides to impose financial restrictions on certain persons and entities. There are specific financial restrictions targeted at the Al-Qaida network, ~~and~~terrorism **and terrorist financing**.

~~5.59~~6.71 Financial restrictions in the UK are governed by various pieces of legislation. The purpose of imposing financial restrictions is to restrict the access to finance by designated persons and to prevent the diversion of funds to terrorism and terrorist purposes. In all circumstances, where an asset freeze is imposed, it is unlawful to make payments to or allow payments to be made to designated persons.

~~5.60~~6.72 A list of all financial restrictions currently in force in the UK is maintained by ~~the~~ **HM** Treasury's Asset Freezing Unit. The Consolidated List of persons designated as being subject to financial restrictions can be found on the **government** ~~HM Treasury~~ web site at: https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets ~~www.hm-treasury.gov.uk/financialsanctions~~. Further information on financial restrictions can also be found via this website. The purpose of the HM Treasury list is to draw together, in one place, all the names of designated persons for the various financial restrictions regimes effective in the UK.

~~5.61~~6.73 Under the relevant legislation, it is a criminal offence for any natural or legal person to:

- deal with the funds of designated persons;
- make funds and economic resources, and in the case of terrorism financial services, available, directly or indirectly to or for the benefit of designated persons; or
- knowingly and intentionally participate in activities that would directly or indirectly circumvent the financial restrictions or enable or facilitate the commission of an offence relating to the above.

~~5.62~~6.74 In this context, 'deal with' means:

- in respect of funds, to use, alter, move, allow access to or transfer;
- in respect of funds, deal with in any other way that would result in any change in volume, amount, location, ownership, possession, character or destination; or
- in respect of funds, make any other change that would enable use, including portfolio management; and
- in respect of economic resources, to use to obtain funds, goods or services in any way, including (but not limited to) by selling, hiring or mortgaging the resources.

~~5.63~~6.75 HM Treasury has the power to grant licences exempting certain transactions from the financial restrictions. Requests to disapply the financial restrictions in relation to a designated person are considered by the Treasury on a case-by-case basis to ensure that there is no risk of funds being diverted to otherwise restricted purposes. To apply for a licence, the Asset Freezing Unit at HM Treasury can be contacted using the contact details provided below.

~~5.64~~6.76 Operators need to have the necessary policies and procedures in place to monitor financial transactions so that payments are not made to designated persons, thereby preventing breaches of the financial restrictions legislation. For manual checking, operators

can register with the HM Treasury Asset Freezing Unit update service (directly or via a third party). If checking is automated, operators will need to ensure that the relevant software includes checks against the latest Consolidated List.

~~5.65~~6.77 The Asset Freezing Unit may also be contacted to provide guidance and to assist with any concerns regarding financial restrictions at:

Asset Freezing Unit
Tel: 020 7270 5664/5454
Fax: 020 7451 7677
Email: assetfreezingunit@hmtreasury.gsi.gov.uk

~~5.66~~6.78 In the event that a customer or a payee is identified as a designated person, payments must not proceed unless a licence is granted by the Treasury, as this would be a breach of the financial restrictions. The Treasury should be informed immediately and the transaction suspended pending their advice. No funds should be returned to the designated person. The ~~firm~~ **operator** may also need to consider whether there is an obligation also to report to **the NCA** ~~SOCA~~ under POCA or the Terrorism Act.

~~5.67~~6.79 Written reports can be made to the Asset Freezing Unit via email.

~~6~~7 Record keeping

General legal and regulatory requirements

~~6~~7.1 This chapter provides guidance on appropriate record keeping procedures required by the Regulations. The purpose of the record keeping requirement is to ensure that there is an audit trail that could assist in any financial investigation by a law enforcement body. **These records are also important when the Commission is conducting an investigation for compliance purposes.**

~~6~~7.2 The operator's record keeping policy and procedure should cover records in the following areas:

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

7.3 The policy and procedure for record-keeping should also make provision for the retention of records held by an employee who leaves the business.

~~6.3~~7.4 The record keeping requirements for supporting records, that is, the records of ongoing transactions with a customer, are based on the nature of the relationship with that customer. There is either:

- no relationship;
- a 'business relationship', depending on the circumstances; or
- an 'occasional transaction'.

Business relationships

6.47.5 Casino operators form business relationships with their customers if, at the point that contact is established, the casino expects their relationship to have an element of duration. Casino operators are encouraged to interpret this definition widely.

6.57.6 ~~C~~**As discussed in paragraph 3.9, c**asinos **will, therefore,** ~~are likely to~~ form a business relationship when:

- the casino starts tracking a customer's drop/win figures;
- a customer opens an account with the operator or joins a membership scheme; or
- a customer obtains a cheque cashing facility.

6.67.7 Ongoing monitoring of business relationships is a requirement for casino operators and includes scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, his business and risk profile.[51]

6.77.8 ~~C~~**As noted in paragraph 6.9, c**asinos are expected to approach this requirement on a risk basis. Dependent on how frequently a casino forms 'business relationships' it may be good practice to apply ongoing monitoring more widely. Regular players should be the subject of closer scrutiny and their level of play should be assessed with reference to the information already known about them, and where necessary, additional information must be collected and retained about the source of their funds.

Occasional transaction

6.87.9 A casino may undertake an occasional transaction with a customer when there is no business relationship but the customer purchases or exchanges chips over €15,000 in value. For example, a customer on a single visit to a casino while on holiday or a business trip who purchases or exchanges chips over the €15,000 limit constitutes an 'occasional transaction'. CDD will need to be done under these circumstances and the casino will have to retain the supporting records, that is, the drop/win data, for five years after the date of the visit.

Other casino customers

6.107.10 Some casino customers may not fall into the business relationship or occasional transaction definitions. For example, customers spending low amounts at gaming during single, infrequent and irregular visits to a casino and who are not subject to tracking. There may be no expectation at any stage that there will be any duration to the relationship with the customer. Strictly speaking such business falls outside of the record-keeping requirements, **however, the Commission nonetheless considers it to be good practice to retain such records**.

Customer information

6.117.11 In relation to the evidence of a customer's identity, operators must keep a copy of, or the references to, the verification evidence of the customer's identity obtained during the application of CDD measures.[52]

6.127.12 An operator may often hold additional information beyond identity in respect of a customer for the purposes of wider **CDD** ~~customer due diligence~~. As a matter of best practice this information and any relevant documents should also be retained.

[51] Regulation 8(1)
[52] Regulation 19(2).

~~6.13~~7.13 There is a separate requirement in the Regulations to ensure that documents, data or information held by casinos are kept up to date.[53] A trigger event for refreshing and extending CDD may be if a customer returns to a casino after a period of non-attendance. Refreshing information about existing customers will ensure that matters such as change of address, or a customer being appointed into a role which attracts PEP status, will be picked up. Keeping information up to date is also a requirement under the Data Protection Act. How these issues which will be dealt with in practice should be covered in the casino's policies and procedures.

~~6.14~~7.14 Where documents verifying the identity of a customer are held in one casino premises they do not also need to be held in duplicate form in another premises in the same group. For the purposes of compliance with the Regulations the whole group forms part of the same 'relevant person'. The records need to be accessible to all premises that have contact with the customer, the nominated officer and law enforcement. The Regulations accept that operators may have more than one casino premises or more than one remote casino site. It is sufficient for the operator to undertake identification and verification providing that the information is available to each premises or site.

Supporting records – non-remote casinos

~~6.15~~7.15 The requirement to keep supporting records is linked to 'business relationships' and 'occasional transactions' which are defined in the Regulations[54] and the extent and nature of records created. In many casinos customers, regardless of whether or not they have formed a business relationship, or are part of an occasional transaction, purchase chips with cash at the gaming tables where, in low risk situations, no records are created and therefore not available to be kept.

~~6.16~~7.16 The Commission expects casino operators to use reasonable endeavours to create and keep supporting records and to make it clear in their policies and procedures what records will be created in light of the known spending patterns and the assessed money laundering and terrorist financing risks at each premises.

~~6.17~~7.17 ~~C~~**Some c**asinos ~~currently~~ undertake a process at the end of each business day to count the total drop (cash used to purchase chips) to compare against the total amount recorded through tracking individual customer spending. The difference between the two figures is the amount of drop that is not attributable to particular customers. This in turn can be calculated against known attendance figures and the number of customers tracked to give an average amount of money used to purchase chips per customer that has not been tracked, and therefore with no supporting records. This process should **be the subject of** ~~continue and should form part of the~~ ongoing risk assessment for each premises. The records created during this process should **also** be retained.

~~6.18~~7.18 Any casino operator devising its record keeping policy and procedure should decide how its business fits within the definitions of 'business relationship' or 'occasional transaction'. The variation in the record-keeping requirements for different circumstances illustrates the flexibility available to casinos which allows them to focus their resources on higher money laundering risk situations.

~~6.19~~7.19 For the purposes of supporting records, the Commission takes the view that in most cases this will consist of records covering the drop/win figures, subject to paragraph ~~6.9~~**7.10**, for each customer for each 24 hour period. There is no requirement to keep detailed records for each customer for each table or game for AML purposes. However, HMRC may require operators to maintain records for each table or game, but not broken down by each customer's transactions.

[53] Regulation 8(2)(b).
[54] Regulation 2(1).

Supporting records – remote casinos

~~6.19~~7.20 Remote casinos will, by the nature of their business, generate detailed records of all transactions with each customer but for the purposes of the record keeping requirements it is sufficient to retain the drop/win figures for each named customer for each 24 hour period.

Supporting records – gaming machines

~~6.20~~7.21 Cash-in with cash-out gaming machines do not produce any supporting records that can be attributed to a customer. They do generate overall cash-in and cash-out data that must be retained by the casino. However, 'ticket in, ticket out' (TITO) and 'smart card' technology may mean that ~~in the future,~~ machines produce supporting records that can be attributed to a customer who falls within the record keeping requirements, in which case such records must be retained in accordance with the Regulations.

~~6.21~~7.22 The essentials of any system of monitoring are that:

- it flags up transactions and/or activities for further examination;
- these reports are reviewed promptly by the nominated officer; and
- appropriate action is taken on the findings of any further examination.

~~6.22~~7.23 Monitoring can be either:

- in real time, in that transactions and/or activities can be reviewed as they take place or are about to take place; or
- after the event, through the nominated officer's review of the transactions and/or activities that a customer has undertaken.

In either case, unusual transactions or activities should be flagged for further examination.

~~6.23~~7.24 In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer risk.

~~6.24~~7.25 Monitoring is not a mechanical process and does not necessarily require sophisticated electronic systems. The scope and complexity of the process will be influenced by the operator's business activities, and whether the operator is large or small. The key elements of any system are having up-to-date customer information, on the basis of which it will be possible to spot the unusual, and asking pertinent questions to elicit the reasons for unusual transactions or activities in order to judge whether they may represent something suspicious.

Retention period

~~6.25~~7.26 Records of identification and verification of customers must be kept for a period of at least five years after the relationship with the customer has ended.[55] The date the relationship with the customer ends is the last date on which they visit or use a casino.

~~6.26~~7.27 Supporting records must be retained for a period of five years beginning on the date any transaction is completed where the records relate to a particular transaction. This creates a rolling five year history of drop/win data. Records of internal and external reports on suspicious activity should be retained for five years from when the report was made.[56]

Form in which records are ~~have~~ to be kept

~~6.27~~7.28 Most operators have record keeping procedures which they keep under review, and will seek to reduce the volume and density of records which have to be stored, whilst still complying with statutory requirements. Retention may therefore be:

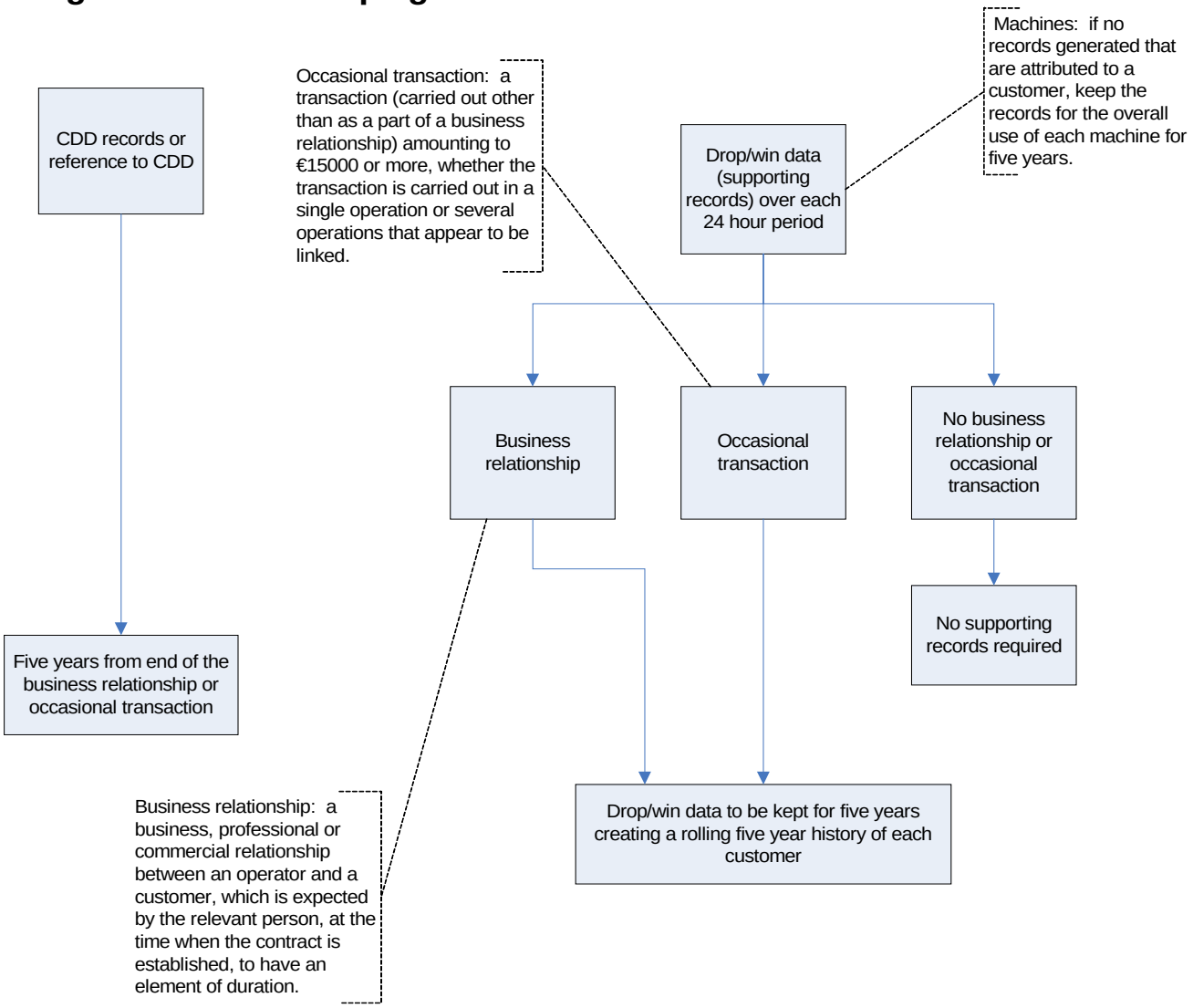
[55] Regulation 19(3).
[56] Regulation 19(3).

- by way of original documents;
- by way of photocopies of original documents;
- on micro**film** ~~fiche~~;
- in scanned form; or
- in computerised or electronic form.

~~6.28~~7.29 Records relating to ongoing investigations should, where possible, be retained until the relevant law enforcement agency has confirmed that the case has been concluded.

~~6.30~~7.30 Where the record keeping obligations under the Regulations are not observed, an operator or person is open to prosecution and sanctions, including imprisonment for up to two years and/or a fine, or regulatory censure.

Figure 6: Record keeping



Note:
Operators should devise and implement a clear and articulated policy and procedure for ensuring all relevant employees are aware of their legal obligations in respect of the prevention of money laundering and terrorist financing.

~~7~~8 Suspicious activities and reporting

Introduction

~~7~~8.1 Employees in casinos are required to make a report in respect of information that comes to them within the course of their business:

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

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

~~7~~8.2 In order to provide a framework within which suspicion reports may be raised and considered:

- each operator must ensure that any employee reports to the operator's nominated officer where they have grounds for knowledge or suspicion that a person or customer is engaged in money laundering or terrorist financing;
- the operator's nominated officer must consider each such report, and determine whether it gives grounds for knowledge or suspicion;
- operators should ensure that employees are appropriately trained in their obligations, and in the requirements for making reports to their nominated officer.

~~7~~8.3 If the nominated officer determines that a report does give rise to grounds for knowledge or suspicion, he must report the matter to **the NCA** ~~SOCA~~. Under POCA, the nominated officer is required to make a report to **the NCA** ~~SOCA~~ as soon as is practicable if he has grounds for suspicion that another person, whether or not a customer, is engaged in money laundering. Under the Terrorism Act, similar conditions apply in relation to disclosure where there are grounds for suspicion of terrorist financing.

What is meant by knowledge and suspicion?

~~7~~8.4 **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. ~~That said,~~ ~~k~~**K**nowledge 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[57]. The knowledge must, however, have come to the operator (or to the employee) in the course of casino business or (in the case of a nominated officer) as a consequence of a disclosure under section 330 of POCA. Information that comes to the operator or employee in other circumstances does not come within the scope of the regulated sector obligation to make a report. This does not preclude a report being made should employees choose to do so. Employees may also be obliged to make a report by other parts of the Act. **Further information can be found in Part 7 of POCA[58].**

~~7~~8.5 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 grounded 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.

[57] Refer to *Baden v Societe Generale pour Favouriser le Developpement du Commerce et de l'Industrie en France* [1983] BCLC 325
[58] Part 7 of POCA

~~7~~8.6 Whether you hold suspicion or not is a subjective test. If you think a transaction is suspicious you are not **required** ~~expected~~ to know the exact nature of the criminal offence or that particular funds are definitely those arising from the crime. You may have noticed something unusual or unexpected and, after making enquiries, the facts do not seem normal or make commercial sense. You do not need to have evidence that money laundering is taking place to have suspicion.

8.7 **A transaction that appears to be unusual is not necessarily suspicious. Many customers will, for perfectly legitimate reasons, have an erratic pattern of gambling transactions or account activity. Even customers with a steady and predictable gambling profile will have periodic transactions that are unusual for them. So an unusual transaction may only be the basis for further enquiry, which may in turn require judgement as to whether the transaction or activity is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report the activity then arises. Likewise, if concern escalates following further enquiries, it is reasonable to conclude that the transaction is suspicious and make a report to the NCA.**

~~7.7~~8.8 Unusual patterns of gambling, including the spending of particularly large amounts of money in relation to the casino or customer's profile, should receive attention, but unusual behaviour should not necessarily lead to grounds for knowledge or suspicion of money laundering, or the making of a report to **the NCA** ~~SOCA~~. The nominated officer is required to assess all of the circumstances and, in some cases, it may be helpful to ask the customer or others more questions. The choice depends on what is already known about the customer and the transaction, and how easy it is to make enquiries.

~~7.8~~8.9 In order for either an internal or external report 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**.

What is meant by reasonable grounds to know or suspect?

~~7.9~~8.10 In addition to establishing a criminal offence relating to when suspicion or actual knowledge of money laundering, POCA creates criminal liability for failing to disclose information when reasonable grounds exist for knowing or suspecting that a person is engaged in money laundering or terrorist financing. This lower test, which introduces an *objective* test of suspicion, applies to all businesses covered by the Regulations, including remote and non-remote casinos. The test would likely be met when there are demonstrated to be facts or circumstances, known to the employee in the course of business, from which a reasonable person engaged in a casino business would have inferred knowledge, or formed a suspicion, that another person was engaged in money laundering or terrorist financing.

~~7.10~~8.11 To defend themselves against a charge that they failed to make a report when the objective test of suspicion has been satisfied, employees within remote and non-remote casinos would need to be able to demonstrate that they took reasonable steps in the particular circumstances (and in the context of a risk-based approach) to conduct the appropriate level of CDD. It is important to bear in mind that, in practice, a court will be deciding, with the benefit of hindsight, whether the objective test was met.

Figure 7: Reasonable grounds to suspect (objective test)

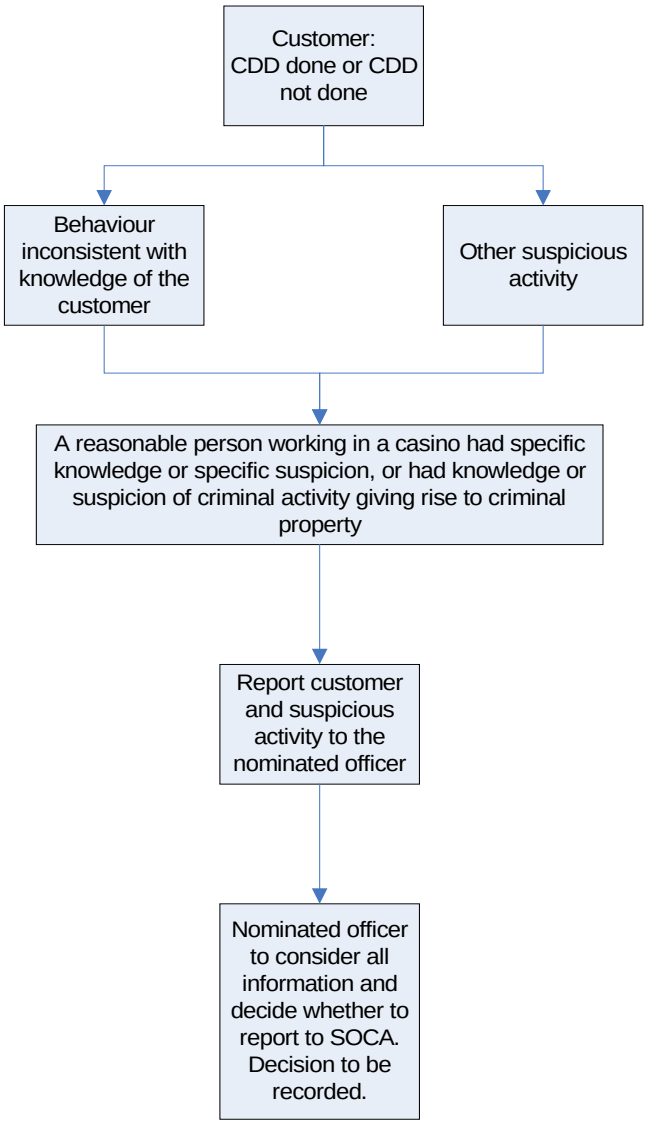
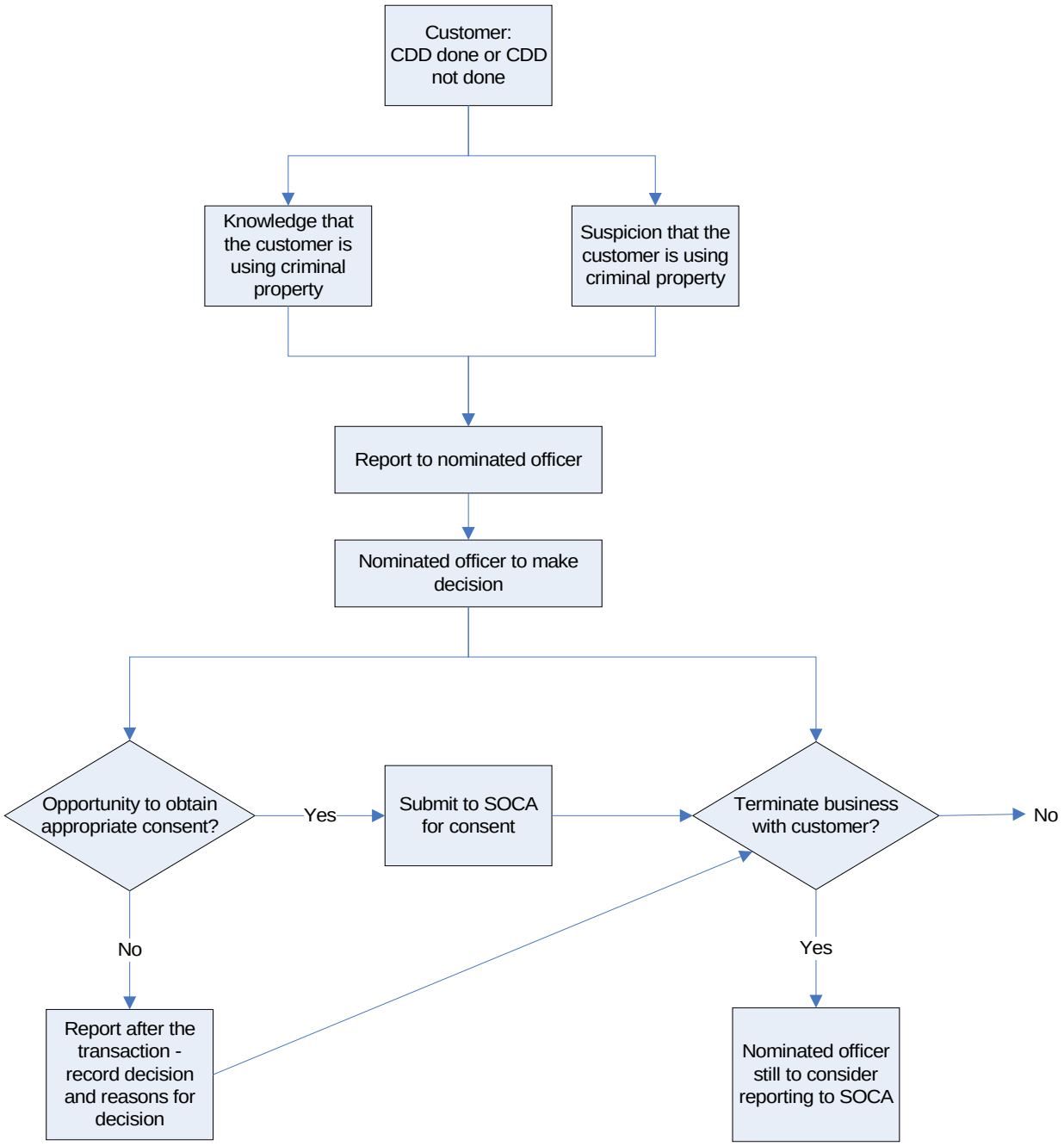


Figure 8: Knowledge or suspicion of money laundering or terrorist financing (subjective test)



What constitutes suspicious activity?

8.12 **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 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 (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. The customer could be laundering money in a way that guarantees minimal loss.**
- **A customer gambles with significant amounts of money in a currency without a reasonable explanation for the source of that currency, such as Scottish and Northern Irish banknotes presented by a customer in an English casino.**
- **Instances of high spend by customers that lead to significant commercial risk for the operator may also indicate suspicious activity.**

8.13 **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, table games), it is good practice to monitor the customer's activity in other areas of the business (for example, gaming machine play).**

Internal reporting

~~7.11~~8.14 Employees of a casino operator **have** ~~obtain~~ a legal defence if they report to the nominated officer where they have grounds for knowledge or suspicion. All casino operators therefore need to ensure that all relevant employees know they should report suspicions to their nominated officer. Internal reports to a nominated officer, and reports made by a nominated officer to **the NCA** ~~SOCA~~, must be made as soon as possible.

~~7.12~~8.15 All suspicions reported to the nominated officer should be documented or electronically recorded. The report should include full details of the customer who is the subject of concern and as full a statement as possible of the information giving rise to the grounds for knowledge or suspicion **of money laundering**. All internal enquiries made in relation to the report should also be documented or electronically recorded. This information may be required to supplement the initial report or as evidence of good practice and best endeavours if, at some future date, there is an investigation **by a law enforcement agency or the Commission**.

~~7.13~~8.16 Once an employee has reported his suspicion to the nominated officer, or to an individual to whom the nominated officer has delegated the responsibility to receive such internal reports, he has fully satisfied his statutory obligation.

Evaluation and determination by the nominated officer

~~7.14~~8.17 The operator's nominated officer must consider each report and determine whether it gives rise to grounds for knowledge or suspicion. The operator must permit the nominated officer to have access to any information, including CDD information, in the operator's possession that could be relevant. The nominated officer may also require further information to be obtained, from the customer if necessary. Any approach to the customer should be made sensitively and probably by someone already known to the customer, to minimise the risk of alerting the customer or an intermediary that a disclosure to **the NCA** ~~SOCA~~ is being considered.

~~7.15~~8.18 If the nominated officer decides not to make a report to **the NCA** ~~SOCA~~, the reasons for not doing so should be clearly documented or electronically recorded, and retained. These records should be kept separately by the nominated officer in order that the information therein is not disclosed accidently.

8.19 **It should be noted that the submission of a report to the NCA is not intended to be used as a way to obtain information from law enforcement in order to assist the nominated officer in deciding whether to continue with the business relationship with the customer, nor should the absence of a response or feedback from the NCA to be taken to imply that the operator should continue with the business relationship until adverse information about the customer is received from the NCA or other law enforcement agency.**

External reporting

~~7.16~~8.20 To avoid committing a failure to report offence, the nominated officer must make a disclosure to **the NCA** ~~SOCA~~ where he decides that a report gives rise to grounds for knowledge or suspicion. The national reception point for the disclosure of suspicions, and

for seeking consent to continue to proceed with the transaction or activity, is the UK Financial Intelligence Unit (UKFIU) within **the NCA** ~~SOCA~~.

~~7.17~~8.21 The nominated officer must report to **the NCA** ~~SOCA~~ any transaction or activity that, after his evaluation, he knows or suspects, or has reasonable grounds to know or suspect, may be linked to money laundering. Such reports must be made as soon as is reasonably practicable after the information comes to the nominated officer.

8.22 **In addition, depending on the circumstances, an operator being served with a court order in relation to a customer may have cause for suspicion, or reasonable grounds for suspicion, in relation to that customer. In such an event, the nominated should review the information that is held about that customer in order to determine whether or not such grounds for suspicion exist, and if necessary make a report to the NCA. Where the nominated officer decides not to make a report to the NCA, the reasons for not doing so should be clearly recorded and retained.**

~~7.18~~8.23 The Secretary of State may by order prescribe the form and manner in which a disclosure under section 330, section 331, section 332, or section 338, may be made. A consultation paper on the form and manner of reporting was issued by the Home Office in the summer of 2007, however, the Home Office decided not to proceed with the introduction of a prescribed form and manner for reporting.

Submission of suspicious activity reports

~~7.19~~8.24 **The NCA** ~~SOCA~~ accepts the submission of SARs in three main ways:

- ~~**Paper based reporting** using the standard SOCA Suspicious Activity Report Form. SOCA prefers submissions to be typed to enable it to be scanned and prevent errors in data entry. The form and guidance on using the form can be found on the SOCA website ().~~

  ~~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.~~

- **SAR Online, which** is a secure web-based reporting system for small or medium sized reporting entities with access to the internet, which allows SARs to be submitted electronically through 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** ~~SOCA~~'s preferred method for small and medium sized report**ing entities**~~ers~~ to submit SARs. The benefit to the reporter is 24/7 reporting, an automatic acknowledgment of receipt with the ELMER reference number, 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 it to be scanned and prevent**

errors in data entry. The form and guidance on using the form can be found on the NCA website.

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.

- **Encrypted bulk data exchange**, is used by high volume reporters, that is reporters with more than 10,000 reports a month. If an operator believes this would be the most appropriate method of reporting for their group, contact the UKFIU on 0207 238 8282 to discuss the **matter**~~issue~~.

~~7.2~~8.25 Operators should include in each SAR as much relevant information about the customer, transaction or activity that it has in its records. **The NCA** ~~SOCA~~ has **published** a ~~published document to assist in the effective reporting of suspicious activity. A SAR~~ glossary of terms ~~is also available~~ which **they** ~~SOCA~~ prefer operators to use when completing SARs. ~~These are available on SOCA's website~~ ~~and~~ **This** will assist in consideration of the report by **the NCA** ~~SOCA~~.

8.26 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 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 casino gaming, but also uses online gambling facilities)?**

~~7.2~~8.27 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.

Appropriate consent

~~7.2~~8.28 If operators handle any proceeds of crime they may commit one of the principal money laundering offences in POCA or the Terrorism Act. However, if the nominated officer **submits**~~makes~~ a **SAR**~~report~~ to **the NCA** ~~SOCA~~ this can **provide** ~~amount to~~ a defence. The**re is** ~~'reporting defence' includes the~~ **a** statutory mechanism which allows **the NCA** ~~SOCA~~ either to **grant or refuse** ~~agree to~~ the **'prohibited act'** ~~transaction~~ going ahead, or to prevent the suspected money laundering going ahead[59]**.** This statutory mechanism is called 'appropriate consent'.

8.29 The decision whether or not to obtain appropriate consent will arise in the following scenarios:

- **concealing, disguising, converting, transferring or removing criminal property[60]**
- **facilitating the acquisition, retention, use or control of criminal property by, or on behalf of, another person[61]**

[59] Section 335 of POCA
[60] Section 327 of POCA

- **acquisition, use or possession of criminal property**[62]**.**

These are referred to as 'prohibited acts'.

8.30 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.

~~7.23~~8.31 The nominated officer needs to consider how he will approach his 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**.

~~7.24~~8.32 A nominated officer, police constable, ~~SOCA~~ **NCA** employee or customs officer can give a person (which may include, for example, a casino employee) *actual* 'appropriate consent' to a suspect transaction proceeding.[63] However, it should be noted that **the NCA** ~~SOCA~~ is the only body able to issue formal notification of consent by means of an official ~~SOCA~~ **NCA** letter, which the nominated officer can then retain for his records.

~~7.25~~8.33 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.[64]

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 paragraphs 8.43 to 8.53 for more detail.

~~7.26~~8.34 However, **POCA** ~~the Act~~ 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** ~~SOCA~~ and, either:

- the **NCA** ~~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' (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.[65]

~~7.27~~8.35 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.[66] Where a customer **request** ~~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** ~~are grounds for~~ knowledge or suspicion, **or**

---

[61] Section 328 of POCA
[62] Section 329 of POCA
[63] Section 335(1) of POCA
[64] Section 335(2) of POCA
[65] Section 336 of POCA
[66] Section 327(2)(b) of POCA

reasonable grounds for suspicion, that the transaction, arrangements, or the funds/property involved, may relate to money laundering, a **SAR**~~report~~ must be **submitted**~~made~~ to **the NCA** ~~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 from the working day following the date of disclosure, unless **the NCA** ~~SOCA~~ gives consent.[67]

8.36 The consent provisions can only apply where there is prior notice to the NCA of the transaction or activity. The NCA cannot provide consent after the transaction or activity has occurred. A consent request which is received after the transaction or activity has taken place will therefore be dealt with as an ordinary SAR.

~~7.28~~8.37 In the casino environment, 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.**~~and i~~ **In these** circumstances **it may sometimes**~~where it is~~ not **be** feasible **or practical** to obtain appropriate consent prior to or during a transaction. ~~Grounds for k~~**K**nowledge or suspicion **of money laundering** may be triggered after a customer has completed **all the** ~~the three~~ stages of a gambling transaction; that is, they have bought in, they have played and they have cashed out. Under th~~e~~**o**se circumstances, it **may** ~~would~~ be reasonable to report after the transaction. However, the defence of 'reasonable excuse' when reporting after the transaction is untested by case law and **should** ~~would need to~~ be considered on a case-by-case basis.[68] **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**.

~~7.29~~8.38 Casinos should include in their policies and procedures details on how they will manage circumstances where there is ~~grounds for~~ knowledge or suspicion of money laundering or terrorist financing. If knowledge or suspicion is present, **particularly if this occurs out of normal office hours**, ~~then~~ there must be a mechanism for involvement of the senior manager on duty and contact with the nominated officer as soon as is practicable. If the circumstances amount to reasonable grounds to suspect, then reporting the matter to the nominated officer should be sufficient, and for the nominated officer to receive the matter at the earliest practicable opportunity.

~~7.30~~8.39 The nominated officer will need to think very carefully about whether or not ~~he wishes~~ to continue to do business with the suspected customer. Relevant considerations should be the potential commission of criminal offences under POCA or the Terrorism Act, as well as potential damage to **business** reputation and other commercial factors.

~~7.31~~8.40 Operators should also note that in the Commission's view 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**n** ~~steadily~~ increasing level of suspicion of money laundering, or ~~even~~ to actual knowledge of money laundering, operators **must** ~~will no doubt~~ seriously consider whether they wish to allow the customer to continue using their gam**bli**ng facilities. Operators are, of course, free to terminate their business relationships if they wish, and provided this is handled **appropriately** ~~sensitively~~ there will be no risk of 'tipping off' **or 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** ~~if the decision has been made to terminate gaming facilities and there is a remaining suspicion of money laundering/terrorist financing with funds to repatriate, consideration should be given to asking for appropriate consent.~~

[67] Section 336(3) and (4) of POCA
[68] Section 327(2)(b) of POCA

~~7.32~~8.41 How customers suspected of money laundering will be dealt with is an important area of risk management for all operators. Casinos should deal with the issue in their policies and procedures under the Regulations 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.

~~7.33~~8.42 ~~Although~~ **For example, the operator may consider** one transaction ~~may~~ **to** be suspicious and ~~be~~ report~~sed~~ as such, **but** ~~there~~ may be less concern**ed** that all of an individual's future transactions **are** ~~will be~~ 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 actual or suspected money laundering has taken place or appears to have taken place, the nominated officer is 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

~~7.34~~8.43 ~~When~~**Where SAR Online is used and appropriate consent is needed, this can be done by checking the box requesting consent. Alternatively, requests** ~~consent is needed reports should~~ **can** be faxed to the **NCA** ~~SOCA~~ UKFIU Consent Desk (see the ~~SOCA~~ **NCA** website www.nationalcrimeagency~~soca~~.gov.uk) ~~or, where SAR Online is used, by checking the box requesting consent~~. **You are advised to make it explicit in your report that you are seeking consent from the NCA**.

8.44 **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.**

8.45 The **UKFIU** Consent Desk applies the criteria set out in the *Home Office Circular 029/2008 Proceeds of Crime Act 2002: Obligations to report money laundering – the consent regime* ~~(available from www.homeoffice.gov.uk/about-us/corporate-publications-strategy/home-office-circulars)~~ to **each** ~~every~~ request for consent, **carry** ~~carries~~ out the necessary internal enquiries, and **will** contact~~s~~ the appropriate law enforcement agency, where necessary, for a consent recommendation. Once **the NCA** ~~SOCA~~'s decision has been reached, the disclosing **nominated officer** ~~operator~~ will be informed of the decision by telephone, and be given a consent number, which should be recorded. A formal consent letter from **the NCA** ~~SOCA~~ will follow.

8.46 ***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.**

8.47 **Although POCA provides that consent can be granted by a constable (which includes authorised NCA officers) or a customs officer, there is a recognised 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.

8.48 **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.**[69] **Nominated officers 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.**

~~7.35~~**8.49** ~~As indicated, i~~**I**n the event that **the NCA** ~~SOCA~~ 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** ~~do business~~ with the customer. However, if consent is refused within that period, **the NCA** ~~SOCA~~ can **prevent the transaction or activity** ~~interrupt business~~ for a further 31 calendar days (the moratorium period) from the day consent is refused.

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

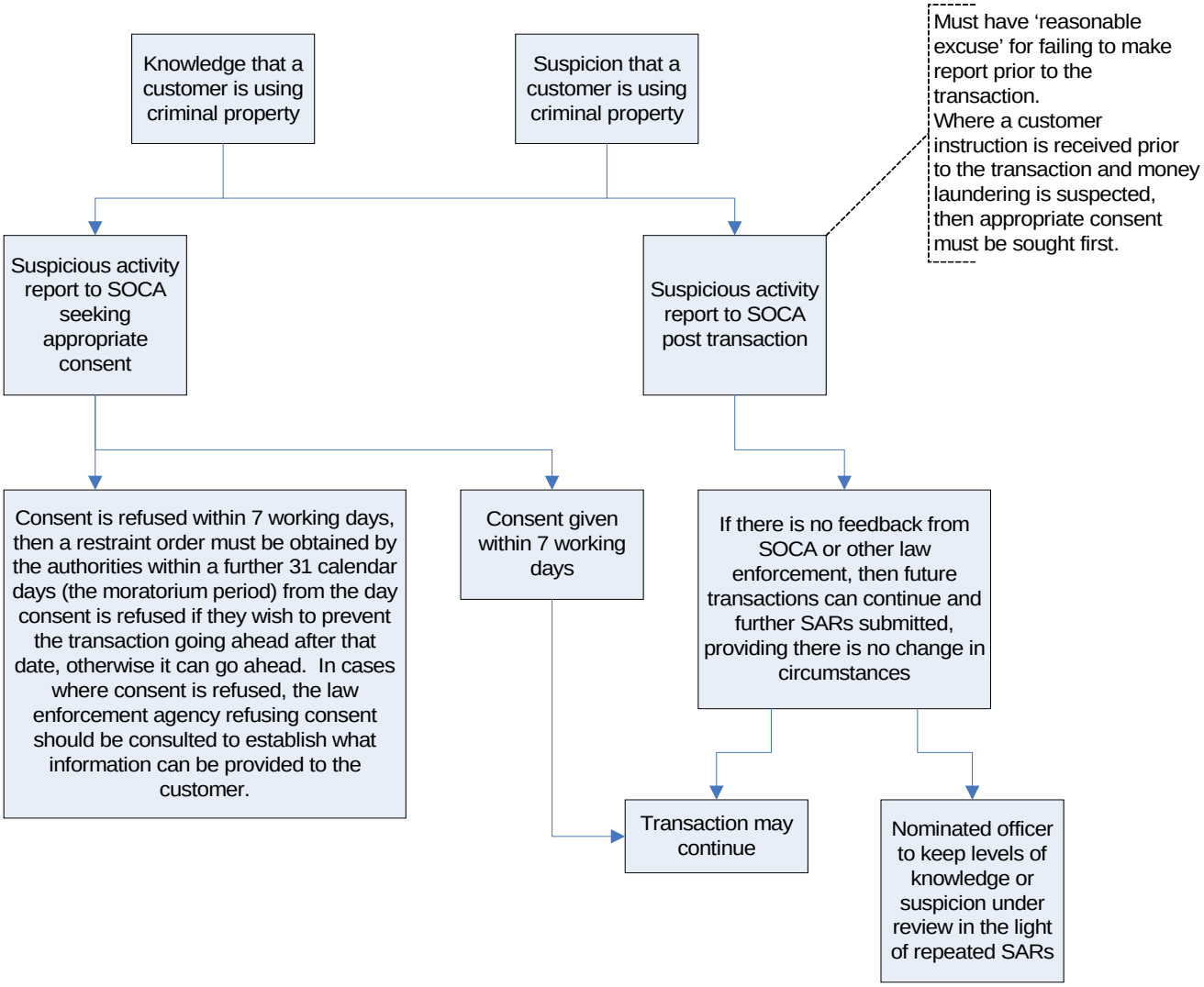
8.51 **Operators should note that consent only applies in relation to individual prohibited acts, and cannot provide cover to deal with a particular customer. Any subsequent activity will require separate consideration and, if necessary, separate consent from the NCA. Where a single money laundering 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 section328(1) of POCA.**

8.52 **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.**

8.53 **The NCA cannot give advice to nominated officers and 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*[70].**

[69] NCA Annual Report
[70] www.nationalcrimeagency.gov.uk

Figure 9: Appropriate consent



~~7.36 All consent requests are dealt with by SOCA on a case-by-case basis and while it may take the maximum of seven working days to deal with a consent request, in practice turnaround time for most SARs is about three days.[71] Nominated officers 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.~~

Failing to report

~~7.37~~8.54 POCA and the Terrorism Act create offences of failing to report suspicious activity. Where a person fails to comply with the obligations to make disclosures to a nominated officer and/or **the NCA** ~~SOCA~~ as soon as practicable after the information giving rise to the knowledge or suspicion comes to the employee they are open to criminal prosecution. The criminal sanction, under POCA or the Terrorism Act, is a prison term of up to five years, and/or a fine.

8.55 **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**.

8.56 **Operators and nominated officers, therefore, must comply with the reporting requirements imposed on them by POCA.**

After a report has been made

~~7.38 Depending on the circumstances, an operator being served with a court order in relation to a customer may have cause for suspicion, or reasonable grounds for suspicion, in relation to that customer. In such an event, operators should review the information it holds about that customer, in order to determine whether or not such grounds for their suspicion exist, and if necessary make a report to SOCA. Where the nominated officer decides not to make a report to SOCA, the reasons for not doing so should be clearly recorded and retained~~.

~~7.39~~8.57 When an enquiry is under investigation, the investigating officer may contact the nominated officer to ensure that he has all the relevant information which supports the original **SAR**~~disclosure~~. This contact may also include seeking supplementary information or documentation from the reporting operator and from other sources by way of a court order.

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

Tipping off, or prejudicing an investigation

~~7.40~~8.59 Under section 333A of POCA a person **in the regulated sector** commits an offence if:

- the person discloses that he or another person has made a disclosure under Part 7 of POCA to a constable , an officer of Revenue or Customs, a nominated officer or a member of staff of **the NCA** ~~SOCA~~ of information that came to that person in the course of a business in the regulated sector;
- the disclosure is likely to prejudice any investigation that might be conducted following the disclosure referred to in (a); and

~~[71] SONCA Annual Report.~~

- the information on which the disclosure is based came to the person in the course of a business in the regulated sector.

A person also commits an offence under section 333A if:

- the person discloses that an investigation into allegations that an offence under Part 7 of POCA has been committed, is being contemplated or is being carried out;
- the disclosure is likely to prejudice the investigation; and
- the information on which the disclosure is based came to the person in the course of a business in the regulated sector.

~~7.41~~**8.60** Under section 342 of POCA a person ~~in the regulated sector~~ also commits an offence if he:

- knows or suspects that an appropriate officer or, in Scotland, a proper person is acting (or proposing to act) in connection with a confiscation investigation, a civil recovery investigation, a detained cash investigation or a money laundering investigation which is being or is about to be conducted, and
- **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.

~~7.42~~**8.61** Under POCA, a person does not falsify, conceal, destroy or otherwise dispose of, or cause or permit the falsification, concealment, destruction or disposal of, documents which are relevant to the investigation if he:

- does not know or suspect that the documents are relevant to the investigation
- does not intend to conceal any facts disclosed by the documents from any appropriate officer or (in Scotland) proper person carrying out the investigation.[72]

~~7.43~~**8.62** POCA therefore, in this regard, contains separate offences of tipping off and prejudicing an investigation. These offences are similar and overlapping, but there are also significant differences between them. It is important for those working in the regulated sector to be aware of the conditions for each offence. Each offence relates to situations where the information on which the disclosure was based came to the person making the disclosure in the course of a business in the regulated sector. The Terrorism Act contains similar offences[73]. There are a number of disclosures which are permitted and that do not give rise to these offences (permitted disclosures) – see paragraphs ~~7.45~~ **8.65** to ~~7.48~~ **8.67**.

~~7.44~~**8.63** Once an internal or external report of suspicious activity has been made, it is a criminal offence for anyone to release information that is likely to prejudice an investigation that might be conducted following that disclosure. An offence is not committed if the person does not know or suspect that the disclosure is likely to prejudice an investigation, or if the disclosure is permitted under POCA or the Terrorism Act[74]. Reasonable enquiries of a customer, conducted in a tactful manner, regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity is prudent practice, forms an integral part of CDD measures and should not give rise to tipping off.

~~7.45~~**8.64** Where a confiscation investigation, a civil recovery investigation, a detained cash investigation or a money laundering investigation is being, or is about to be, conducted, it is a criminal offence for anyone to disclose this fact if that disclosure 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). It is, however, a defence if the person does not know or suspect that disclosure is likely to prejudice the investigation, or if the disclosure is permitted under POCA or the Terrorism Act (see paragraphs ~~7.46~~ **8.65** to ~~7.48~~ **8.67**).

~~7.46~~**8.65** An offence is not committed under POCA or the Terrorism Act if the disclosure is made to the relevant supervisory authority (the Commission) for the purpose of:

[72] Section 342(6) of POCA
[73] Sections 21D and 39 of the Terrorism Act
[74] Section 342(3) of POCA and section 20 of the Terrorism Act

- the detection, investigation or prosecution of a criminal offence in the UK or elsewhere
- an investigation under POCA
- the enforcement of any order of a court under POCA.[75]

~~7.47~~8.66 An employee, officer or partner of a casino operator does not commit an offence under POCA or the Terrorism Act if the disclosure is to an employee, officer or partner of the casino operator.[76]

~~7.48~~8.67 A person does not commit an offence under POCA or the Terrorism Act if the person does not know or suspect that the disclosure is likely to prejudice:

- any investigation that might be conducted following a disclosure; or
- an investigation into allegations that an offence under Part 7 of POCA or Part III of the Terrorism Act has been committed, is being contemplated or is being carried out.[77]

~~7.49~~8.68 The fact that a transaction is notified to **the NCA** ~~SOCA~~ before the event, and **the NCA** ~~SOCA~~ does not refuse consent within seven working days following the day after disclosure is made, or a restraint order is not obtained within the moratorium period, does not alter the position so far as 'tipping off' is concerned.

~~7.50~~8.69 This means that an operator:

- cannot, at the time, tell a customer that a transaction is being delayed because a report is awaiting consent from **the NCA** ~~SOCA~~;
- cannot, later, tell a customer that a transaction or activity was delayed because a report had been made under POCA or the Terrorism Act, unless law enforcement or **the NCA** ~~SOCA~~ agrees, or a court order is obtained permitting disclosure; and
- cannot tell the customer that law enforcement is conducting an investigation.

~~7.51~~8.70 The judgement in *K v Natwest* [2006] EWCA Civ 1039 confirmed the application of these provisions. The judgement in this case also dealt with the issue of suspicion stating that the '*The existence of suspicion is a subjective fact. There is no legal requirement that there should be reasonable grounds for the suspicion. The relevant bank employee either suspects or he does not. If he does suspect, he must (either himself or through the Bank's nominated officer) inform the authorities.*' It was further observed that the '*truth is that Parliament has struck a precise and workable balance of conflicting interests in the 2002 Act*'. The Court appears to have approved of the seven and 31 day scheme and said that in relation to the limited interference with private rights that this scheme entails '*many people would think that a reasonable balance has been struck*'. A copy of the judgement is available on the ~~SOCA~~ **NCA** website (www.nationalcrimeagency.gov.uk).

~~7.52~~8.71 The existence of a SAR cannot be revealed to any customer of the casino at any time, whether or not consent has been requested. However, there is nothing in POCA which prevents operators from making normal enquiries about customer transactions in order to help remove any concerns about the transaction and enable the operator to decide whether to proceed with the transaction. These enquiries will only constitute tipping off if the operator discloses that a SAR has been made to **the NCA** ~~SOCA~~ or a nominated officer, or that a money laundering investigation is being carried out or is being contemplated.

~~7.53~~8.72 The combined effect of these two offences is that one or other of them can be committed before or after a disclosure has been made.

~~7.54~~8.73 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 UK. A person does not commit an offence where

[75] Section 333D of POCA and section 21G of the Terrorism Act
[76] Section 333B of POCA and section 21E of the Terrorism Act
[77] Section 333D of POCA and section 21G of the Terrorism Act

it is known or believed on reasonable grounds that the conduct occurred outside the UK; and the conduct was not criminal in the country where it took place. However, if the criminal activity would constitute an offence in the UK if committed here and would be punishable by imprisonment for a maximum term in excess of twelve months then the defence does not apply except if the offence is an offence under section 23 or 25 of the Financial Services and Markets Act 2000.

~~7.55~~8.74 There is also a specific offence of failure to disclose terrorist financing which was added to the Terrorism Act through the Anti Terrorism Crime and Security Act 2001. This offence is limited to the regulated sector, which includes casinos. The offence can be committed if a person forms knowledge or suspicion of terrorist financing or reasonable grounds for suspecting terrorist financing, during the course of working for a casino, but does not make a report. Guidance issued by the Commission and approved by Treasury must be taken into consideration by any court considering whether this offence has been committed.

Customer interaction

8.75 Normal customer enquiries will not, in the Commission's view, amount to tipping off or 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 CDD measures (and may be driven by social responsibility concerns) and should not give rise to tipping off or the prejudicing of an investigation.

8.76 If patterns of gambling lead to an increasing level of suspicion of money laundering, or even to actual knowledge of money laundering, operators should seriously consider whether they wish to allow the customer to continue using their gaming facilities. If an operator wishes to terminate a customer relationship, and provided this is handled sensitively, there will be low risk of tipping off or 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.

8.77 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, relevant timescales provided, the gravity of the offences being investigated and the purpose of the request), and how this may change the management of risks to the licensing objectives. Given the operator's heightened exposure to risk, it is advisable for the operator to ask for confirmation in writing of such requests from law enforcement. The operator should also continue to submit SARs and/or seek consent from the NCA if they decide to persist with a business relationship with such customers.

Annex 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 a casino 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 (also known as lifestyle spend).**
CTF	Countering terrorist financing.
Customer tracking	The process of capturing drop and win data for a customer.
Drop/win figures	Data recorded by casinos that covers the total value of chips purchased as well as the total loss or win for a customer over a 24 hour period.
Money laundering	The process by which criminal or 'dirty' money is legitimised or made 'clean', including any action taken to conceal, arrange, use or possess the proceeds of any criminal conduct. Defined in section 340 of POCA.
Non-remote casinos	Casinos licensed to operate commercial casino premises.
Operators	Firms holding an opera**ting** ~~or's~~ licence issued by the Commission.
PFL	Personal functional licence.
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.
PML	Personal management licence.
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.
Remote casinos	Casinos licensed to offer casino games by means of remote communication.
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 ~~SOCA~~ under POCA or the Terrorism Act.
Source of funds	**Where the funds, money or cash to finance the transaction come from.**

~~**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.~~
Supervisory authorities	Supervisory authorities, which are listed in regulation 23 of the Regulations. The Commission is the supervisory authority for casinos.
The Act	**The Gambling Act 2005.**
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.**
The Regulations	The Money Laundering Regulations 2007.
The Terrorism Act	The Terrorism Act 2000.
UKFIU	The United Kingdom Financial Intelligence Unit, which is the unit within **the NCA** ~~SOCA~~ that operates the disclosure regime for money laundering.

Appendix B – Summary of consultation questions

Q1. What are your views on the introduction of an additional "key event" obliging operators to provide information to the Commission about investigations of crimes committed against them, crimes committed by their staff or crimes committed using its gambling facilities (for example, spending or laundering the proceeds of crime)?

Q2. For operators, what information about gambling-related crime does your organisation already record centrally, and in what form?

Q3. What are your views on the most proportionate way to ensure that the Commission is provided with information about gambling-related crime in a way that strikes an effective balance between the need for this information and the regulatory burden that providing it would impose?

Q4. Do you consider the proposed wording above to be sufficiently clear on what kinds of gambling-related crimes the Commission would expect to be provided with information about? If not, what wording or additional guidance would be helpful?

Q5. Do you agree that it should be a condition of an operator's licence that they undertake an assessment of money laundering risks?

Q6. If you are an operator, do you already undertake a money laundering risk assessment or would the proposed licence condition require significant additional work?

Q7. Do you have any comments on the draft addition of the licence condition requiring licensees to conduct and review money laundering risk assessments, and devise an action plan to mitigate the risks?

Q8. Do you agree that identifying customers is an important measure to manage heightened money laundering risks presented by specific customers?

Q9. Do you have any comments on the draft addition of the licence condition requiring licensees to identify customers where there is a heighted risk or money laundering and to satisfy themselves about the legitimacy of the customers' funds?

Q10. Do you agree that, in order to have a comprehensive picture of customer risk, it is necessary to monitor customers across all the operator's outlets, platforms and products?

Q11. Do you think that an ordinary code provision is necessary to address this need?

Q12. Do you have any comments on the proposal which will require operators to report on the number of customers where they have ended the business relationship due to money laundering concerns?

Q13. How far would such a requirement add to the regulatory burden on operators?

Q14. Do you have any comments on the draft new licence condition for remote casino operators who have remote gambling equipment located outside of Great Britain?

Q15. Do you agree that licence condition 5.1.1 should apply to remote gambling operators and that it should be amended to make clear that operators must have effective policies and procedures for the handling of both cash and cash equivalents?

Q16. Do you have any views on the licence condition as redrafted?

Q17. Do you have any views whether we should introduce a licence condition to cover this risk, and what it should contain?

Q18. Do you think that this requirement should be limited to cash stakes only?

Q19. Do you have any other views on how to manage risk in this area?

Q20. Do you have any views on whether the Commission should change the status of these ordinary code provisions to make them licence conditions, requiring all operators to comply with the anti-money laundering guidance or advice issued by the Commission?

Q21. Do you have any comments on the revised sections of the guidance document?

Q22. Do you have any comments on the new sections of the guidance document?

Q23. Are there any other areas which you think should be covered in the guidance?

Q24. What are your views on introducing a requirement, potentially via a Social Responsibility code provision for licensees to take all reasonable measures to ensure that digital adverts placed by themselves, or third parties, do not appear on copyright infringing websites?

Q25. What are your views on introducing an ordinary code provision on measures licensees should consider taking to prevent adverts appearing on illegal sites, such as the use of commercial content verification software?

Q26. What other steps or measures do you think could be considered?

Q27. What are your views on the introduction of new ordinary code provisions advising betting operators that they should put in place new employment terms and conditions to require employees to report indicators of suspicious betting and impose restrictions?

Q28. What are your views on the introduction of a new ordinary code provision to advise betting operators that they should include a clause to state that breaches of sports or other rules will also constitute a breach of the operator's customer betting terms and conditions?

Q29. Looking at the challenges in the use of digital currencies listed above, do you see any omissions or oversights? What are your views on the validity of those challenges?

Q30. How might these and any other challenges that you have identified, especially those associated with AML, be mitigated?

Q31. Given the potential difficulty in identifying customers and managing AML risks, what would be the potential benefits in the use of digital currencies compared to the extra compliance work involved?

Q32. Do you see the business drivers to use digital currencies increasing or diminishing, and to what extent?

Q33. What additional AML measures might be needed when accepting deposits from a payment intermediary where their source is digital currencies?

Gambling Commission • Victoria Square House • Victoria Square • Birmingham B2 4BP

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