GAMBLING COMMISSION

The prevention of money laundering and combating the financing of terrorism

Guidance for remote and non-remote casinos
Fourth edition

September 2017

Contents

Figures

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, and the prevention and detection of terrorist financing. For some businesses (including casinos) this includes the more specific requirements of the business and its employees to have policies, procedures and controls in place covering the risks they face from money laundering and terrorist financing.

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

1.4 Money laundering is a term that is often misunderstood. It is defined in section 340 of the Proceeds of Crime Act 2002 (POCA)[1] and covers wide ranging circumstances involving any activity concerning the proceeds of any crime. By way of example, this may include:

- 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
- 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.

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.

[1] http://www.legislation.gov.uk/ukpga/2002/29/contents

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

Legal background

The FATF Recommendations and EU Directive

1.11 The Financial Action Task Force (FATF), which is an international inter-governmental body, issues recommendations on anti-money laundering (AML) and countering terrorist financing (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[2] 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 (the 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 EU Anti-Money Laundering Directive (the EU Directive)[3] 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, financial institutions and a wide range of non-financial businesses and professions (including gambling services, and casinos in particular), to identify their customers, keep appropriate records, establish

[2] The latest Recommendations are available here: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.
[3] Directive (EU) 2015/849: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.141.01.0073.01.ENG.

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 Criminal offences of money laundering were first introduced in the United Kingdom (the 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.

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 The principal offences criminalise any involvement in the proceeds of any crime if the person knows or suspects that the property is criminal property.[4] 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.

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 casino operator)
- removes criminal property from the UK (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 gamble.

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 a casino 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).

[4] Sections 327, 328 and 329 of POCA.

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.[5]

1.21 The principal money laundering offences are wide and can be committed by any person, including, for example, a casino employee, who has 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 UK. However, a person does not commit an offence of money laundering where it is known or believed, on reasonable grounds, that the relevant criminal conduct occurred outside the United Kingdom and the relevant conduct was not criminal in the country where it took place and is not of a description prescribed by an order made by the Secretary of State.[6]

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.[7]

1.24 The penalty for conviction on indictment for an offence under sections 327, 328 or 329 of POCA is imprisonment for a term not exceeding 14 years, a fine, or both[8]. In addition, POCA contains provisions for the recovery of the proceeds of crime and forfeiture can be granted, regardless of whether a conviction for any offence has been obtained or is intended to be obtained. Under certain circumstances, criminal property can be recoverable even if it is disposed of to another person.[9]

The Terrorism Act

1.25 The Terrorism Act 2000 (the Terrorism Act) establishes several offences about engaging in or facilitating terrorism, as well as raising or possessing funds for terrorist purposes. It establishes a list of proscribed organisations that are believed to be involved in terrorism. In December 2007, tipping off offences and defences to the principal terrorist property offences were introduced[10].

1.26 The Terrorism Act applies to all persons and includes obligations to report suspected terrorist financing. The offences of failing to disclose and tipping off are specific to people working in firms covered by the Money Laundering Regulations (the Regulations), and who are therefore in the regulated sector, which includes casinos.

---

[5] Section 329(2)(c) of POCA.
[6] Sections 327(2A), 328(3) and 329(2A) of POCA.
[7] Note that, following the decision in relation to *R v Anwoir* [2008] 2 Cr. App. R. 36, the Prosecution does not need to *prove* a specific criminal offence, but can instead show that it derived from conduct of a specific kind or kinds and that conduct of that kind or those kinds was unlawful, and by evidence of the circumstances in which the property had been handled, which were such as to give rise to the irresistible inference that it could only have been derived from crime.
[8] Section 334 of POCA.
[9] Section 304 of POCA.
[10] Introduced by the Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007.

The Money Laundering Regulations

1.27 The Regulations[11] represent the UK's response to the EU Directive and implement the law in the UK on this topic. They set requirements for the AML/CTF regime within the regulated sector (which includes casinos).

1.28 The Regulations apply to non-remote and remote casinos, licensed by the Commission, who act in the course of business carried on by them in the UK. This includes remote casinos which either:

- have at least one piece of remote gambling equipment situated in Great Britain, or
- do not have remote gambling equipment situated in Great Britain, but the gambling facilities provided by remote casino are used in Great Britain.[12]

1.29 The Regulations impose additional requirements on the regulated sector. These include risk assessments and requirements in respect of written policies, procedures and controls, internal controls, CDD, record keeping and training.

1.30 This guidance sets out how casino operators must and can comply with the law governing money laundering and terrorist financing. 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, and 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.

The role of gambling operators

1.31 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 from being a source of crime or disorder, being associated with crime or disorder or being used to support crime.

1.32 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).

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

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

[11] The current regulations (The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017) came into effect on 26 June 2017 and implement the 4th EU Anti-Money Laundering Directive.
[12] Regulations 8 and 9.

The role of the Gambling Commission

1.35 The Commission requires operators to prevent gambling being a source of crime or disorder, being associated with crime or disorder or being used to support crime. This guidance document is an important frame of reference to help casino 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 this guidance will assist casino operators to meet their obligations under POCA, the Regulations and the Terrorism Act, where appropriate.

1.36 Under the Regulations[13], the Commission is designated as the supervisory authority for casinos. The Regulations[14] stipulate that a supervisory authority must:

- effectively monitor the relevant persons for which it is the supervisory authority and take necessary measures for the purpose of securing compliance by such persons with the requirements of the Regulations
- adopt a risk-based approach to the exercise of its supervisory functions, having identified and assessed the risks of money laundering and terrorist financing to which the relevant persons for which it is the supervisory authority are subject
- ensure that its employees and officers have access to relevant information on the risks of money laundering and terrorist financing which affect its sector
- base the frequency and intensity of its on-site and off-site supervision on the risk profiles it has prepared
- keep a record in writing of the actions it has taken in the course of its supervision and of its reasons for deciding not to act in a particular case
- take effective measures to encourage its sector to report breaches of the provisions of the Regulations to it.

1.37 In accordance with its risk-based approach, the supervisory authority must take appropriate measures to review:

- the risk assessments carried out by relevant persons to identify and assess the risks of money laundering and terrorist financing to which the business is subject
- the adequacy of the policies, procedures and controls adopted by the relevant persons and the way that those policies, procedures and controls have been implemented[15].

1.38 The Commission therefore adopts a risk-based approach to its role as supervisory authority. We focus our attention on circumstances where the processing of criminal funds or criminal spend indicates serious failures in an operator's arrangements for the management of risk and compliance with POCA, the Regulations and the Terrorism Act or a breach of a licence condition, or makes a reasonably significant contribution to the financial performance of the business, particularly concerning their continued suitability to hold a licence[16].

1.39 Where a casino operator fails 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, or breaches an applicable licence condition, the Commission will consider reviewing the operating licence 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. The Commission may also consider imposing a financial penalty where a licence condition has been breached, in accordance with section 121 of the Act.

---

[13] Regulation 7(1)(d).
[14] Regulation 46(1) and (2).
[15] Regulation 46(4).
[16] See the public statements available here: http://www.gamblingcommission.gov.uk/news-action-and-statistics/news/news.aspx?searchKeywords=&categories=0/1/24/51&page=0#main.

1.40 Certain activities carried out by non-remote casinos regarding the methods of payment that they accept in respect of gambling services are categorised as money service business (MSB) activities. By acting as a cheque casher or currency exchange, or by accepting winners' cheques and foreign currency, casinos are subject to registration with, and supervision by, HM Revenue and Customs (HMRC). The exemptions that remove this requirement, where the MSB activities are occasional or very limited, do not apply to casinos because of the value of the transactions typically involved. However, in order to avoid dual regulation, and as provided by the Regulations[17], there is an agreement between HMRC and the Commission that the Commission performs the supervisory role for the MSB activities in question. This means that it is not necessary for non-remote casinos to register with HMRC in this regard.

Purpose of the guidance

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

1.42 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 casino operators to design and implement the policies, procedures and controls necessary to mitigate the risks of being used in connection with money laundering and the financing of terrorism.

1.43 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.

1.44 While the guidance focuses primarily on the relationship between casino 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[18].

How should the guidance be used?

1.45 The purpose is to give guidance to those who set casino operators' risk management policies, procedures and controls for preventing money laundering and terrorist financing. This guidance aims to assist casino 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. Casino operators will need to establish more detailed and more specific internal arrangements directed by senior management and nominated officers to reflect the risk profile of their business.

1.46 This guidance is not intended to be a substitute for legal advice and nothing in this document should be construed as such. Anyone requiring clarification on the legal issues contained in this document should seek their own independent legal advice. Neither is this

[17] Regulation 7(2) and (3).
[18] Attention is drawn to paragraph 2.10 and code provision 1.1.2.

document a substitute for casino operators' individual risk management plans. Casino operators should refer to the Regulations and associated legislation in making decisions in relation to the Regulations. The examples used throughout are for illustrative purposes only. The references to legislation and case law are accurate at the time of writing, but these may be subject to repeal or amendment.

Content of the guidance

1.47 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 casino operators to adopt and evidence. The Commission will expect casino operators to be able to explain the reasons for any departures from that standard.

1.48 This guidance emphasises the responsibility of senior management to manage the casino 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, including the obligation to monitor customer activity.

1.49 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.

1.50 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 casino 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; and
- the identification and reporting of suspicious activity.

Status of the guidance

1.51 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[19]. The Regulations require that a court must consider whether someone has followed this guidance if they are prosecuted for failing to comply with the Regulations.[20]

1.52 Casino 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.

1.53 The Commission is not a 'designated supervisory authority' under the Regulations and therefore has no powers to take action against casino operators that breach the

[19] Section 21A(6) of the Terrorism Act.
[20] Sections 330 and 331 of POCA, section 21(6) of the Terrorism Act and Regulation 86(2).

Regulations.[21] However, an ordinary code provision[22] within the licence conditions and codes of practice requires casino operators to act in accordance with this guidance.

1.54 The Commission and other agencies or authorities that have the appropriate authorisation under POCA in England and Wales[23] can, in certain circumstances, apply for orders and warrants in relation to money laundering, for the purpose of for example:

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

1.55 The guidance provides a sound basis for casino 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 to, amongst others, the Commission.

Licence conditions and codes of practice

1.56 Casino operators are required to comply with the applicable licence conditions and codes of practice[24], and should read this guidance in conjunction with the conditions and codes. Should casino operators breach the licence conditions or not follow the code provisions, the Commission may consider reviewing the operating licence in accordance with 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. The Commission may also consider imposing a financial penalty where we think that a licence condition has been breached, in accordance with section 121 of the Act.

2 Risk-based approach

Introduction

2.1 The Regulations impose compulsory requirements and a breach can constitute a criminal offence.[25] However, within this legal framework of requirements, casinos have flexibility to devise policies, procedures and controls which best suit their assessment of the money laundering and terrorist financing risks faced by their business. The Regulations require the identification and assessment of money laundering and terrorist financing risks, and policies, procedures and controls to mitigate and manage effectively the risks identified.[26]

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, procedures and controls they have put in place to manage the risks to the licensing objectives. The approach to managing the risks of the operator being used for money laundering or terrorist financing is consistent with the regulatory requirements.

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

[21] Regulation 76.
[22] Ordinary code provision 2.1.1.
[23] See The Proceeds of Crime Act 2002 (References to Financial Investigators) (England and Wales) Order 2015 (Statutory Instrument No. 2015/1853), as amended.
[24] www.gamblingcommission.gov.uk/for-gambling-businesses/Compliance/LCCP/Licence-conditions-and-codes-of-practice.aspx
[25] Regulation 86.
[26] Regulations 18 and 19.

purpose. The detail and complexity of these systems will depend on the operator's size and the complexity of their business.

2.4 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, procedures and controls to manage and mitigate these assessed risks
- monitor and improve the effective operation of these controls
- record what has been done, and why.

2.5 The possibility of gambling facilities being used by criminals to assist in money laundering or terrorist financing poses many risks for casino 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.

2.6 Casino operators can offset any burden of taking a risk-based approach with the benefits of having 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.

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

Identifying and assessing the risks

2.8 The Regulations require casino operators to take appropriate steps, taking into account the size and nature of its business, to identify and assess the risks of money laundering and terrorist financing to which its business is subject, taking into account:

- information on the risks of money laundering and terrorist financing made available to them by the Commission
- risk factors, including factors relating to:
    - its customers
    - the countries or geographic areas in which it operates
    - its products or services
    - its transactions
    - its delivery channels[27].

2.9 Casino operators must:

- keep an up-to-date record in writing of all the steps taken to identify and assess the risks of money laundering and terrorist financing risks to which its business is subject
- provide the written record, the risk assessment it has prepared and the information on which it was based to the Commission on request[28].

[27] Regulation 18(1), (2) and (3).
[28] Regulation 18(4) and (6).

2.10 The casino operator should assess its risks in the context of how it is most likely to 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 casino 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 (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, multiple bank accounts and cash, particularly where this is in different currencies or uncommon bank notes)?
- In relation to remote gaming, does the customer use shared internet protocol addresses, dormant accounts or virtual private network (VPN) connections (among other things, this could indicate that a group of people are using the same device or location to gamble for the purposes of committing fraud)?

As noted in paragraph 1.44, operators should also give due consideration to the money laundering risks posed by their business-to-business relationships, including any third parties they contract with. The assessment of these risks is based, among other things, on the risks posed to the operator by transactions and arrangements with business associates and third party suppliers such as payment providers and processors, including their beneficial ownership and source of funds. Effective management of third party relationships should assure operators that the relationship is a legitimate one, and that they can evidence why their confidence is justified.[29]

Risk assessments

2.11 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.

2.12 Risk, therefore, is a function of three factors:

- *threats* – which are persons, or groups of people, objects or activities with the potential to cause harm, including criminals, terrorist groups and their facilitators,

[29] An example of good practice guidelines on conducting third party due diligence can be found here: http://www3.weforum.org/docs/WEF_PACI_ConductingThirdPartyDueDiligence_Guidelines_2013.pdf.

their funds, as well as past, present and future money laundering or terrorist financing activities
- *vulnerabilities* – which are those things that can be exploited by the threat or that may support or facilitate its activities and means focussing on the factors that represent weaknesses in AML/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.

2.13 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.

2.14 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.

2.15 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.

2.16 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.

2.17 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 casino 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.

Casinos should also consider the risks posed by particular products they offer.[30]

Country/geographic risk

2.18 Some countries pose an inherently higher money laundering and terrorist financing risk than others. In addition to considering their own experiences, casino operators should take into account a variety of other credible sources of information identifying countries with risk factors in order to determine that a country and customers from that country pose a higher

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

risk. Casino 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.

2.19 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 should check customer location because of the additional risks which arise from cross-border operations.

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

Customer risk

2.21 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, family members of PEPs or known close associates of PEPs
- high spenders – the level of spending which will be considered to be high for an individual customer will vary among casino operators, and among casinos managed by the same operator
- disproportionate spenders – casino operators should obtain information about customers' financial resources so that they can determine whether customers' spending is proportionate to their income or wealth
- casual customers – this includes tourists, participants in junkets and local customers who are infrequent visitors
- regular customers with changing or unusual spending patterns
- 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 – junkets can pose several higher risks, including criminal control of the junket operator or participants, the movement of funds across borders which obscures the source and ownership of the money gambled by participants and their identities, and structuring, refining and currency exchange risks
- 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)

2.22 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 been gained through criminal activity, 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 casino 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 casino operators normally cannot perform the same level of checks on the cards as they can on bank accounts
    - e-wallets – some e-wallets accept cash on deposit or cryptocurrencies, which pose 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

2.23 Product risk includes the consideration of the vulnerabilities associated with the particular products offered by the casino 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. These are more fully discussed in paragraph 2.22, and include the use of cash and casino deposit accounts, and the redemption of chips. 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.

2.24 Products which may pose a money laundering risk for the casino 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.

2.25 The risk categories or factors described above are not intended to be prescriptive or comprehensive. They will not apply universally to all casino 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 casino operators conduct their own customer risk assessments, and to devise AML/CTF policies, procedures and controls which accurately and proportionately reflect those assessments.

2.26 The weight given to the risk factors used by the casino 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, casino operators also have to make their own determination as to the weight given to risk factors.

2.27 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 casino operator's business model is focused on:
  - attracting a large number of customers who gamble relatively small amounts
  - attracting a small number of customers who gamble relatively large amounts
- speed and volume of business
- for non-remote 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 casino 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 casino operator is based in one country or has a gambling presence in multiple countries.

2.28 Deciding that a customer presents a higher risk of money laundering or terrorist financing does not automatically mean that the person is a criminal, money launderer or 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 laundering money or engaging in criminal spend. Employees therefore need to remain vigilant and use their experience and common sense in applying the casino operator's risk-based criteria and rules, seeking guidance from their nominated officer as appropriate.

2.29 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).

2.30 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 bank notes. 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.

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

2.32 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. Casino 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.

2.33 In order to be able to detect customer activity that may be suspicious, it is necessary to monitor all transactions or activity.[31] The monitoring of customer activity should be carried out using the risk-based approach. Higher risk customers should be subjected to a frequency and depth of scrutiny greater than may be appropriate for lower risk customers. Casino operators should be aware that the level of risk attributed to customers may not correspond to their commercial value to the business.

2.34 Casino operators are best placed to identify and mitigate risks involved in their business activity. A crucial element of this is to have systems and controls to identify and link player activity, and for senior management to oversee risk management and determine whether their policies, procedures and controls are effective in design and application. Reliance on

[31] Regulation 8.

third parties to conduct risk assessment and management functions does not relieve the operator of its responsibility to assess and manage its own risks. Third party services should not be used in isolation or relied upon solely, and casino operators should be satisfied that the information supplied by the third party is sufficiently detailed, reliable and accurate.

2.35 There is a risk that customers will place and layer criminal proceeds through gambling transactions. We recommend that 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, for example in cash or back to the same bank account, limits the opportunity for a money launderer to layer the proceeds of criminal activity. Where it is not feasible to return funds to the source or in the same form, casino operators should have controls in place to manage the risk of money laundering occurring in these circumstances.

Risk management is dynamic

2.36 A money laundering/terrorist financing risk assessment is not a one-off exercise. Casino operators must therefore ensure that their policies, procedures and controls 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.

2.37 Casino operators need to continually identify, assess and manage these risks, just like any other business risk. They should assess the level of risk in the context of how their business is structured and operated, and the controls in place to minimise the risks posed to their business by money launderers, including those engaged in criminal spend. The risk-based approach means that casino 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.

2.38 There is a specific requirement in the Regulations that, when new technology is adopted by casino operators, appropriate measures are taken in preparation for, and during, the adoption of such technology to assess and, if necessary, mitigate any money laundering or terrorist financing risks the new technology may cause.[32]

3 Customer relationships

3.1 Casino operators should be mindful that some risk indicators (for example, a pattern of increasing spend or spend inconsistent with apparent source of income) could be indicative of money laundering, but also equally of problem gambling, or both. There may also be patterns of play (for example, chasing losses) that appear to be indicative of problem gambling that could also be considered to indicate other risks (for example, spend that is inconsistent with the individual's apparent legitimate income could be the proceeds of crime). While patterns of play may be one indicator of risk, casino 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.

[32] Regulation 19(4)(c).

3.2 Casino operators are subject to both certain provisions of POCA, the Regulations and the Act (and the relevant licence conditions and codes of practice). Operators have the responsibility to comply with the licensing objectives and, therefore, they should carry out appropriate enquiries and assessments to ensure they do so. While the conclusions drawn and actions taken may differ according to whether money laundering and/or social responsibility risks are identified, the effective identification and management of these risks rests upon the ability of casino 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 casino operator is able to reconcile information relating to customers' gambling activities in different parts of the business so that they have a more complete picture of the risks posed by the activities of individual customers.

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 casino operator to proactively monitor high risk customers in relation to their money laundering risk.

3.5 Customer relationships need to be managed proficiently and records should be maintained as to what information was communicated to the customer, why it was communicated and what considerations were made. If players expect that customer interaction is likely should they play with large amounts of money, or for lengthy periods, and such interaction is consistently applied, there would be less reason for players to question or become suspicious of the motives of these interactions. Casino 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 casino 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, procedures and controls 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 the obtaining of a defence (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); whether there is a need to report suspicious activity or seek a defence (appropriate consent); and any risks posed to the licensing objectives.

Establishment of business relationship

3.9 A business relationship is a business, professional or commercial relationship between a casino operator and a customer which arises out of the business of the casino operator and is expected by the operator, at the time when the contact is established, to have an element of duration.[33] Casino operators are advised to interpret this definition widely.

3.10 A business relationship with a customer of a casino operator:

- is likely to occur when, for example:

[33] Regulation 4(1).

    - a customer opens an account with the casino operator or becomes a member of a casino (when a membership scheme is operated by the casino), or
    - a customer obtains a cheque cashing facility
  - may occur when, for example:
    - the casino starts tracking a customer's drop/win figures, other than to establish when the customer reaches the €2,000 threshold for CDD.

3.11 The list above is not exhaustive and a casino operator will need to form its own view of when contact is established, or circumstances otherwise arise, with a customer from which it expects, or it could reasonably be inferred that it expects, that the relationship with the customer will have an element of duration. The Commission acknowledges that this may not necessarily be the case when a casino operator permits a customer to join a casino loyalty scheme.

3.12 When establishing a business relationship, casino 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).

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

3.14 There is further discussion of business relationships in paragraphs 7.5 to 7.9.

Customer monitoring

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

3.16 Casino 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 casino 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.

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

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

3.19 Customer monitoring forms part of ongoing monitoring, which is discussed in paragraphs 6.20 and 6.21, and 7.8 and 7.9.

Termination of business relationship

3.20 As already discussed, to avoid potentially committing one of the principal money laundering offences, casino 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.

3.21 Additionally, where, in relation to any customer, the casino operator is unable to apply CDD measures, the business relationship with the customer *must* be terminated and the operator must submit a SAR to the NCA where they consider the circumstances to be suspicious.[34]

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

4 Senior management responsibility

Introduction

4.1 For the purposes of the Regulations and this guidance, 'senior management' means officers or employees of the casino operator with sufficient knowledge of the operator's money laundering and terrorist financing risk exposure, and of sufficient authority, to take decisions affecting its risk exposure.[35]

4.2 Senior management must be fully engaged in the processes for a casino 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.

4.3 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.

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

Obligations on all casino operators

4.5 An officer of a licensed casino 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

[34] Regulation 31.
[35] Regulation 3(1).

commission of offences under the Regulations, or where the commission of any such offence is attributable to any neglect on their part, will be individually liable for the offence.[36]

4.6 Senior management should require that the nominated officer provides an annual report covering the operation and effectiveness of the operator's systems and controls to combat money laundering and terrorist financing, 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, procedures and controls

4.7 Casino operators must establish and maintain policies, procedures and controls to mitigate and manage effectively the risks identified in the operator's risk assessment of money laundering and terrorist financing. The policies, procedures and controls must be:

- proportionate with regard to the size and nature of the operator's business
- approved by its senior management.[37]

4.8 In determining what is appropriate or proportionate with regard to the size and nature of their business, casino operators may take into account any guidance issued by the Commission or appropriate body, *and* approved by HM Treasury.[38] An appropriate body is a body which regulates or is representative of any trade, profession, business or employment carried on by a casino operator[39] (and includes trades bodies such as the National Casino Forum and the Remote Gambling Association).

4.9 Casino operators must maintain a record in writing of:

- their policies, procedures and controls
- any changes to those policies, procedures and controls
- the steps they have taken to communicate the policies, procedures and controls, or any changes to them, within the operator's business.[40]

4.10 The policies, procedures and controls must include:

- risk management practices
- internal controls
- CDD measures and ongoing monitoring, including enhanced measures for high risk customers
- reliance and record keeping
- the monitoring and management of compliance with, and the internal communication of, such policies, procedures and controls.[41]

4.11 The policies, procedures and controls must also include specific policies, procedures and controls:

- that provide for the identification and scrutiny of:
  - complex or unusually large transactions, or unusual patterns of transactions, that have no apparent economic or legal purpose
  - and other activity or situation that the casino operator regards as particularly likely, by its nature, to be related to money laundering or terrorist financing

[36] Regulation 92.
[37] Regulation 19(1) and (2).
[38] Regulation 19(5).
[39] Regulation 3(1).
[40] Regulation 19(1)(c).
[41] Regulation 19(3).

- that specify the undertaking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of products or transactions that might favour anonymity
- which ensure that, when new technology is adopted by the casino operator, appropriate measures are taken in preparation for, and during, the adoption of such technology to assess and, if necessary, mitigate any money laundering or terrorist financing risks this new technology may cause
- under which anyone in the operator's business who knows or suspects, or has reasonable grounds for knowing or suspecting, money laundering or terrorist financing must report such knowledge or suspicion to the operator's nominated officer.[42]

4.12 The casino operator's policies, procedures and controls should also cover:

- the arrangements for nominated officer reports to senior management
- the systems for customer identification and verification, including enhanced arrangements for high risk customers, including 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 submission to the NCA
- the mechanisms for contact between the nominated officer and law enforcement or the NCA, including the circumstances in which or defence (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, procedures and controls
- the communication of such policies, procedures and controls, including details of how compliance is monitored by the nominated officer, and the arrangements for communicating the policies, procedures and controls to all relevant employees;
- employee training records; and
- supporting records in respect of business relationships, and the retention period for the records.

4.13 Casino operators must, where relevant, communicate the policies, procedures and controls they establish and maintain to their branches and subsidiary undertakings which are located outside the United Kingdom.[43]

Internal controls

4.14 Where appropriate, with regard to the size and nature of the business, a casino operator must appoint a member of its board of directors (or equivalent management body if there is no board) or of its senior management as the officer responsible for the operator's compliance with the Regulations.[44]

4.15 In determining what is appropriate or proportionate with regard to the size and nature of their business, casino operators must take into account any guidance issued by the Commission or appropriate body, *and* approved by HM Treasury.[45] An appropriate body is a body which regulates or is representative of any trade, profession, business or employment carried on by a casino operator[46] (and includes trades bodies such as the National Casino Forum and the Remote Gambling Association).

[42] Regulation 19(4).
[43] Regulation 19(6).
[44] Regulation 21(1)(a).
[45] Regulation 21(10).
[46] Regulation 3(1).

4.16 Where the casino operator appoints a board member as the officer responsible for the operator's compliance with the Regulations, it is important that this member and the director or senior manager who is allocated the overall responsibility for the establishment and maintenance of the operator's AML and CTF systems (where they are not the same person) are clear of their responsibilities.

4.17 The casino operator must, within 14 days of the appointment, inform the Commission of the identity of the individual appointed as the officer responsible for the operator's compliance with the Regulations, and any subsequent appointment to that position.[47]

4.18 The internal controls envisaged in paragraph 4.10 must, where appropriate with regard to the size and nature of the casino operator's business, provide for:

- the appointment of one individual who is a member of the board of directors (or, if there is no board, of the equivalent management body) or of its senior management as the officer responsible for the operator's compliance with the Regulations
- carrying out screening of relevant employees appointed by the operator, both before the appointment is made and during the course of the appointment, where:
    - screening means an assessment of the skills, knowledge and expertise of the individual to carry out their functions effectively, and the conduct and integrity of the individual
    - a relevant employee is an employee whose work is:
        - relevant to the operator's compliance with any requirement in the Regulations
        - otherwise capable of contributing to the identification or mitigation of the risks of money laundering and terrorist financing to which the operator is subject, or the prevention or detection of money laundering and terrorist financing in relation to the operator's business
- the establishment of an independent audit function with the responsibility to:
    - examine and evaluate the adequacy and effectiveness of the policies, procedures and controls adopted by the operator to comply with the Regulations
    - make recommendations in relation to those policies, procedures and controls
    - monitor the operator's compliance with those recommendations.[48]

4.19 In determining what is appropriate or proportionate with regard to the size and nature of their business, casino operators must take into account any guidance issued by the Commission or appropriate body, *and* approved by HM Treasury.[49] An appropriate body is a body which regulates or is representative of any trade, profession, business or employment carried on by a casino operator[50] (and includes trades bodies such as the National Casino Forum and the Remote Gambling Association).

4.20 Casino operators must establish and maintain systems that enable them to respond fully and rapidly to enquiries from financial investigators accredited under section 3 of POCA, persons acting on behalf of the Scottish Ministers in their capacity as an enforcement authority under POCA, or constables or equivalent officers of any law enforcement authority, in relation to:

- whether it maintains, or has maintained during the previous five years, a business relationship with any person, and
- the nature of the relationship.[51]

[47] Regulation 21(4).
[48] Regulation 21.
[49] Regulation 21(10).
[50] Regulation 3(1).
[51] Regulation 21.

Training

4.21 The Regulations require that all relevant employees of casinos must be trained on the prescribed AML and CTF topics[52]. Casino operators must ensure that their employees understand the Regulations, the Terrorism Act and POCA, and data protection, and apply the operator's policies, procedures and controls, including the requirements for CDD, record keeping and SARs.

4.22 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 casino operator's AML/CTF strategy.

4.23 Casino 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. Casino 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.

4.24 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.

4.25 The Regulations require casino operators to take appropriate measures so that their relevant employees are:

- made aware of the law relating to money laundering and terrorist financing, and to the requirements of data protection, which are relevant to the implementation of the Regulations
- regularly given training in how to recognise and deal with transactions and other activities or situations which may be related to money laundering or terrorist financing.[53]

4.26 Casino operators must maintain a record in writing of the appropriate training measures they have taken and, in particular, of the training given to their relevant employees.[54]

4.27 'Relevant employees' are employees whose work is:

- relevant to the casino operator's compliance with any requirements in the Regulations, or
- able to contribute to:
    - the identification or mitigation of the risk of money laundering or terrorist financing to which the operator's business is subject, or
    - the prevention or detection of money laundering or terrorist financing in relation to the operator's business.[55]

This includes the holders of personal management licences and personal functional licences issued by the Commission as well as employees responsible for completing CDD measures.

---

[52] Regulation 24.
[53] Regulation 24(1).
[54] Regulation 24(1)(b).
[55] Regulation 24(2).

4.28 In deciding what training measures are appropriate, a casino operator:

- must take account of the nature of its business, its size, and the nature and extent of the money laundering and terrorist financing risks to which its business is subject
- should take account of the guidance issued by the Commission or by any body which represents the casino industry in Britain, such as the National Casino Forum or the Remote Gaming Association.[56]

4.29 The content of any training, the regularity of training and the assessment of competence following training are matters for each casino operator to assess and decide in light of the money laundering and terrorist financing risks they identify, provided the requirements of regulation 24 are met. The Commission will expect such issues to be covered in each operator's policies and procedures. These should make provision for the attainment of an appropriate competence level by the relevant employees identified in paragraph 4.27, 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.

4.30 Casino 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
- 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
- how PEPs, family members of PEPs and known close associates of PEPs will be identified.

4.31 There is no single solution when determining how to deliver training and a mix of training methods may, therefore, be appropriate. Online 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.

4.32 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.

4.33 Ongoing training must 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.

4.34 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.

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

[56] Regulation 24(3).

4.36 It is also recommended that casino operators consult the Commission's AML webpage, which has useful information (including statements regarding AML controls) and links to other AML resources.[57]

5 Nominated officer

5.1 Casino operators must appoint an individual in their firm as a nominated officer[58], who is responsible for:

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

5.2 This does not allow the nominated officer function to be outsourced to an individual independent of the firm. The requirement to appoint a nominated officer does not apply where the casino operator does not employ, or act in association with, any other person[59]. The casino operator must, within 14 days of the appointment, inform the Commission of the identity of the individual appointed as the nominated officer and any subsequent appointment to that position[60].

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

5.4 The nominated officer should be able to monitor 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.

5.5 The term 'nominated officer' is used and defined in the Regulations[61].

Standing of the nominated officer

5.6 The nominated officer is responsible for the oversight of all aspects of the casino 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 should 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.

5.7 The nominated officer must:

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

[57] www.gamblingcommission.gov.uk/for-gambling-businesses/Compliance/General-compliance/AML/Anti-money-laundering.aspx
[58] Regulation 21(3).
[59] Regulation 21(6).
[60] Regulation 21(4).
[61] Regulation 3(1).

5.8 In determining the status of the nominated officer and identifying the appropriate position for this officer within the overall organisational structure, casino 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.

5.9 The Commission recognises that some casino 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.

5.10 The casino operator's senior management must ensure that the nominated officer has sufficient resources available, including appropriate employees, technology and training. This should include arrangements that apply in the temporary absence of the nominated officer.

5.11 Where a nominated officer is temporarily unavailable, another PML holder may deputise. Casino operators should consider appointing a permanent deputy nominated officer.

5.12 Where a casino operator's nominated officer delegates to another employee, the nominated officer remains responsible for AML issues and is likely to remain liable for the commission of any criminal offences relating to POCA, the 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 by way of acceptance of responsibility
- all employees who need to be aware of the delegation should be notified immediately.

Internal and external reports

5.13 A casino 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 makes an internal report to their nominated officer.

5.14 Whilst disclosure to another of the fact that a person may be engaged in money laundering is generally an offence[62], such disclosures to a nominated officer, constable or customs officer are specifically protected, where they are made as soon as is practicable and the information came to their attention in the course of their trade, profession, business or employment.[63] We recommend that casino operators make employees 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. Whether or not this defence would be successful would be a matter for the court based on the exact circumstances of the case.

5.15 Any internal report should be considered by the nominated officer, in the light of all other relevant information available to the nominated officer, to determine whether or not the report gives rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion, that a person is engaged in money laundering or terrorist financing.

[62] Section 333A of POCA.

[63] Section 337 of POCA.

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

5.17 The nominated officer must be fully conversant with the legal obligations to make external reports to the NCA.

5.18 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.

6 Customer due diligence

Introduction

6.1 In the Regulations, a key requirement is to make checks on customers, known as customer due diligence or CDD.

6.2 Casino operators must apply CDD measures if they:

- establish a business relationship (see paragraphs 3.9 to 3.13 and 7.5 to 7.9)
- suspect money laundering or terrorist financing
- doubt the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification
- carry out an occasional transaction that amounts to a transfer of funds[64] which is more than €1,000[65].

6.3 Regardless of whether they have established a business relationship with the customer, suspect money laundering or terrorist financing, or doubt the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification, casino operators must *also* apply CDD measures in relation to any transaction that amounts to €2,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked.[66]

6.4 'Transaction' consists of:

- the wagering of a stake, including:
  - the purchase from, or exchange with, the casino of tokens for use in gambling at the casino
  - payment for the use of gaming machines
  - the deposit of funds required to take part in remote gambling, or
- the collection of winnings, including the withdrawal of funds deposited to take part in remote gambling or winnings arising from the staking of such funds.[67]

6.5 In determining whether a transaction amounts to €2,000 or more, casino operators do not need to take account of winnings from a previous transaction which had not been collected from the casino, gaming machine or remote gambling, but are being re-used in the

[64] In this context, 'transfer of funds' means any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same, including: (a) a credit transfer as defined in point (1) of Article 2 of Regulation (EU) No 260/2012; (b) a direct debit as defined in point (2) of Article 2 of Regulation (EU) No 260/2012; (c) a money remittance as defined in point (13) of Article 4 of Directive 2007/64/EC, whether national or cross border; (d) a transfer carried out using a payment card, an electronic money instrument, or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics.
[65] Regulation 27(1).
[66] Regulation 27(5).
[67] Regulation 27(6).

transaction in question.[68] This means that casino operators do not need to include re-staked winnings (so called 'recycled winnings', 'turnover' or 'churn') when determining whether a customer has reached the €2,000 threshold.

6.6 Casino operators must *also* apply CDD measures:

- at other appropriate times to existing customers on a risk-based approach
- when the operator becomes aware that the circumstances of an existing customer relevant to its risk assessment for that customer have changed.[69]

6.7 In determining when it is appropriate to apply CDD measures to existing customers, casino operators must take into account the following, among other things:

- any indication that the identity of the customer, or of the customer's beneficial owner, has changed
- any transactions which are not reasonably consistent with the operator's knowledge of the customer
- any change in the purpose or intended nature of the operator's relationship with the customer
- any other matter which could affect the operator's assessment of the money laundering or terrorist financing risk in relation to the customer.[70]

Customer due diligence measures

6.8 CDD measures consist of:

- identifying the customer, unless the identity of the customer is known to, and has been verified by, the casino operator
- verifying the customer's identity, unless the customer's identity has already been verified by the casino operator
- where there is a beneficial owner who is not the customer, identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner so that the casino operator is satisfied that it knows who the beneficial owner is
- assessing and, where appropriate, obtaining information on the purpose and intended nature of the business relationship.[71]

6.9 Where a person claims to act on behalf of a customer (such as an agent), the casino operator must:

- verify that the person is authorised to act on the customer's behalf
- identify the person
- verify the person's identity on the basis of documents or information which, in either case, is obtained from a reliable source which is independent of both the person and the customer.[72]

6.10 For the purposes of CDD, 'verify' means verifying on the basis of documents or information which, in either case, have been obtained from a reliable source which is independent of the person whose identity is being verified. Documents issued or made available by an official body are to be regarded as being independent of a person even if they are provided or made available to the casino operator by, or on behalf of, that person.[73]

6.11 These requirements apply to customers of both remote and non-remote casinos. Aside from these checks being a statutory requirement in the Regulations, they also help casino operators to avoid the commission of criminal offences under POCA.

---

[68] Regulation 27(7).
[69] Regulation 27(8).
[70] Regulation 27(9).
[71] Regulation 28.
[72] Regulation 28(10).
[73] Regulation 28(18).

6.12 The Regulations define casino as 'the holder of a casino operating licence'.[74] The holder of a casino operating licence does not need to repeat CDD if a customer visits another casino operated by that licensee, it may be conducted just once. 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. Casino operators should note that CDD is ongoing and may need updating for changes in the customer's circumstances and personal details.

6.13 The ways in which a casino operator meets the requirements for CDD and the extent of the measures it takes must reflect the risk assessment it has carried out, and its assessment of the level of risk arising in any particular case. This may differ from case to case.[75]

6.14 In assessing the level of risk arising in a particular case, casino operators must take account of factors including, among other things:

- the purpose of a customer account, transaction or business relationship
- the amount deposited by a customer or the size of the transactions undertaken by the customer
- the regularity and duration of the business relationship.[76]

6.15 A casino operator is not required to *continue* to apply CDD measures in respect of a customer where *all* of the following requirements are met:

- the operator has taken CDD measures in relation to the customer
- the operator has submitted a suspicious activity report under POCA or the Terrorism Act, and
- continuing to apply CDD measures in relation to the customer would result in the operator committing tipping off offences under POCA or the Terrorism Act.[77]

6.16 Casino 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.

6.17 Casino operators must be able to demonstrate to the Commission that the extent of the CDD measures they take are appropriate in view of the risks of money laundering and terrorist financing, including risks:

- identified by the operator's risk assessment
- identified by the Commission and in information made available by the Commission.[78]

Timing of verification

6.18 Casino operators must comply with the requirement to verify the identity of the customer, any person claiming to act on behalf of the customer and, where applicable, any beneficial owner before the establishment of a business relationship or the carrying out of the transaction.[79]

6.19 The Regulations, however, permit casino operators to complete verification during the establishment of a business relationship if:

- this is necessary so as not to interrupt the normal conduct of business

[74] Regulation 14(1)(b).
[75] Regulation 28(12).
[76] Regulation 28(13).
[77] Regulation 28(15).
[78] Regulation 28(16).
[79] Regulation 30(2).

- there is little risk of money laundering and terrorist financing occurring, but
- only provided that the verification is completed as soon as practicable after contact is first established with the customer.[80]

Ongoing monitoring

6.20 The Regulations require casino operators to conduct ongoing monitoring of a business relationship. This must include 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 casino's knowledge of the customer, the customer's business and risk profile
- undertaking reviews of existing records and keeping the documents or information obtained for the purpose of applying CDD measures up-to-date.[81]

6.21 Casinos are expected to approach this requirement on a risk-sensitive 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.

Enhanced customer due diligence and enhanced ongoing monitoring

6.22 Casino operators must apply enhanced customer due diligence measures and enhanced ongoing monitoring, in addition to the required CDD measures, to manage and mitigate the money laundering or terrorist financing risks arising in the following cases:

- in any case identified by the operator or in information provided by the Commission to the operator as one where there is a high risk of money laundering or terrorist financing[82]
- in any business relationship or transaction with a customer situated in a high-risk third country identified by the European Commission
- if the operator has determined that a customer or potential customer is a PEP, or a family member or known close associate of a PEP
- in any case where the operator discovers that a customer has provided false or stolen identification documentation or information and the operator proposes to continue to deal with the customer
- in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, and the transaction or transactions have no apparent economic or legal purpose
- in any other case which, by its nature, can present a higher risk of money laundering or terrorist financing.[83]

6.23 These enhanced measures:

- must include:
  - examining the background and purpose of the transaction, as far as reasonably possible

[80] Regulation 30(3).
[81] Regulation 28(11).
[82] A key source of information provided by the Commission in relation to where there is a high risk of money laundering or terrorist financing is *Money laundering and terrorist financing risk within the British gambling industry*. This risk assessment is updated at least annually and is available at www.gamblingcommission.gov.uk.
[83] Regulation 33(1).

    - increasing the degree and nature of monitoring of the business relationship in which the transaction is made, to determine whether the transaction or the relationship appear to be suspicious[84]
- depending on the requirements of the case, may also include, among other things:
    - seeking additional independent, reliable sources to verify information provided or made available to the casino operator
    - taking additional measures to understand better the background, ownership and financial situation of the customer, and other parties to the transaction
    - taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship
    - increasing the monitoring of the business relationship, including greater scrutiny of the transactions[85].

6.24 When assessing whether there is a high risk of money laundering or terrorist financing in a particular situation, and the extent of the measures which should be taken to manage and mitigate the risk, casino operators must take account of the following risk factors, among other things:

- whether:
    - the business relationship is conducted in unusual circumstances
    - the customer is resident in a geographical area of high risk
    - the product or transaction might favour anonymity
    - the situation involves non-face-to-face business relationships or transactions (as in the case of remote casinos), without certain safeguards such as electronic signatures[86]
    - payments will be received from unknown or unassociated third parties of the customer
    - new products and new business practices are involved, including new delivery mechanisms, and the use of new or developing technologies (such as virtual currencies) for both existing and new products
- the business relationship or transaction involves countries:
    - identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter money laundering or terrorist financing
    - identified by credible sources as having significant levels of corruption or other criminal activity, such as money laundering, terrorism, and the production and supply of illicit drugs
    - subject to sanctions, embargoes or similar measures issued by, for example, the European Union or the United Nations
    - providing funding or support for terrorism
    - that have organisations operating within their territory which have been designated, by the government of the UK, as proscribed organisations under the Terrorist Act or, by other countries, international organisations or the European Union as terrorist organisations
    - identified by credible sources (such as evaluations, detailed assessment reports or follow-up reports published by FATF, the International Monetary Fund, the World Bank, the organisation for Economic Cooperation and Development or other international bodies or non-governmental organisations) as not implementing requirements to counter money laundering and terrorist financing that are consistent with the FATF recommendations.[87]

[84] Regulation 33(4).
[85] Regulation 33(5).
[86] An electronic signature should be taken to mean data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign. Other safeguards mentioned by the European Supervisory Authorities in their Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 are electronic identification certificates issued in accordance with Regulation EU (No) 910/2014, and anti-impersonation fraud checks. If no safeguards are in place, non-face-to-face business relationships or transactions must be considered to present a high risk of money laundering or terrorist financing.
[87] Regulation 33(6).

6.25 The Commission recommends that casino operators also consider the following factors when assessing whether there is a high risk of money laundering or terrorist financing:

- the customer transacts with significant amounts of cash
- the customer provides false, forged or stolen identification documentation upon establishing a business relationship
- the customer transacts with multiple remote gambling operators, particularly where this occurs across multiple geographical areas
- the product, service or transaction involves peer-to-peer gaming
- the product is electronic roulette
- the product, service or transaction involves Ticket In/Ticket Out (TITO) or similar technology.[88]

6.26 In assessing whether there is a high risk of money laundering or terrorist financing, casino operators must bear in mind that the presence of one or more of the risk factors listed above may not always indicate that there is a high risk in a particular situation.[89]

Threshold approach

6.27 As discussed in paragraphs 6.3 to 6.5, the Regulations set out thresholds which, if customer transactions reach these levels, require the casino operator to apply customer due diligence measures. These limits are:

- in non-remote casinos the 'threshold approach for tokens' – identification and verification is required when a customer purchases from or exchanges with the casino tokens for use in gambling at the casino with a value of €2,000 or more
- in non-remote casinos the 'threshold approach for gaming machines' – identification and verification is required when a customer pays €2,000 or more for the use of gaming machines, or collects winnings amounting to €2,000 or more
- in remote casinos the 'threshold approach for remote gaming' – identification and verification is required when a customer deposits funds to take part in remote gambling or withdraws such funds or winnings amounting to €2,000 or more.

6.28 The threshold applies to the wagering of a stake or the collection of winnings, and is to be applied to single transactions or transactions that appear to be linked. Customers may execute a series of linked transactions that are individually below the €2,000 threshold but, when taken cumulatively, they meet or exceed the threshold. Transactions should be considered to be linked if, for example, they are carried out by the same customer through the same game or in one gaming session, or in the case of remote casinos, if they are part of the overall activity undertaken by a customer during a single period of being logged on to the operator's gambling facilities. These examples are not exhaustive and casino operators will need to consider whether there are other circumstances in which transactions are linked. Casino operators will also need to consider, among other things, whether a customer is deliberately spreading their wagering or collection of winnings over a number of transactions in order to circumvent the CDD requirements. They should also ensure that the triggering of the threshold by a customer is not evaded through the customer opening multiple accounts under fictitious names. The measures taken by the operator must be balanced against the requirement to conduct CDD upon establishing a business relationship with a customer (discussed in paragraphs 6.2 and 6.3), requirements for the timing of verification (discussed in paragraphs 6.18 and 6.19) and the need to conduct enhanced customer due diligence in high risk situations (discussed in paragraphs 6.22 to 6.26)[90]. This should be informed by the risk profile of the particular customer, including circumstances which alter the risk attributed to the customer (see paragraphs 6.6, 6.13 and 6.14).

---

[88] These factors are considered by the Commission in *Money laundering and terrorist financing risk within the British gambling industry*.
[89] Regulation 33(7).
[90] Remote casinos should note that, where no safeguards are in place, non-face-to-face business relationships or transactions must be considered to present a high risk of money laundering or terrorist financing, which requires the use of enhanced customer due diligence measures. See paragraph 6.24.

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

6.30 It should be noted that, under the Regulations, 'gaming machine' has the same meaning as that in the Act[91]. 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 tokens.

6.31 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 the threshold is picked up in good time to allow CDD to be conducted. Where the casino operator has a number of premises, the Commission will consider the use of the threshold approach for each casino premises rather than for an operator.

6.32 Casinos adopting the threshold approach may wish to defer both identification and verification until the threshold is triggered. Alternatively, they may consider that it is more practical to conduct both identification and verification on entry, or conduct identification on entry and defer verification until the threshold is triggered. For example, a premises based casino may operate a membership scheme where customers are identified on admission to the casino but verification only occurs once the threshold is triggered. 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 triggered. This is sometimes called the hybrid approach.

6.33 There may be 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. In deciding which approach to take, operators must satisfy themselves and the Commission on a premises-by-premises basis that they have effective procedures, controls and systems in place to track and monitor customers across all the products and platforms that are offered.

6.34 A key challenge for casinos wishing to adopt the threshold approach is keeping track of all an individual customer's purchases and exchanges of tokens, spend on gaming machines, and the collection of their winnings. However, it may be appropriate to do so in light of the known spend patterns in each premises.

6.35 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 and terrorist financing risk and spending profile at each premises.

6.36 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 deposits money 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 deposited. 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.

[91] Regulation 27(6)(a)(ii).

6.37 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.

Identification and verification on entry

6.38 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 gambling facilities (see paragraphs 6.18 and 6.19). Once the customer's identity is verified, they may commence gaming.

6.39 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 gambling. In non-remote casinos this does not allow guests of known customers a single entry without undertaking CDD. However, casino operators should consider using variations of the threshold CDD approach for guests of casino members.

Identification and verification

6.40 Applying CDD measures involves several steps. The casino operator is required to identify customers and then verify their identities, either upon entry or when reaching the threshold. Identification of a customer means being told or coming to know of the customer's identifying details, such as their name and address. Verification means obtaining some evidence which supports this claim of identity. The operator *identifies* the customer by obtaining a range of information about the customer. 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

6.41 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.

6.42 Casino operators should identify their customers by asking them for personal information, including name, home address and date of birth, or by using other sources of identity, including:

- identity documents, such as passports and photo card 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.

6.43 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 assessment about whether a customer's level of gambling is proportionate to their approximate income, or whether it is suspicious.

Verification

6.44 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, from banks).

No method of verification, either documentary or electronic, can conclusively prove that the customer 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 casino operators to verify this identity using an independent source. This is particularly relevant where the casino providing the confirmation is located in another jurisdiction.

6.45 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.

6.46 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

6.47 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'.

6.48 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.

6.49 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 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.

6.50 Some external electronic databases are accessible directly by casinos but it is 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.

6.51 A number of commercial agencies which access many data sources are accessible online by casino operators, and may provide 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.

6.52 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. This may be a source that requires an individual to prove their identity, or address, in some way in order to be included, as opposed to one where no such proof is required.

6.53 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 verification provider

6.54 Before using a commercial agency for electronic verification, casino operators should be satisfied that information supplied by the verification 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
- 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.

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

6.56 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
- a second match on an individual's full name and either his current address or his date of birth.

6.57 Commercial agencies that provide electronic verification use various methods of displaying results – for example, by the number of documents checked, or through scoring mechanisms. Casino 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

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

6.59 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 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, fake European Driving Permits, International Drivers Licenses and National Identity Cards which are freely available through the internet. 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.

6.60 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.

6.61 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.

6.62 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 photo card 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.

6.63 Alternatively, government issued documents without a photograph which incorporate the customer's full name may be used, 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.

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

- current signed passport
- birth certificate
- current photo card 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
- HMRC self-assessment statement or tax demand
- house or motor insurance certificate.

6.65 Customers who are not resident in the UK should be asked to produce their passport, national identity card or photo card 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.

6.66 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 (PEPs)

Definition

6.67 A PEP is an individual who is entrusted with prominent public functions, other than middle-ranking or more junior officials, including the following individuals:

- heads of state, heads of government, ministers and deputy or assistant ministers
- members of parliament or of similar legislative bodies
- members of the governing bodies of political parties
- members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances
- members of courts of auditors or of the boards of central banks
- ambassadors, chargés d'affaires and high-ranking officers in armed forces
- members of the administrative, management or supervisory bodies of state-owned enterprises
- directors, deputy directors and members of the board or equivalent function of an international organisation.[92]

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

- family members of the individuals listed above, including spouse, partner, children and their spouses or partners, and parents
- known close associates of the individuals listed above, including individuals with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relations, or who is a sole beneficial owner of a legal entity or arrangement set up for the benefit of the PEP.[93]

[92] Regulation 35(12) and (14). See paragraph 6.79 in relation to the treatment of PEPs.
[93] Regulation 35(12). See paragraph 6.79 in relation to the treatment of family members and known close associates of PEPs.

6.69 When deciding whether an individual is a known close associate of a PEP, casino operators need only consider information which is in their possession, or credible information which is publicly available.[94]

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

Risk-based approach to PEPs

6.71 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 casino operator needs to consider screening all customers for this purpose.

6.72 Establishing whether individuals are PEPs is not always straightforward and can present difficulties. Where casino operators need to carry out specific checks, they may be able to rely on an internet search 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. The International Monetary Fund, World Bank and some non-governmental organisations also publish relevant reports. If there is a need to conduct more thorough checks, or if there is a high likelihood of a casino operator having PEPs for customers, subscription to a specialist PEP database may be a valuable tool in assessing the risk.

6.73 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, 12 months after they change their job or retire[95]. The casino 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 customer is a PEP or is linked to one.

6.74 Although under the definition of a PEP an individual ceases to be so regarded after he has left office for 12 months, casino 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.[96]

PEPs requirements

6.75 Casino operators are required, on a risk-sensitive basis, to:

[94] Regulation 35(15).
[95] Regulation 35(9)(a).
[96] Regulation 35(9)(b).

- have in place appropriate risk management systems and procedures to determine whether a customer (or the beneficial owner of a customer) is a PEP, or a family member or known close associate of a PEP
- have approval from its senior management for establishing or continuing a business relationship with such persons
- take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or transaction with such persons
- where a business relationship is entered into, conduct enhanced ongoing monitoring of the business relationship with such persons.[97]

6.76 Each casino operator's policies and procedures should cover when and how customers will be checked for PEP status and 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 by senior management.

6.77 The appropriateness of the risk management systems and procedures adopted must take account of:

- the money laundering and terrorist risk assessment that the casino operator has conducted
- the level of risk of money laundering or terrorist financing inherent in the operator's business
- the extent to which that risk would be increased by a business relationship with a PEP, or a family member or know close associate of a PEP
- any relevant information made available by the Commission.[98]

6.78 Where the casino operator has determined that a customer or potential customer is a PEP, or a family member or known close associate of a PEP, the operator must assess:

- the level of risk associated with that customer
- the extent of the enhanced due diligence measures to be applied in relation to that customer, taking into account any guidance issued by the Commission or any other appropriate body (and approved by HM Treasury), and any relevant information made available by the Commission.[99]

6.79 There is a hierarchy of risk for individual PEPs, where some PEPs have higher relative risk and others have lower relative risk. The measures taken for particular PEPs should therefore be informed by the relative risk attributed to the PEP, including consideration of the jurisdiction from which they originate. The Financial Conduct Authority (the FCA) has published guidance in relation to the treatment of PEPs and, while casino operators are not subject to the rules made by the FCA[100], they are advised to consult this guidance when considering the level of risk posed by a particular PEP. The guidance provides advice on who should be treated as a PEP, who should be treated as a family member or known close associate of a PEP, and the level of risk posed by particular PEPs, family members and close associates. Among other things, it recommends that only those individuals in the UK who hold truly prominent positions should be treated as PEPs, and not to apply the definition to local government, more junior members of the senior civil service or anyone other than the most senior military officials[101]. However, this recommendation does not apply when dealing with PEPs from foreign jurisdictions.

6.80 A casino operator who proposes to have, or to continue, a business relationship with a PEP, or a family member or known close associate of a PEP must, in addition to the enhanced customer due diligence measures described in paragraphs 6.22 to 6.26:

---

[97] Regulation 33(5).
[98] Regulation 35(2).
[99] Regulation 35(3) and (4).
[100] Regulation 48(1).
[101] https://www.fca.org.uk/publication/finalised-guidance/fg17-06.pdf. See the Appendix to this guidance.

- have approval from its senior management for establishing or continuing the 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 or transactions with that person
- where the business relationship is entered into, conduct enhanced ongoing monitoring of the business relationship with that person.[102]

6.81 Where an individual who was a PEP is no longer entrusted with a prominent public function, casino operators must continue to apply the requirements for PEPs:

- for a period of at least 12 months after the date on which the individual ceased to be entrusted with a public function
- or for a longer period that the casino operator considers appropriate to address the risks of money laundering or terrorist financing in relation to that individual.[103]

6.82 When an individual who was a PEP is no longer entrusted with a prominent public function, casino operators are no longer required to apply enhanced customer due diligence measures to the family members or close associates of the PEP. The 12 month period referred to above does not apply in this case.[104]

Simplified customer due diligence

6.83 A casino operator is permitted to apply simplified customer due diligence measures in relation to a particular business relationship or transaction if it determines that the business relationship or transaction presents a low degree of money laundering and terrorist financing risk, taking into account its money laundering and terrorist financing risk assessment, any relevant information made available by the Commission and the risk factors in the following paragraph.[105] The casino operator's risk assessment should identify what products, services, transactions, customers or countries present a low degree of money laundering and terrorist financing risk. Remote casinos operators should note that business relationships and transactions with its customers cannot be considered to present a low degree of money laundering and terrorist financing risk, if no safeguards are in place (see paragraph 6.24).

6.84 When assessing whether there is a low degree of risk of money laundering and terrorist financing in a particular situation, and the extent of the simplified customer due diligence in that situation, casino operators must take account of the following risk factors, among other things:

- the country where the customer is resident is:
  - an EEA state
  - a third country which has effective systems to counter money laundering and terrorist financing
  - a third country identified by credible sources as having a low level of corruption or other criminal activity, such as terrorism, money laundering , and the production and supply of illicit drugs
  - a third country which, on the basis of credible sources, such as evaluations, detailed assessment reports or published follow-up reports published by FATF, the International Monetary Fund, the World Bank, the Organisation for Economic Co-operation and Development or other international bodies or non-governmental organisations, has requirements to counter money laundering and terrorist financing that are consistent with the

[102] Regulation 35(5).
[103] Regulation 35(9). This requirement does not apply to individuals who were no longer entrusted with a prominent public function before 26 June 2017 (Regulation 35(10)).
[104] Regulation 35(11).
[105] Regulation 37(1).

Recommendations published by FATF and effectively implements those Recommendations.[106]

6.85 In making an assessment of a low degree of risk, casino operators must bear in mind that the presence of one or more risk factors may not always indicate that there is a low risk of money laundering and terrorist financing in a particular situation.[107]

6.86 Where a casino operator applies simplified due diligence measures, it must:

- continue to comply with the customer due diligence requirements, but it can adjust the extent, timing or type of the measures it undertakes to reflect the determination it has made under paragraph 6.83 in regard to the low degree of money laundering or terrorist financing risk associated with a particular business relationship or transaction, and
- carry out sufficient monitoring of any business relationships or transactions subject to simplified measures to enable it to detect any unusual or suspicious transactions.[108]

6.87 A casino operator must discontinue applying simplified due diligence measures, if:

- it doubts the veracity or accuracy of any documents or information previously obtained for the purposes of identification or verification
- its money laundering and terrorist financing risk assessment changes and it no longer considers that there is a low degree of risk of money laundering and terrorist financing
- it suspects money laundering or terrorist financing, or
- any of the high risk situations or conditions in paragraph 6.22 apply.[109]

Reliance

6.88 A casino operator may rely on certain third parties to apply the required CDD measures, however, the operator remains liable for any failure to apply such measures.[110]

6.89 The third parties which may be relied on are:

- other persons who are subject to the requirements of the Regulations (financial institutions, credit institutions, auditors, insolvency practitioners, external accountants, tax advisers, independent legal professionals, trust or company service providers, estate agents, high value dealers, and other casinos)
- persons who carry on business in another EEA state (other than the United Kingdom) who is subject to requirements in national legislation implementing the Directive as an obliged entity, and is supervised for compliance with the requirements in the Directive
- persons who carry on business in a third country who are subject to requirements in relation to CDD and record keeping which are equivalent to those in the Directive, and are supervised for compliance with those requirements.[111]

6.90 A casino operator may not rely on a third party established in a country which has been identified by the EC as a high risk third country.[112]

6.91 When a casino operator relies on a third party to apply CDD measures, it:

[106] Regulation 37(3).
[107] Regulation 37(4).
[108] Regulation 37(2).
[109] Regulation 37(8).
[110] Regulation 39(1).
[111] Regulation 39(3).
[112] Regulation 39(4).

- must immediately obtain from the third party all the information needed to satisfy the requirements for the identification and verification of the customer, any beneficial owner and any person acting on behalf of the customer
- must have an arrangement with the third party that:
    - enables the operator to obtain from the third party immediately on request copies of any identification and verification data and other relevant documentation on the identity of the customer, beneficial owner or any person acting on behalf of the customer
    - requires the third party to retain copies of such data and documents for a period of five years.[113]

6.92 A casino operator will be treated as having complied with the requirements listed in the previous paragraph if:

- the operator is relying on information provided by a third party which is a member of the same group as the operator (for example, in the case of group companies with overseas casinos)
- that group applies CDD measures, rules on record keeping and programmes against money laundering and terrorist financing in accordance with the Regulations, the Directive or rules having equivalent effect
- the effective implementation of these requirements is supervised at group level by an authority of an EEA state with responsibility for implementation of the Directive or by an equivalent authority of a third country.[114]

6.93 A casino operator is permitted to apply CDD measures by means of an agent or an outsourcing service provider, provided that the arrangements between the operator and the agent or service provider make clear that the operator remains liable for any failure to apply the CDD measures.[115]

6.94 In this context, an outsourcing service provider is a person who performs a process, service or activity on behalf of the casino operator and is not an employee of the operator.[116]

6.95 Your attention is also drawn to paragraph 1.44 which highlights the need for operators to consider the risks posed by third parties they contract with.

Requirements to cease transactions or terminate relationship

6.96 Where a casino operator is unable to apply the required CDD measures in relation to a particular 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 a transaction with the customer other than through a bank account
- must terminate any existing business relationship with the customer
- must consider whether they are required to make a report, or a further report, to the NCA. [117]

6.97 Where the casino operator is required not to carry out a transaction with or for a customer through a bank account, this does not prevent money deposited in a customer's gambling account being repaid to the customer, provided that, where the operator is required to make a report to the NCA, the operator has a defence (appropriate consent) under POCA, or consent under the Terrorism Act, to the transaction.[118]

---

[113] Regulation 39(2).
[114] Regulation 39(6).
[115] Regulation 39(7).
[116] Regulation 39(8).
[117] Regulation 31.
[118] Regulation 31(2).

6.98 Casinos must therefore have clear policies in place on how they will manage situations where they are unable to apply the CDD measures.

Requirements for remote casinos

6.99 Where remote casino operators are unable to complete or apply the required CDD measures[119] in relation to a particular customer at the point the CDD threshold for transactions[120] is reached, and are accordingly required to cease transactions or terminate the business relationship with the customer[121], they should adopt the following procedure:

- at the point where the threshold is reached, remote casino operators should put all funds 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 CDD cannot be completed, then the operator must proceed in line with regulation 31(1)(c) and terminate the existing business relationship with the customer
- if funds are to be repaid, then the amount repaid should consist of all funds owed to the customer at the point that the threshold was reached, plus all deposits made at that point and thereafter
- funds should be refunded back to the originating account, and:
    - there should be appropriate risk mitigation
    - where it is suspected that the funds are the proceeds of crime, remote casino operators should submit SARs or seek a defence (appropriate consent) before refunding any of the funds
- 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 or terrorist financing concern?
        - above €2,000 – is the amount above the threshold for CDD?
    - there should be appropriate risk mitigation
    - where it is known or suspected that the funds are the proceeds of crime, remote casino operators should submit SARs or seek a defence (appropriate consent) before refunding any of the funds
- 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).

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

List of persons subject to financial sanctions

6.101 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

[119] These measures are discussed in paragraphs 6.8 to 6.17.
[120] See paragraphs 6.3 to 6.5.
[121] In accordance with regulation 31(1).

persons and entities. There are specific financial restrictions targeted at organisations and entities involved in terrorism and terrorist financing.

6.102 Financial restrictions in the UK are governed by various pieces of legislation. The purpose of imposing financial restrictions is to restrict 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.

6.103 A list of all financial restrictions currently in force in the UK is maintained by HM Treasury's Office of Financial Sanctions Implementation (OFSI). The Consolidated List of persons designated as being subject to financial restrictions can be found on the government website at: www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets. The purpose of the Consolidated List is to draw together, in one place, all the names of designated persons for the various financial restrictions regimes effective in the UK. Further information on financial restrictions, including guidance, can be found on the OFSI website: www.gov.uk/government/organisations/office-of-financial-sanctions-implementation.

6.104 There are prohibitions for carrying out certain activities or behaving in a certain way if financial sanctions apply. This will depend on the exact terms of the EU or UK legislation which imposes the financial sanction in the given situation.

6.105 Further information regarding the prohibitions can be found in the OFSI publication available here: www.gov.uk/government/publications/financial-sanctions-faqs.

6.106 OFSI 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 OFSI 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, OFSI can be contacted using the contact details provided below.

6.107 Casino operators need to have the necessary policies, procedures and controls 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 OFSI 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.

6.108 OFSI may also be contacted to provide guidance and to assist with any concerns regarding financial restrictions at:

Office of Financial Sanctions Implementation
Tel: 020 7270 5454 (Weekdays 9am to 5pm)
Email: ofsi@hmtreasury.gsi.gov.uk

6.109 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 OFSI, as this would be a breach of the financial restrictions. OFSI should be informed immediately and the transaction suspended pending their advice. No funds should be returned to the designated person. The operator may also need to consider whether there is an obligation also to report to the NCA under POCA or the Terrorism Act.

6.110 Written reports can be made to OFSI via email.

6.111 Casino operators should consider the likelihood of sanctioned persons using the casino's facilities, taking into account matters such as where the person is resident, and the local demographics of the casino and the its customer base. Operators should bear in mind that

sanctioned persons are not exclusively resident abroad, but may also live and operate in the UK and use either a high end casino or a small provincial casino.

6.112 Casino operators should also note that PEPs and financial sanctions cannot be conflated as the requirements in relation to each are different. The Regulations do not prohibit doing business with a PEP, whereas there is a prohibition on doing business with a person on the financial sanctions list, so the way in which casino operators manage the respective risks should be different.

7 Record keeping

General legal and regulatory requirements

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.

7.2 The casino 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 or terrorist financing 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
- employee training records
- internal and external SARs, including decisions and actions taken by the nominated officer
- contact between the nominated officer and law enforcement or the NCA, including records connected to requests for a defence (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.

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, or
- a 'business relationship', depending on the circumstances.

Business relationships

7.5 A business relationship is a business, professional or commercial relationship between a casino operator and a customer which arises out of the business of the casino operator and is expected by the operator, at the time when the contact is established, to have an element of duration.[122] Casino operators are advised to interpret this definition widely.

7.6 A business relationship with a customer of a casino operator:

- is likely to occur when, for example:

[122] Regulation 4(1).

    - a customer opens an account with the casino operator or becomes a member of a casino (when a membership scheme is operated by the casino), or
    - a customer obtains a cheque cashing facility
- may occur when, for example:
    - the casino starts tracking a customer's drop/win figures, other than to establish when the customer triggers the €2,000 threshold for CDD.

7.7 The list above is not exhaustive and a casino operator will need to form its own view of when contact is established, or circumstances otherwise arise, with a customer from which it expects, or it could reasonably be inferred that it expects, that the relationship with the customer will have an element of duration. The Commission accepts that this may not necessarily be the case when a casino operator permits a customer to join a casino loyalty scheme.

7.8 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 casino's knowledge of the customer, the customer's business and risk profile.[123]

7.9 As noted in paragraph 6.21, casinos are expected to approach this requirement on a risk-sensitive 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.

Other casino customers

7.10 Some casino customers may not fall into the business relationship definition. 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

7.11 In relation to the evidence of a customer's identity, casino operators must keep a copy of any documents or information obtained to satisfy the CDD measures required under the Regulations.[124]

7.12 A casino operator may often hold additional information beyond identity in respect of a customer for the purposes of wider CDD. As a matter of best practice, this information and any relevant documents should also be retained.

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.[125] 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

[123] Regulation 28(11).
[124] Regulation 40(2).
[125] Regulation 28(11).

Act. How these issues which will be dealt with in practice should be covered in the casino's policies, procedures and controls.

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 casino 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)

7.15 The requirement to keep supporting records is linked to 'business relationships' which is defined in the Regulations[126] and the extent and nature of records created. In many casinos, customers (regardless of whether or not they have formed a business relationship) purchase chips with cash at gaming tables where, in low risk situations, no records are created and therefore are not available to be kept.

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, procedures and controls what records will be created in light of the known spending patterns and the assessed money laundering and terrorist financing risks at each premises.

7.17 Some casinos 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. Where this process is used, it should be the subject of ongoing risk assessment for each premises and the records created during the process should also be retained.

7.18 Any casino operator devising its record keeping policy and procedure should decide how its business fits within the definition of 'business relationship'. 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 or terrorist financing risk situations.

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 7.10, for each customer. There is no requirement to keep detailed records for each customer for each table or game for AML purposes. However, HMRC may require casino operators to maintain records for each table or game, but not broken down by each customer's transactions.

Supporting records (remote casinos)

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 deposit and withdrawal figures for each named customer.

[126] Regulations 3 and 4.

Supporting records (gaming machines)

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 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.

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
- appropriate action is taken on the findings of any further examination.

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
- 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.

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.

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 casino 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

7.26 Records of identification and verification of customers must be kept for a period of five years after the business relationship with the customer has ended, for example where the customer closes his gambling account with the operator or ceases to visit or use the casino.[127]

7.27 Supporting records must be retained for a period of five years from the date the business relationship ended.[128] This creates a rolling five year history of drop/win data.

7.28 Upon expiry of the five year retention period, any personal data must be deleted unless:

- the casino operator is required to retain records containing personal data by or under any law or the purposes of any court proceedings
- the subject of the data has agreed to the retention of the data, or
- the casino operator has reasonable grounds for believing that records containing the personal data need to be retained for the purposes of legal proceedings.[129]

7.29 Records of internal and external reports on suspicious activity should be retained for five years from when the report was made.

[127] Regulation 40(3).
[128] Regulation 40(3).
[129] Regulation 40(5).

Form in which records are to be kept

7.30 Most casino 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:

- by way of original documents
- by way of photocopies of original documents
- on microfilm
- in scanned form
- in computerised or electronic form.

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

7.32 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.[130]

Data protection

7.33 Any personal data obtained by casino operators for the purposes of the Regulations may only be processed for the purposes of preventing money laundering and terrorist financing.[131]

7.34 Personal data should not be used for any other purpose unless:

- use of the data is permitted by or under any law other than the Regulations, or
- the casino operator has obtained the agreement of the subject of the data to the proposed use of the data.[132]

7.35 Casino operators are obliged to provide new customers with the following information before they establish a business relationship with them:

- the registrable particulars of the operator
- a statement that any personal data received from the customer will be processed only for the purposes of preventing money laundering or terrorist financing, or as permitted by the circumstances described in paragraph 7.34 above.[133]

8 Suspicious activities and reporting

Introduction

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

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

that a person is engaged in money laundering or terrorist financing, including criminal spend, or attempting to launder money or finance terrorism. In this guidance, these obligations are collectively referred to as 'grounds for knowledge or suspicion'.

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

[130] Regulation 83(1).
[131] Regulation 41(1).
[132] Regulation 41(3).
[133] Regulation 41(4).

- each casino 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
- the operator should ensure that employees are appropriately trained in their obligations, and in the requirements for making reports to their nominated officer.

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. Under POCA, the nominated officer is required to make a report to the NCA as soon as is practicable if he has grounds for suspicion that another person, whether or not 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?

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. Knowledge can be inferred from the surrounding circumstances, so, for example, a failure to ask obvious questions may be relied upon by a jury to infer knowledge[134]. The knowledge must, however, have come to the casino 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 casino 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.[135]

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.

8.6 Whether a person holds a suspicion or not is a subjective test. If a person thinks a transaction is suspicious they are not required to know the exact nature of the criminal offence or that particular funds are definitely those arising from the crime. The person may have noticed something unusual or unexpected and, after making enquiries, the facts do not seem normal or make commercial sense. It is not necessary to have evidence that money laundering is taking place to have suspicion.

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

[134] Refer to *Baden v Societe Generale pour Favouriser le Developpement du Commerce et de l'Industrie en France* [1983] BCLC 325.
[135] http://www.legislation.gov.uk/ukpga/2002/29/part/7.

concern escalates following further enquiries, it is reasonable to conclude that the transaction is suspicious and will need to be reported to the NCA.

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. 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.

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 have suspicion that money laundering has taken place.

What is meant by reasonable grounds to know or suspect?

8.10 In addition to establishing a criminal offence relating to failing to report when there is 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.

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.

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 bank notes 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

8.14 Employees of a casino operator have a legal defence if they report to the nominated officer where they have grounds for knowledge or suspicion of money laundering or terrorist financing. 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, must be made as soon as is practicable.

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 or terrorist financing. 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.

8.16 Once an employee has properly 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 satisfied his statutory obligation.

Evaluation and determination by the nominated officer

8.17 The casino 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 is being considered.

8.18 If the nominated officer decides not to make a report to the NCA, 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 be taken to imply that the casino 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

8.20 To avoid committing a failure to report offence, the nominated officer must make a disclosure to the NCA 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 a defence (consent) to proceed with the transaction or activity, is the UK Financial Intelligence Unit (UKFIU) within the NCA.

8.21 The nominated officer must report to the NCA 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 or terrorist financing. Such reports must be made as soon as is practicable after the information comes to the nominated officer.

8.22 In addition, depending on the circumstances, a casino 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 officer 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.

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[136]

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

- **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 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.

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

  SAR Online is the NCA's preferred method for small and medium sized reporting entities 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 at: www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu/how-to-report-sars.

  Completed forms should be posted to UKFIU, PO Box 8000, London, SE11 5EN. If using the form to request a defence (appropriate consent), it should be faxed immediately to 0207 238 8286, but it is not necessary to post and fax a 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, namely reporters with more than 10,000 reports a month. If an operator believes this would be the most appropriate method of reporting for their group, contact the UKFIU on 0207 238 8282 to discuss the matter.

8.25 Casino operators should include in each SAR as much relevant information about the customer, transaction or activity that it has in its records. The NCA has published a glossary of terms which they prefer operators to use when completing SARs.[137] This will assist in consideration of the report by the NCA.

8.26 Casino 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?

[136] Remote casino operators, particularly those based in a foreign jurisdiction, should consult the Commission's advice note on *Anti-money laundering: Suspicious activity reporting requirements for remote operators*. It is intended to assist remote operators in determining to which body or Financial Intelligence Unit (FIU) known or suspected money laundering activity should be reported, and the circumstances in which a defence (appropriate consent) should be sought.

[137] http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu/how-to-report-sars

- 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)?

8.27 In order that an informed overview of the situation may be maintained, all contact between the casino operator and law enforcement agencies should be controlled through, or reported back to, the nominated officer or a deputy acting in the absence of the nominated officer. The NCA may apply to the magistrates' court (or, in Scotland, the sheriff) for an order (a further information order), following the submission of a SAR, requiring the nominated officer to provide more information in respect of the SAR[138]. Law enforcement agencies may also apply for a disclosure order requiring any person considered to have information relevant to an investigation to answer questions, provide information or to produce documents[139].

8.28 POCA also makes provision for the voluntary sharing of information between persons in the regulated sector when deciding whether to submit a SAR, and joint SARs by persons in the regulated sector, subject to certain limitations. The exchange of information in these circumstances is protected from breaching any confidentiality obligations or other restrictions.[140]

Requesting a defence

8.29 If casino 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 a SAR to the NCA this can provide a defence. There is a statutory mechanism which allows the NCA either to grant or refuse the 'prohibited act' going ahead, or to prevent the suspected money laundering going ahead[141]. This statutory mechanism is called 'appropriate consent' and is referred to by the NCA as *Requesting a defence from the NCA under POCA and TACT*.[142]

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

- concealing, disguising, converting, transferring or removing criminal property[143]
- facilitating the acquisition, retention, use or control of criminal property by, or on behalf of, another person[144]
- acquisition, use or possession of criminal property[145].

These are referred to as 'prohibited acts'.

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

8.32 Nominated officers need to consider how they will approach their reporting obligations and consider:

---

[138] Section 339ZH of POCA.
[139] Section 357 of POCA.
[140] Sections 339ZB to 339ZG of POCA.
[141] Section 335 of POCA.
[142] http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu/seeking-consent-for-financial-transactions
[143] Section 327 of POCA.
[144] Section 328 of POCA.
[145] Section 329 of POCA.

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

8.33 A nominated officer, police constable, 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.[146] However, it should be noted that the NCA is the only body able to issue formal notification of a defence (consent) by means of an official NCA letter, which the nominated officer can then retain for his records.

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

- consent is not refused within seven working days (beginning with the day after the notice is given)
- if consent is refused and following such refusal, the 'moratorium period' (31 calendar days starting with the day on which the person receives notice that consent to the doing of the act is refused) has expired (but see paragraph 8.35).[147]

Although notice can be given to a constable or customs officer, there is a need to ensure that the practices of all law enforcement agencies are consistent in this area. Therefore, the NCA operates as the national centre for all SARs and for the issue of decisions concerning the granting or refusal of a defence (appropriate consent). To avoid confusion requests for a defence (consent) should be routed through the NCA. See paragraphs 8.45 to 8.56 for more detail.

8.35 Casino operators should be aware that the NCA and other authorities, such as the FCA and Serious Fraud Office, can apply to the Crown Court (or, in Scotland, the sheriff) for an order to extend the moratorium period for a further 31 days. An order can be given on up to six occasions which allows the moratorium period to be extended for a maximum period of 186 days in total. To grant an order for an extension, in each case the Court must be satisfied that the NCA or other authority's investigation is being carried out "diligently and expeditiously", additional time is needed to complete the investigation and an extension would be reasonable in the circumstances.[148]

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

- the NCA employee has provided a defence (consented to the transaction)
- a defence (consent) is not refused within seven working days (beginning with the day after the notice is given)
- if a defence (consent) is refused and following such refusal, the 'moratorium period' (31 calendar days starting with the day on which the person receives notice that consent to the doing of the act is refused) has expired (but see paragraph 8.35).[149]

8.37 Reporting suspicious activity before or reporting after the event are not equal options which a casino 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.[150] Where a customer request is received prior to a transaction or activity taking place, or arrangements being put in place (for example, where a customer requests the opening of a gambling account), and there is knowledge or suspicion, or reasonable grounds for suspicion, that the transaction, arrangements, or the funds/property involved, may relate to money laundering, a SAR must

[146] Section 335(1) of POCA.
[147] Section 335(2) of POCA.
[148] Section 336A of POCA.
[149] Section 336 of POCA.
[150] Section 327(2)(b) of POCA.

be submitted to the NCA and a defence (consent) sought to proceed with that transaction or activity. In such circumstances, it is an offence for a nominated officer to agree to a transaction or activity going ahead within the seven working day notice period from the working day following the date of disclosure, unless the NCA provides a defence (gives consent).[151]

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

8.39 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. In these circumstances it may sometimes not be feasible or practical to obtain a defence (appropriate consent) prior to or during a transaction. Knowledge or suspicion of money laundering or terrorist financing may be triggered after a customer has completed all the stages of a gambling transaction; that is, they have bought in, they have played and they have cashed out. Under those circumstances, it may be reasonable to report after the transaction. However, the defence of 'reasonable excuse' when reporting after the transaction is untested by case law and should be considered on a case-by-case basis.[152] Where the relationship with the customer is expected to have an element of duration and involve numerous transactions, it is advisable to seek a defence (consent) prior to transacting with the customer.

8.40 Casinos should include in their policies, procedures and controls details on how they will manage circumstances where there is knowledge or suspicion of money laundering or terrorist financing. If knowledge or suspicion is present, particularly if this occurs out of normal office hours, there must be a mechanism for involvement of the senior manager on duty and contact with the nominated officer 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.

8.41 The nominated officer will need to think very carefully about whether or not 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.

8.42 Casino 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 an increasing level of suspicion of money laundering, or to actual knowledge of money laundering, operators must seriously consider whether they wish to allow the customer to continue using their gambling facilities. Casino operators are, of course, free to terminate their business relationships if they wish and, provided this is handled appropriately, 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.

8.43 How customers suspected of money laundering or terrorist financing will be dealt with is an important area of risk management for all casino operators. They should deal with the

[151] Section 336(3) and (4) of POCA.
[152] Section 327(2)(b) of POCA.

issue in their policies, procedures and controls. As all operators are at risk of committing the principal offences, it is advisable to consider these issues carefully before they arise in practice.

8.44 For example, the casino operator may consider one transaction to be suspicious and report it to the NCA as such, but may be less concerned that all of an individual's future transactions are suspicious. In these circumstances, each transaction should be considered on a case-by-case basis and reports made accordingly, and a defence (appropriate consent) sought where necessary. Where subsequent reports are also made after actual or suspected money laundering or terrorist financing 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 a defence (appropriate consent) was not requested before the suspected money laundering or terrorist financing took place.

Applying for a defence

8.45 Where SAR Online is used and a defence (appropriate consent) is needed, this can be done by ticking the 'consent requested' box. Alternatively, requests can be faxed to the NCA UKFIU Consent Desk (see the NCA website www.nationalcrimeagency.gov.uk). You are advised to make it explicit in your report that you are seeking a defence (consent) from the NCA.

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

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

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

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

8.49 *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.

8.50 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 a defence (consent). To avoid confusion those making requests for a defence (consent) should route requests through the NCA. The decision making process will consist of a collaborative effort between the NCA and the other law enforcement agencies, with the latter providing a

recommendation to the NCA. While the final decision will be taken by the NCA, in most cases it is likely to be based largely on the recommendation provided by the interested law enforcement agency.

8.51 All requests for a defence (consent) are dealt with by the NCA on a case-by-case basis. It may take the maximum of seven working days to deal with a defence (consent) request, however, in most cases the NCA is able to respond to requests for a defence (consent) within three days.[153] Nominated officers should take this into account when deciding whether it is practical and reasonable to request a defence (consent) prior to the transaction or activity rather than making a report after the transaction or activity.

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

8.53 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 casino operator. Even if a defence (consent) is obtained from the NCA, the operator is not obliged to proceed with the transaction or arrangement.

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

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

8.56 The NCA cannot give advice to nominated officers and casino operators in relation to the specific circumstances where SARs should be submitted or the terms for requesting a defence (appropriate consent). Comprehensive guidance on requesting a defence is available on the NCA's website. We draw your attention, 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*[154].

Suspicious activity reporting requirements for remote casinos

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

[153] NCA Annual Report.
[154] Available from www.nationalcrimeagency.gov.uk

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

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

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

Suspicious activity reporting

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

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

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

8.64 These reporting requirements are summarised in the table below:

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

* See paragraphs 8.57 and 8.58 ** Britain means England, Scotland and Wales

Applying for a defence

8.65 Where remote casino operators wish to make use of the defences provided by sections 327(2)(a), 328(2)(a) and 329(2)(a) of POCA where they believe that, by proceeding with a transaction with a British customer, they will be committing a prohibited act, they should apply for a defence (appropriate consent), in accordance with section 335 of POCA, from the NCA.[155]

Failing to report

8.66 POCA and the Terrorism Act create offences of failing to report suspicious activity[156]. Where a person fails to comply with the obligations to make disclosures to a nominated officer and/or the NCA 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.

8.67 For all failure to disclose offences under POCA, it will be necessary to prove that the person or nominated officer either:

- knows the identity of the money launderer or the whereabouts of the laundered property
- believes the information on which the suspicion was based may assist in identifying the money launderer or the whereabouts of the laundered property.[157]

8.68 Casino operators and nominated officers, therefore, must comply with the reporting requirements imposed on them by POCA and the Terrorism Act.

After a report has been made

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

8.70 The investigating officer will 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

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

[155] See paragraphs 8.45 to 8.56.
[156] Sections 330 and 331 of POCA, and section 19 of the Terrorism Act.
[157] Sections 330(3A) and 331(3A) of POCA.

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

8.72 Under section 342 of POCA a person also commits an offence if the person:

- 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
- makes a disclosure which is likely to prejudice the investigation
- 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.

8.73 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 the person:

- 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.[158]

8.74 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[159]. There are a number of disclosures which are permitted and that do not give rise to these offences (permitted disclosures) – see paragraphs 8.65 to 8.67.

8.75 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[160]. 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.

8.76 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 8.77 to 8.79).

8.77 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:

---

[158] Section 342(6) of POCA.
[159] Sections 21D and 39 of the Terrorism Act.
[160] 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.[161]

8.78 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.[162]

8.79 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
- 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.[163]

8.80 The fact that a transaction is notified to the NCA before the event, and the NCA does not refuse a request for a defence (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.

8.81 This means that a casino operator:

- cannot, at the time, tell a customer that a transaction is being delayed because a report is awaiting a defence (consent) from the NCA
- 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 agrees, or a court order is obtained permitting disclosure
- cannot tell the customer that law enforcement is conducting an investigation.

8.82 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 NCA website (www.nationalcrimeagency.gov.uk).

8.83 The existence of a SAR cannot be revealed to any customer of the casino at any time, whether or not a defence (consent) has been requested. However, there is nothing in POCA which prevents casino 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 or a nominated officer, or that a money laundering investigation is being carried out or is being contemplated.

8.84 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.

[161] Section 333D of POCA and section 21G of the Terrorism Act.
[162] Section 333B of POCA and section 21E of the Terrorism Act.
[163] Section 333D of POCA and section 21G of the Terrorism Act.

8.85 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 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.

8.86 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 HM Treasury must be taken into consideration by any court considering whether this offence has been committed[164].

Interaction with customers

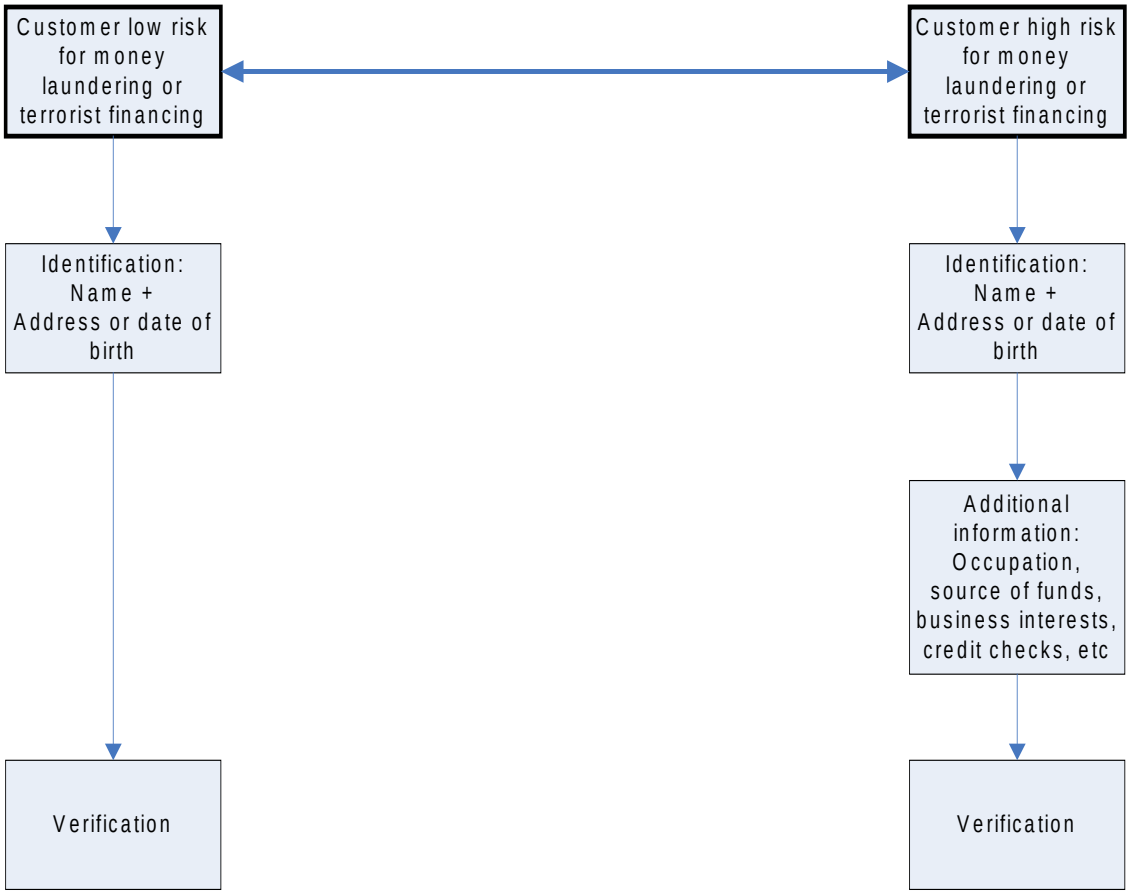
8.87 Normal customer enquiries will not, in the Commission's view, amount to tipping off or prejudicing an investigation under POCA, unless you know or suspect that a SAR has already been submitted and that an investigation is current or impending and make the enquiries of the customer in a way that 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.

8.88 If patterns of gambling lead to an increasing level of suspicion of money laundering, or even to actual knowledge of money laundering, casino operators should seriously consider whether they wish to allow the customer to continue using their gaming facilities. If a casino 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 a defence (appropriate consent).

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

[164] Sections 330 and 331 of POCA and Regulation 86(2).

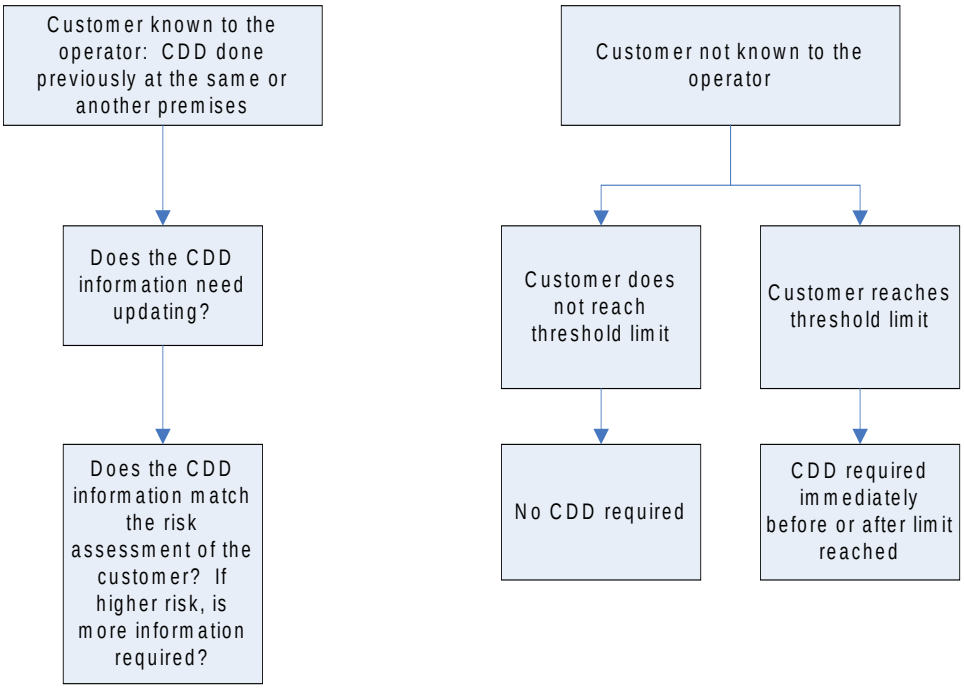
Figure 1: Risk-based approach



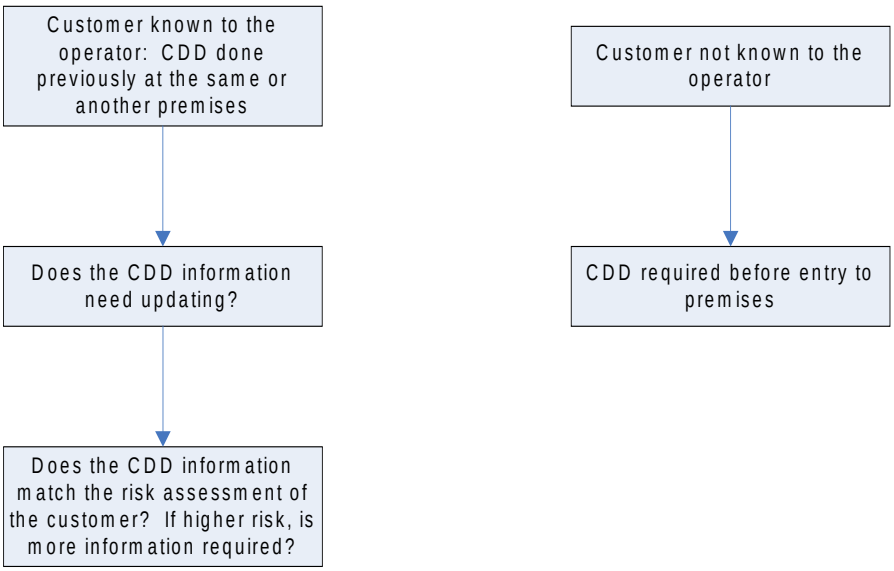
Note:
Casino operators should undertake risk assessments of each premises and each remote site and:
(a) look at the average drop/win per customer, and
(b) risk assess each customer.

Figure 2: Customer due diligence

Threshold model

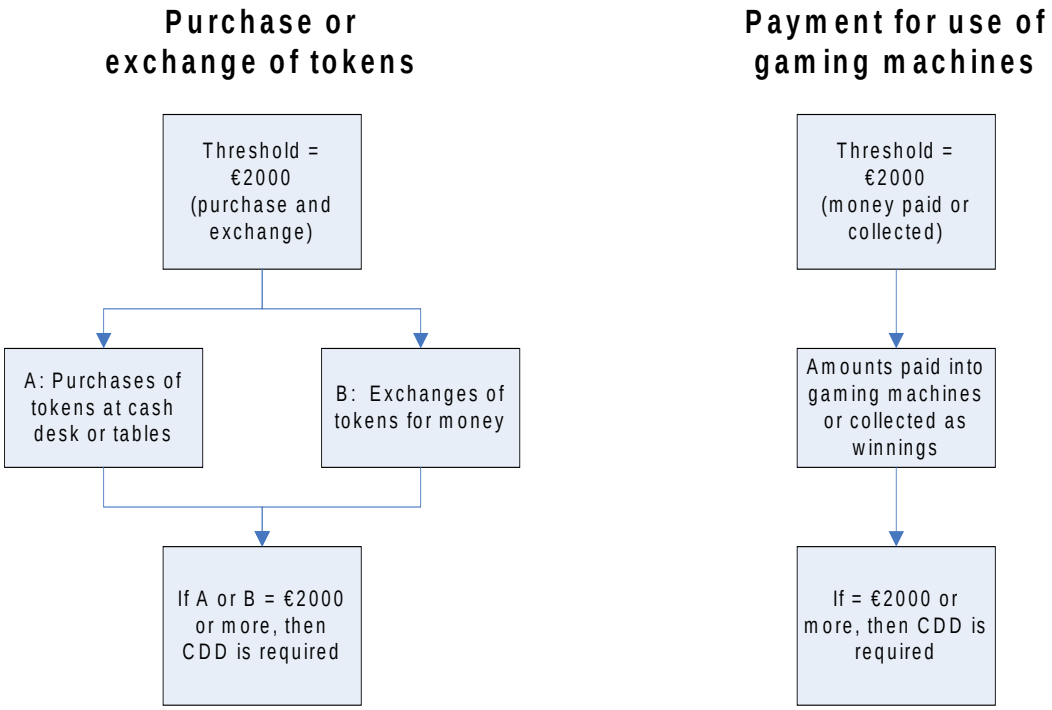


On entry model



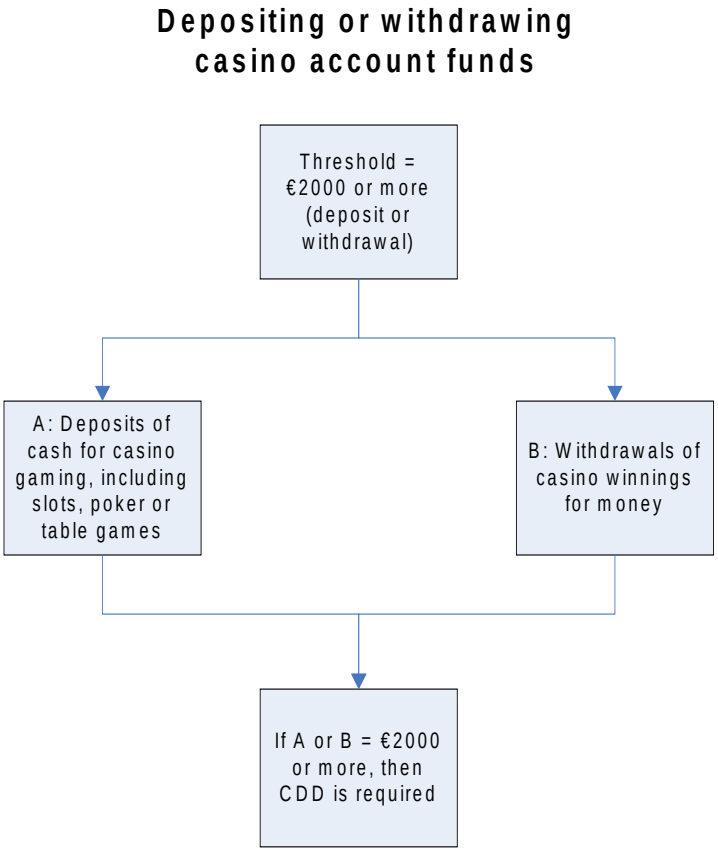
Notes:
1. Operator to be reasonably satisfied that the customer is who they claim to be.
2. The requirement applies to an operator, not to each premises.
3. Identification: Name, plus residential address or date of birth.
4. Verification: Documents or electronically.
5. Records of CDD to be kept for 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) – tokens and gaming machines



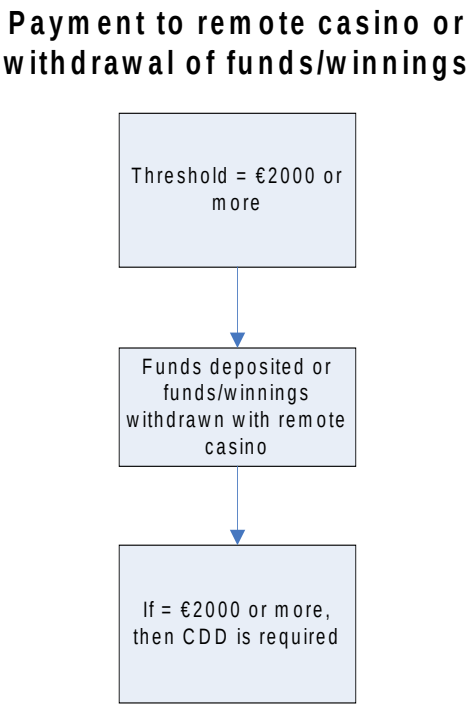
Notes:
1. A customer could spend €1800 on tokens and a further €1800 in a gaming machine and not reach the threshold.
2. Risk-based approach – operator analysis of spending behaviours at each premises and an objective assessment made of the likelihood of customers reaching either threshold. Measures 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



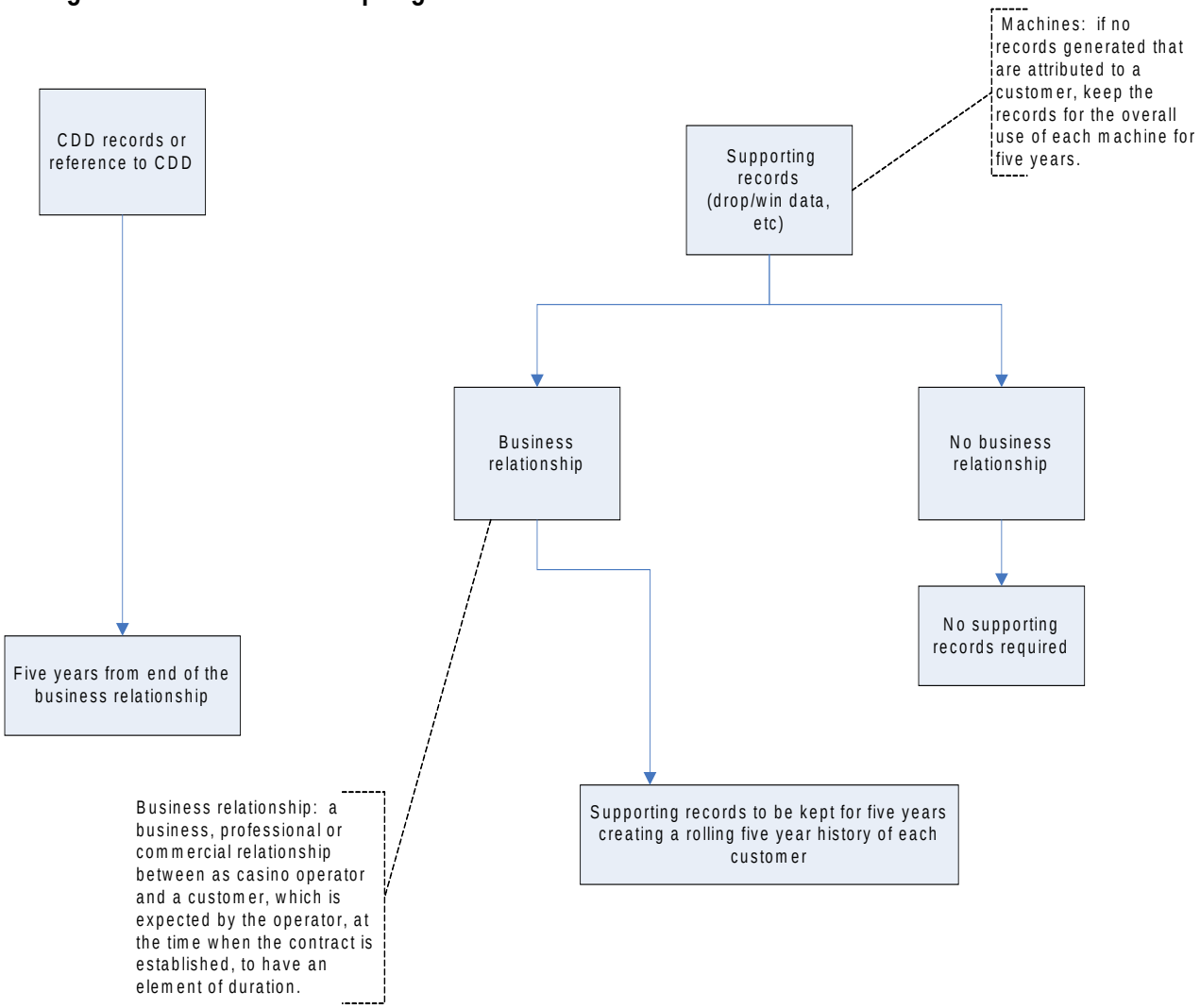
Note:
Risk-based approach – operator analysis of spending behaviours at each premises and an objective assessment made of the likelihood of customers reaching the threshold. Measures then put in place need to capture all customers likely to hit the threshold.

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



Note:
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.

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.

Figure 7: Reasonable grounds to suspect (objective test)

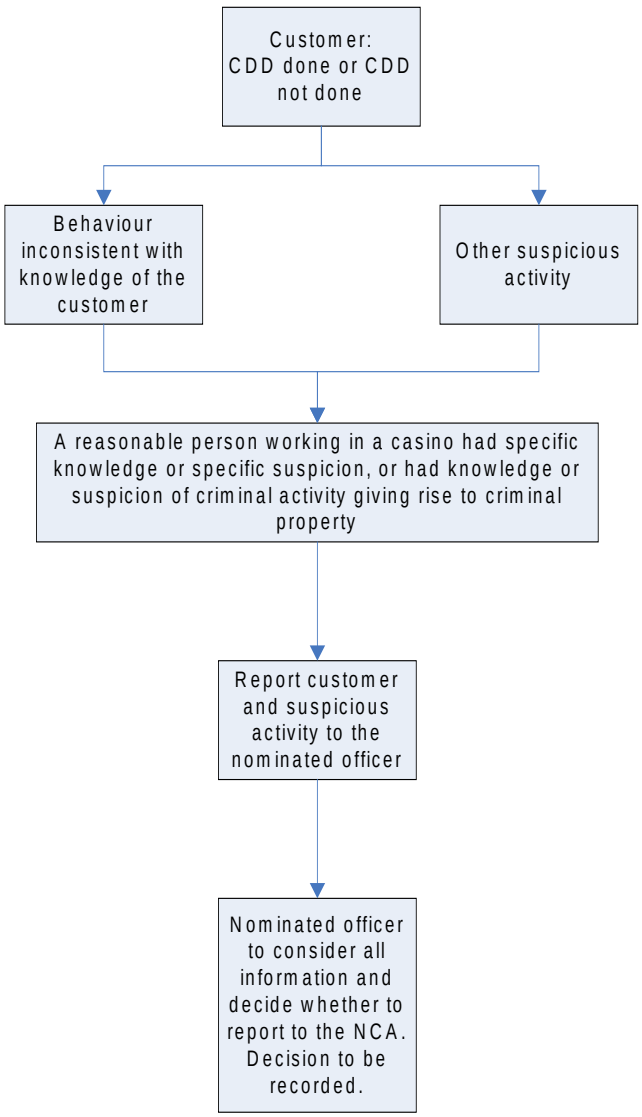


Figure 8: Knowledge or suspicion of money laundering or terrorist financing (subjective test)

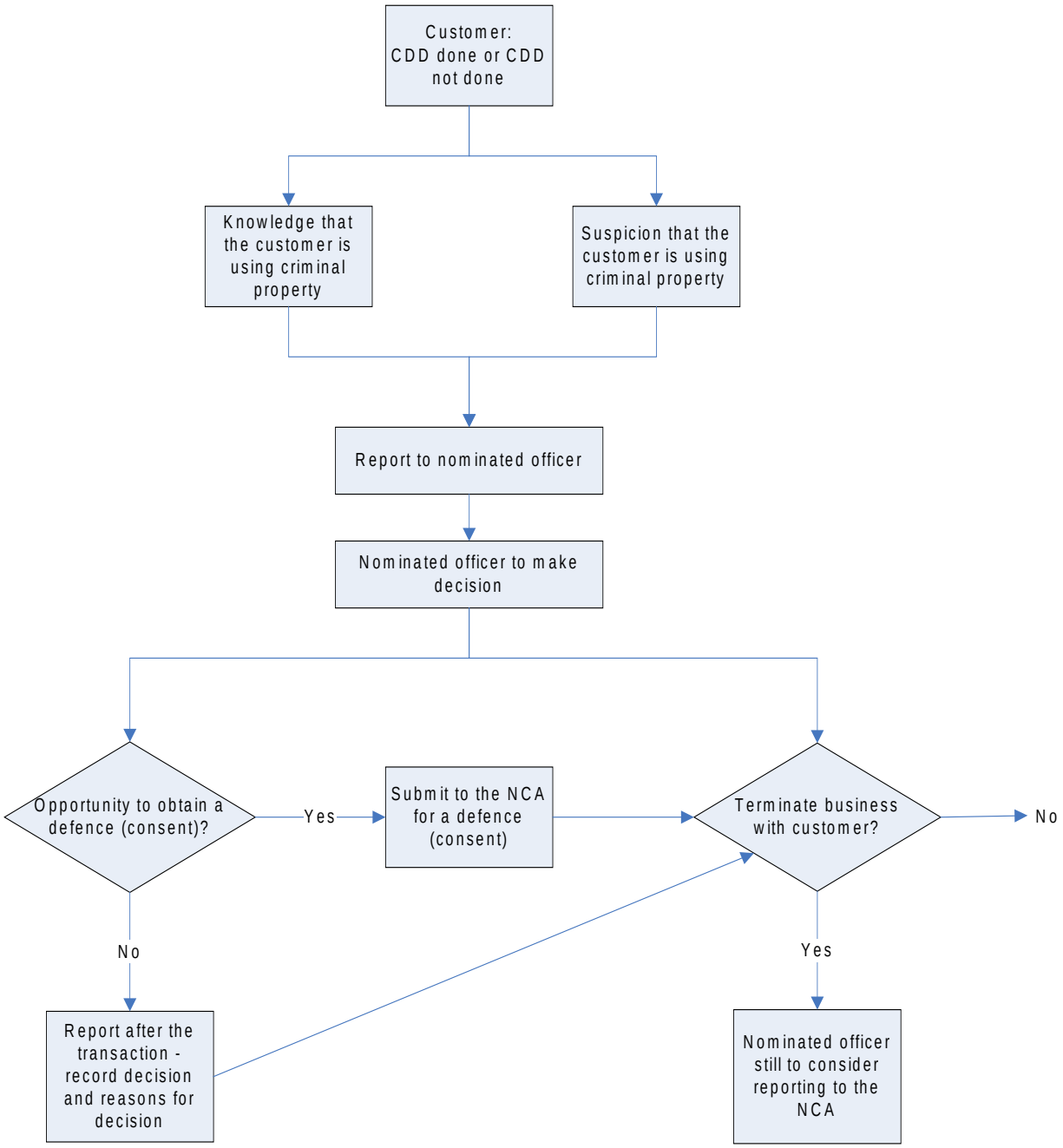


Figure 9: Defence under POCA or Terrorism Act

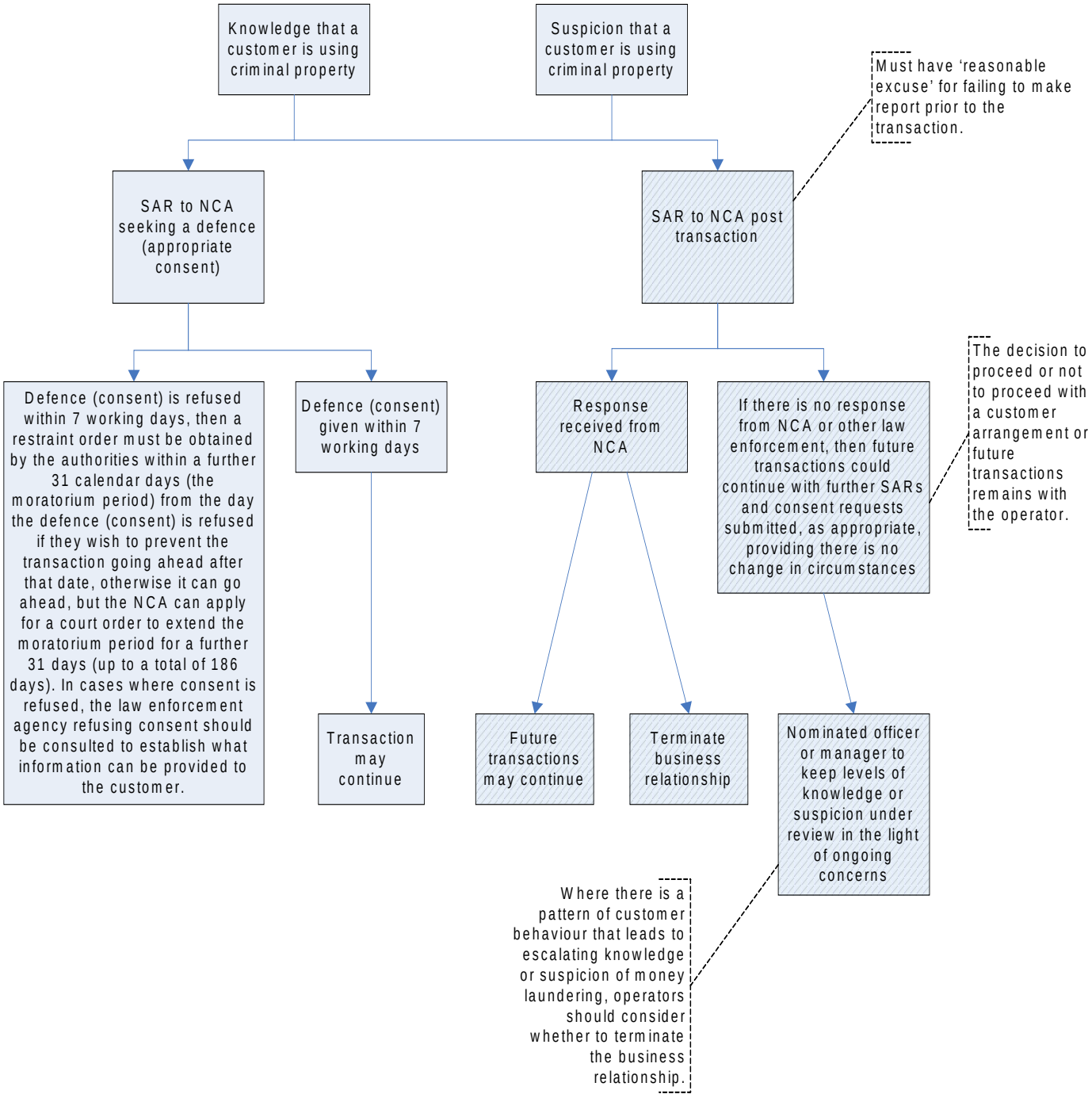
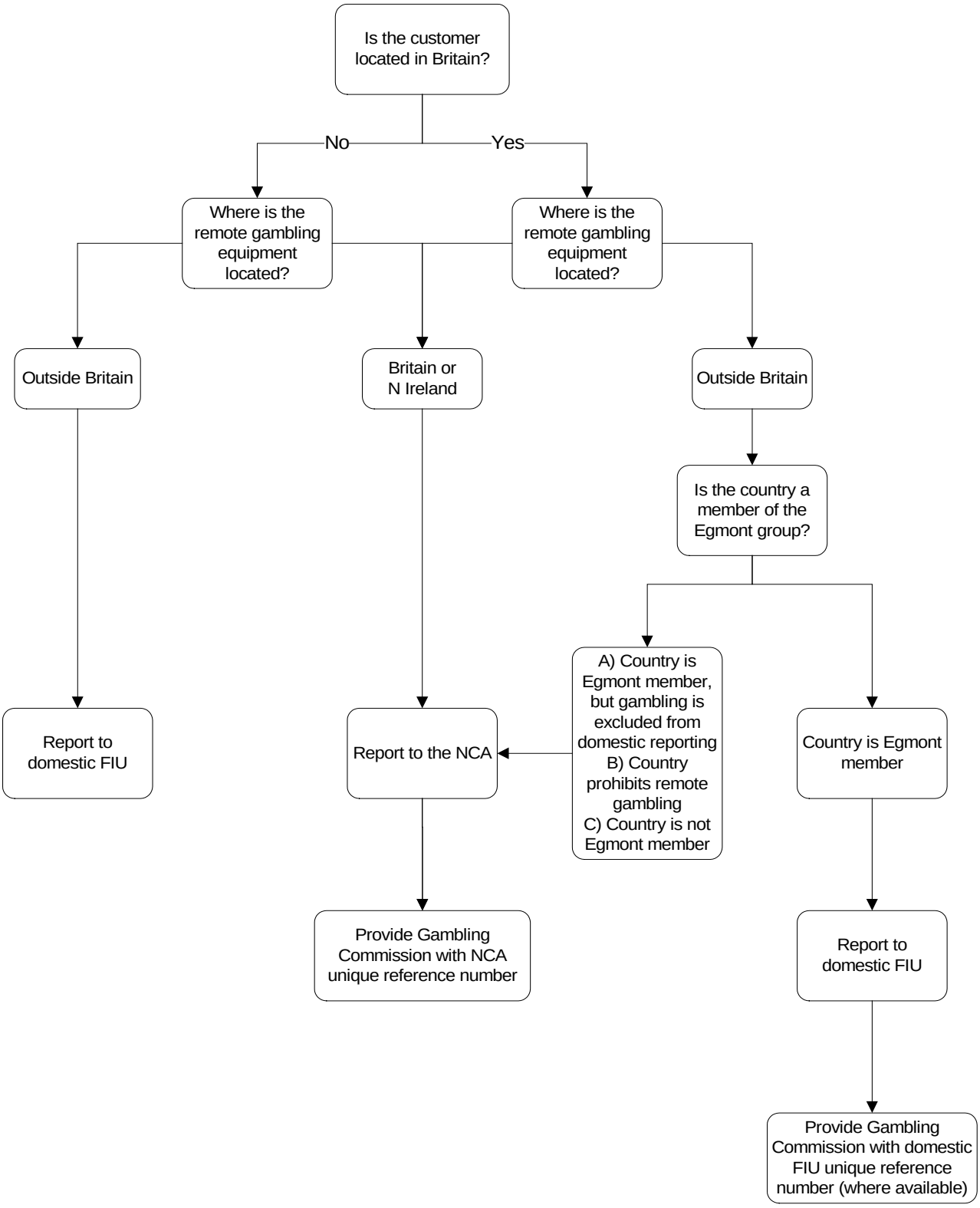


Figure 10: Suspicious activity reporting requirements for remote casinos



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. The term is defined in the Regulations.
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).
Casino operators	Firms holding a casino operating licence issued by the Commission.
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 operating 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 under POCA or the Terrorism Act.
Source of funds	Where the funds, money or cash to finance the transaction come from.
Supervisory authorities	Supervisory authorities, which are listed in regulation 7 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, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.
The Terrorism Act	The Terrorism Act 2000.
Third country	A country which is outside the European Union.
UKFIU	The United Kingdom Financial Intelligence Unit, which is the unit within the NCA that operates the disclosure regime for money laundering.

September 2017

Keeping gambling fair and safe for all

www.gamblingcommission.gov.uk

Finalised guidance

FG 17/6 The treatment of politically exposed persons for anti-money laundering purposes

July 2017

1 Executive Summary

Legislative Background

1.1 In March 2017, we consulted on guidance in connection with politically exposed persons ('PEPs') under section 333U of the Financial Services and Markets Act 2000 (section 333U'). Section 333U contained a duty on the FCA to issue guidance in connection with PEPs prior to the coming into force of regulations transposing the fourth money laundering directive or any subsequent EU measures.

1.2 However, as of 6 July 2017, section 333U has yet to be commenced. We now have a duty under regulation 48(1) of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ('the Regulations') to issue guidance about the enhanced customer due diligence measures in respect of PEPs. In addition, under the Regulations it says that "the duty to issue guidance under section 333U does not apply to the extent that that duty is otherwise satisfied as a result of guidance issued by us under the Regulations".

1.3 Accordingly, we issue this guidance under regulation 48(1) of the Regulations and in doing so consider that we will have satisfied the duty under section 333U when this provision is commenced. We have decided not to consult again on this guidance as the

substance of the guidance has already been consulted on and so no useful purpose would served to consult on it again.

1.4 We have made a number of amendments to the draft during the consultation period. The EU is currently negotiating targeted amendments to the 4th Money Laundering Directive and the final text may impact this guidance. Alongside the guidance, we are publishing a feedback statement.

Summary of the Guidance

1.5 The FCA expects that firms take appropriate but proportionate measures in meeting their financial crime obligations. The MLRs set out that all firms must apply a risk sensitive approach to identifying PEPs and then applying enhanced due diligence measures. The legislation and guidance clarifies that a case by case basis is required with the risk assessed of individual PEPs rather than applying a generic approach to all PEPs.

1.6 The guidance provides clarity on how firms should apply the definitions of a PEP in the MLRs in a UK context. This includes providing that firms should only treat those in the UK who hold truly prominent positions as PEPs and not to apply the definition to local government, more junior members of the senior civil service or anyone other than the most senior military officials. As such it is unlikely in practice that a large number of UK customers should be treated as PEPs.

1.7 Even where a UK customer does meet the definition of PEP because of the position they hold- or another country assessed as having similarly transparent anti-corruption regimes- a firm is required to recognise the lower risk of such customer s and apply the guidance on measures they can take in lower risk situations to meet their EDD obligations.

1.8 The guidance does, however, require firms to apply more stringent approaches where the customer is assessed as having a greater risk. In those circumstances firms will need to take further steps to verify information about the customer and the proposed business relationship. This is in line with the FCA's financial crime guidance to date where the focus has been on managing higher risk PEP relationships.

2 Final guidance

Introduction

2.1 This guidance is aimed at any institution that has its anti-money laundering systems and controls overseen by the FCA.[1] It discusses how they can meet their obligations when opening new relationships or monitoring existing relationships. It applies only to business relationships undertaken in the course of business in the UK.

2.2 The Financial Ombudsman Service will consider complaints from PEPs, their family members or close associates – and will take the guidance into account when deciding what is fair and reasonable in all the circumstances of a complaint.

2.3 This guidance has not been approved by Treasury under Regulation 35(4)(b) and sections 330 & 331 of the Proceeds of Crime Act. However, Regulation 35)(4)(b)(i) states that firms may take into account any guidance that has been issued by the FCA.

2.4 In this guidance, where we are interpreting rather than restating legal obligations, this is shown in italics.

2.5 Firms should only take additional measures beyond this guidance where:

- this is justified on the basis of their risk assessment
- risk factors are associated with that customer unrelated to their position or connection to a PEP

Why do PEPs, family members of PEPs or known close associates of PEPs pose a risk?

2.6 PEPs (as well as their families and persons known to be close associates) are required to be subject to enhanced scrutiny by firms subject to the Regulations. This is because international standards issued by the Financial Action Taskforce (FATF) recognise that a PEP may be in a position to abuse their public office for private gain and a PEP may use the financial system to launder the proceeds of this abuse of office. As FATF says 'these requirements are preventive (not criminal) in nature, and should not be interpreted as stigmatising PEPs as such being involved in criminal activity'.[2]

2.7 It is because of their function that a person becomes a PEP and is required to be subject to enhanced scrutiny by firms.

[1] Regulation 7(1)(a) of the Regulations sets out who we supervise.
[2] www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf

2.8 Likewise, a PEP's family or close associates may also benefit from, or be used to facilitate, abuse of public funds by the PEP. It is as a result of this connection that family and known close associates are required to be subject to greater scrutiny. Family and close associates are not themselves PEPs solely as a result of their connection to a PEP.

What are firms' obligations under the Regulations?

2.9 The Regulations require firms to have in place appropriate risk-management systems and procedures to determine whether a customer or the beneficial owner of a customer is a PEP (or a family member or a known close associate of a PEP) and to manage the risks arising from the firm's relationship with those customers. *This includes where a PEP, family member or close associate is operating via an intermediary or introducer (this may include others in the regulated sector such as banking staff, lawyers, estate agents etc). There are many legitimate reasons for doing so (eg a solicitor acting in a property transaction). In these situations, and in line with FATF guidance, we expect firms to understand as part of their due diligence why a PEP, family member or close associate is using such an arrangement and use that as part of their assessment of risk.*

2.10 The Regulations state[3] that in determining whether these systems and procedures are appropriate, a firm should refer to:

- Its own risk assessment of the money laundering/terrorist financing risks it is subject to. *The FCA's financial crime guide[4] contains guidance on our expectations of risk assessments in relation to overall financial crime (Box 2.3) and specifically money laundering (Box 3.3).*
- An assessment of the extent to which the risk would be increased by a business relationship with a PEP, family member or close associate. *The FCA would expect that this is a case-by-case assessment and not an automatic assessment that a relationship creates a high risk of money laundering*.
- Any information provided by the FCA. This will include the FCA's publication 'Financial Crime: a guide for firms', thematic reviews, speeches on financial crime issues or enforcement action and the FCA's annual AML report.

2.11 *The FCA expects firms to make use of information that is reasonably available to them in identifying PEPs, family members or known close associates. This could include the following:*

- *Public domain information such as websites of parliaments and governments, reliable news sources and work by reputable pressure groups focused on corruption risk such as Transparency International or Global Witness. Firms should use a variety of sources where possible.*
- *Reliable Public Registers – in the UK this includes Companies House's register of companies and persons of significant control (PSC)[5] and those maintained by the Electoral Commission.[6]*

[3] Regulation 35(2)
[4] www.handbook.fca.org.uk/handbook/FC/link/?view=chapter
[5] https://beta.companieshouse.gov.uk/
[6] http://search.electoralcommission.org.uk/

- *In line with the nature and size of the firm, it may choose, but is not required, to use commercial databases that contain lists of PEPs, family members and known close associates. A firm choosing to use such lists would need to understand how such databases are populated and will need to ensure that those flagged by the system fall within the definition of a PEP, family member or close associate as set out in the Regulations and this guidance.*

2.12 Where a firm has identified that a customer (or beneficial owner of a customer) does meet the definition of a PEP (or a family member or known close associate of a PEP), a firm must[7] assess the level of risk associated with that customer and, as a result of that assessment, the extent to which enhanced due diligence measures need to be carried out.[8] *The risk factors set out in this guidance will help firms to consider relevant factors when meeting these obligations. A firm's assessment[9] and its decision to apply relevant enhanced due diligence measures[10] need to be clearly documented.*

2.13 *The FCA expects that a firm will not decline or close a business relationship with a person merely because that person meets the definition of a PEP (or of a family member or known close associate of a PEP). A firm may, after collecting appropriate information[11] and completing its assessment,[12], conclude the risks posed by a customer are higher than they can effectively mitigate; only in such cases will it be appropriate to decline or close that relationship.*

2.14 *If, having assessed the risk associated with the customer and decided on an appropriate level of enhanced due diligence measures in line with this guidance, a firm is unable to apply those measures, a firm needs to comply with the requirement[13] not to establish, or to terminate, a business relationship.*

2.15 Where a firm proposes to have, or to continue, a business relationship with a PEP, family member or known close associate of a PEP, they are required[14] to:

- Have approval from senior management for establishing or continuing the business relationship with that person. *For these purposes, senior management is to be, as a minimum, the person holding the CF11/SMF17 Money Laundering Reporting Officer role. In any case identified as one where there is a high risk of money laundering or terrorist financing,[15], it may be appropriate to seek approval from the person with overall responsibility for the firm's policies and procedures for countering the risk that the firm might be used to further financial crime; for firms subject to the Senior Management Regime, this will be the person with that prescribed responsibility. But firms should note that in lower risk situations sign-off may be at a lower level as set out further on in this guidance.*

[7] See Regulation 35(3) of the MLRs
[8] As set out in Regulation 33(4) and (5)
[9] See Regulation 35(3)(a)
[10] See Regulation 35(3)(b)
[11] In accordance with Regulation 35(3)(b)
[12] Under Regulation 35(3)(a)
[13] See Regulation 31(1) (b) and (c)
[14] See Regulation 35(5)
[15] Per the assessment in Regulation 35(3)(a)

- Take adequate measures to establish the customer's source of wealth and source of funds relevant to the proposed business relationship or transaction. *Adequate measures will vary according to the risks assessed [16] depending on the nature of the relationship/transaction, with greater measures to clarify source of wealth and source of funds required for unusual or unexpected transactions, while for lower risk products or relationships, reliance might be placed on funds coming from credit or financial institution.[17] We set out our expectations further in this guidance.*
- Once the business relationship is entered into, conducting enhanced ongoing monitoring of the business relationship with that person. *The nature and extent of this monitoring will depend on the risk assessment.[18]*

Who should be treated as a PEP?

2.16 PEPs are defined[19] as individuals entrusted with prominent public functions, including:

- heads of state, heads of government, ministers and deputy or assistant ministers
- members of parliament or of similar legislative bodies – *similar legislative bodies include regional governments in federalised systems and devolved administrations, including the Scottish Executive and Welsh Assembly, where such bodies have some form of executive decision-making powers. It does not include local government in the UK but it may, where higher risks are assessed, be appropriate to do so in other countries.*
- members of the governing bodies of political parties – *the FCA considers that this only applies to political parties who have some representation in a national or supranational Parliament or similar legislative body as defined above. The extent of who should be considered a member of a governing body of a political party will vary according to the constitution of the parties, but will generally only apply to the national governing bodies where a member has significant executive power (eg over the selection of candidates or distribution of significant party funds).*
- members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional circumstances – *in the UK this means only judges of the Supreme Court; firms should not treat any other member of the judiciary as a PEP and only apply EDD measures where they have assessed additional risks.[20]*
- members of courts of auditors or of the boards of central banks
- ambassadors, charges d'affaires and high-ranking officers in the armed forces – *the FCA considers this is only necessary where those holding these offices on behalf of the UK government are at Permanent Secretary/Deputy Permanent Secretary level, or hold the equivalent military rank (eg Vice Admiral, Lieutenant General, Air Marshal or senior)*
- members of the administrative, management or supervisory bodies of State-owned enterprises – *the FCA considers that this only applies to for profit enterprises where the state has ownership of greater than 50% or where information reasonably available points to the state having control over the activities of such enterprises*
- directors, deputy directors and members of the board or equivalent function of an international organisation – *the FCA considers that international organisations*

[16] In accordance with Regulation 35(3)(a)
[17] Where this meets the requirements of Regulation 37(3)(a)(iii)
[18] Regulation 35(3)
[19] Regulation 35(12)(a)
[20] In accordance with Regulation 33

only includes international public organisations such as the UN and NATO. The Government made clear in their consultation of 15 March 2017 that they do not intend this definition to extend to international sporting federations.

2.17 *The definition of a 'prominent public function' will vary according to the nature of the function held by a person. The FCA would expect firms to understand the nature of the position held and whether the function gives rises to the risk of large-scale abuse of position. If a position is held in a country assessed as being at a lower risk of large-scale corruption (because of the system and checks and balances in place that reduce the threat) then only those with true executive power should be considered to hold a prominent public function. In the UK, it will not normally be necessary to treat public servants below Permanent or Deputy Permanent Secretary as having a prominent public function.*

2.18 *The regulations exclude from the definition of a PEP those who are 'junior or mid-ranking'.*[21] *In those cases it will normally only be necessary to meet the obligations to undertake customer due diligence.*[22] *However, a firm should be alive to the potential that middle ranking and more junior officials could act on behalf of a PEP when assessing the overall risks a customer might present; where it assesses there might be a risk, a firm should consider what additional measures it needs to take.*[23] *This includes any transaction or business relationship established in a high-risk third country.*[24]

2.19 If a person who is a PEP is no longer entrusted with a prominent public function, that person should continue to be subject to risk-based enhanced due diligence[25] for a period of at least 12 months after the date they ceased to be entrusted with that public function. Firms may apply measures for a longer period to address risks of money laundering or terrorist financing in relation to that person,[26] *but the FCA consider this will only be necessary in the cases of PEPs where a firm has assessed that PEP as posing a higher risk.*

2.20 *Firms should note that the Regulations*[27] *explicitly state that they cannot apply these measures to those who were not a PEP under the Money Laundering Regulations 2007 (ie those who held a prominent public position in the UK (such as a former MP, retired member of the House of Lords or a former UK ambassador) where they ceased that office prior to 26 June 2017).*

Who should be considered a family member?

[21] Regulation 35(12)(a)
[22] As required by Regulation 28
[23] Under Regulation 33(1)
[24] Regulation 33(1)(b)- 'high-risk third country' in this guidance has the same meaning as in that regulation
[25] In accordance with the MLRs and this guidance
[26] Regulation 35(9)(b)
[27] Regulation 35(10)

2.21 Family members of a PEP are defined as including:[28]

- spouse, or civil partner
- children and their spouses or civil partner
- parents

2.22 This is not an exhaustive list. *The FCA considers that this definition also includes brothers and sisters of a PEP.*

2.23 *Firms should take a proportionate and risk-based approach to the treatment of family members who do not fall into this definition. A corrupt PEP may use members of their wider family to launder the proceeds of corruption on his/her behalf. It may be appropriate to include a wider circle of family members (such as aunts and uncles) in cases where a firm has assessed a PEP to pose a higher risk. This would not apply in relation to lower risk PEPs. In low-risk situations, a firm should not apply any EDD measures to someone who is not within the definition above and should apply normal customer due diligence measures.[29] A family member of a PEP is not a PEP themselves purely as a consequence of being associated with a PEP.*

2.24 *A PEP must [30] be treated as a PEP after he or she leaves office for at least 12 months, depending on risk. This does not apply to family members, who should be treated as ordinary customers, subject to customer due diligence obligations[31] from the point that the PEP leaves office. The FCA considers a family member of a former PEP should not be subject to enhanced due diligence measures unless this is justified by the firm's assessment of other risks posed by that customer. The ESA guidelines set out factors that might point to potential higher risk.[32]*

People who are 'known to be close associates' of a PEP

2.25 A 'known close associate' of a PEP is defined[33] as including:

- an individual known to have joint beneficial ownership of a legal entity or a legal arrangement or any other close business relationship with a politically exposed person
- an individual who has sole beneficial ownership of a legal entity or a legal arrangement that is known to have been set up for the benefit of a PEP

2.26 *A known close associate of a PEP is not a PEP themselves purely as a consequence of being associated with a PEP.*

Do all PEPs pose the same risk?

[28] Regulation 35(12)(b)
[29] Regulation 28
[30] Regulation 35(9)
[31] Regulation 28
[32] https://www.eba.europa.eu/-/esas-publish-aml-cft-guidelines
[33] Regulation 35(12)(c)

2.27 *No – the risk of such corruption will differ between PEPs. We expect firms to take a differentiated approach that considers the risks an individual PEP poses based on an assessment of:*

- *the prominent public functions the PEP holds*
- *the nature of the proposed business relationship*
- *the potential for the product to be misused for the purposes of corruption*
- *any other relevant factors the firm has considered in its risk assessment.*[34]

2.28 *This guidance discusses how firms may differentiate between PEPs. In this guidance, we use the terms 'lower risk' and 'higher risk' to recognise that firms are required to apply Enhanced Due Diligence on a risk-sensitive basis.*[35] *An overall risk assessment will consider all risk factors that a customer may present and come to a holistic view of what measures should be taken to comply. No one risk factor set out below means a customer should automatically be treated as posing a higher risk; it is necessary to consider all features of the customer.*

What are some indicators that a PEP might pose a lower risk?

2.29 *In the FCA's view, the following indicators suggest a PEP poses a lower risk:*

Lower risk indicators – product

The customer is seeking access to a product the firm has assessed to pose a lower risk. This will include products assessed as low risk by the firm to which it applies simplified due diligence measures.[36]

Lower risk indicators – geographical

A PEP who is entrusted with a prominent public function in the UK should be treated as low risk, unless a firm has assessed that other risk factors not linked to their position as a PEP mean they pose a higher risk. Regulation 18 and the risk factors guidance produced by the European Supervisory Authorities set out factors that might point to potential higher risk.

A PEP may also pose a lower risk if they are entrusted with a prominent public function by a country where information available to the firm shows that it has the following characteristics:

- *associated with low levels of corruption*
- *political stability, and free and fair elections*
- *strong state institutions*
- *credible anti-money laundering defences*
- *a free press with a track record for probing official misconduct*
- *an independent judiciary and a criminal justice system free from political interference*
- *a track record for investigating political corruption and taking action against wrongdoers*

[34] Required by regulation 18
[35] Regulation 35
[36] Regulation 37

- *strong traditions of audit within the public sector*
- *legal protections for whistleblowers*
- *well-developed registries for ownership of land, companies and equities*

Lower risk indicators – personal and professional

A PEP may pose a lower risk if they:

- *are subject to rigorous disclosures requirements (such as registers of interests, independent oversight of expenses)*
- *does not have executive decision-making responsibilities (eg an opposition MP or an MP of the party in government but with no ministerial office)*

What are indicators that a PEP might pose a higher risk?

2.30 *In the FCA's view, the following indicators suggest a PEP poses a higher risk:*

Higher risk indicator – product

The firm's risk assessment finds the product or relationship a PEP is seeking is capable of being misused to launder the proceeds of large-scale corruption.

Higher risk indicators – geographical

A PEP may pose a greater risk if they are entrusted with a prominent public function in a country that is considered to have a higher risk of corruption. In coming to this conclusion, a firm should have regard to whether, based on information available, the country has the following characteristics:

- *associated with high levels of corruption*
- *political instability*
- *weak state institutions*
- *weak anti-money laundering defences*
- *armed conflict*
- *non-democratic forms of government*
- *widespread organised criminality*
- *a political economy dominated by a small number of people/entities with close links to the state*
- *lacking a free press and where legal or other measures constrain journalistic investigation*
- *a criminal justice system vulnerable to political interference*
- *lacking expertise and skills related to book-keeping, accountancy and audit, particularly in the public sector*
- *law and culture antagonistic to the interests of whistleblowers*
- *weaknesses in the transparency of registries of ownership for companies, land and equities*
- *human rights abuses*

Higher risk indicators – personal and professional

The following characteristics might suggest a PEP is higher risk:

- *personal wealth or lifestyle inconsistent with known legitimate sources of income or wealth; if a country has laws that do not generally permit the holding of a foreign bank account, a bank should satisfy itself that the customer has authority to do so before opening an account*
- *credible allegations of financial misconduct (eg facilitated, made, or accepted bribes)*
- *responsibility for, or able to influence, large public procurement exercises, particularly where procurement is not subject to competitive tender, or otherwise lacks transparency*
- *is responsible for, or able to influence, allocation of scarce government licenses such as mineral extraction concessions or permission for significant construction projects.*

What are some indicators that a PEP's family or known close associates pose a lower risk?

2.31 *A family member or close associate of a politically exposed person may pose a lower risk if the PEP themselves poses a lower risk. To clarify, the FCA expects family or known close associates of UK PEPs to be treated as lower risk unless there are circumstances to suggest otherwise.*

What are some indicators that a PEP's family or known close associates pose a higher risk?

2.32 *The following characteristics might suggest a family member or close associates of a politically exposed person poses a higher risk:*

- *wealth derived from the granting of government licences (such as mineral extraction concessions, licence to act as a monopoly provider of services, or permission for significant construction projects)*
- *wealth derived from preferential access to the privatisation of former state assets*
- *wealth derived from commerce in industry sectors associated with high-barriers to entry or a lack of competition, particularly where these barriers stem from law, regulation or other government policy*
- *wealth or lifestyle inconsistent with known legitimate sources of income or wealth*
- *credible allegations of financial misconduct (eg facilitated, made, or accepted bribes)*
- *appointment to a public office that appears inconsistent with personal merit*

What measures should firms take when they identify a customer is a PEP, or a family member or known close associate of a PEP?

2.33 The following measures are taken where a customer meets the definition of a PEP, or a family member or known close associate of a PEP:[37]

- obtain senior management approval for establishing or continuing business relationships with such persons
- take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons
- conduct enhanced, ongoing monitoring of those business relationships

[37] See Regulation 35

2.34 *The nature and extent of this due diligence should be appropriate to the risk that the firm has assessed in relation to the customer. A firm should apply more extensive measures for relationships assessed as high risk and less extensive measures for lower risk customers.*

What measures may firms take in lower risk situations?

2.35 *In the FCA's view, in lower risk situations a firm may take the following measures:*

- *Seek to make no enquiries of a PEP's family or known close associates except those necessary to establish whether such a relationship does exist.*
- *Take less intrusive and less exhaustive steps to establish the source of wealth and source of funds of PEPs, family members or known close associates of a PEP; for example, only use information already available to the institution (such as transaction records or publicly available information) and do not make further inquiries of the individual unless anomalies arise. It is necessary to seek source of wealth information but in all lower risk cases, especially when dealing with products that carry a lower risk of laundering the proceeds of corruption, firms should minimise the amount of information they collect and how they verify the information provided (for example, via information sources it has available).*
- *Oversight and approval of the relationship takes place at a level less senior than board of director level. For lower risk situations, this can be the MLRO.*
- *A business relationship with a PEP or a PEP's family and close associates is subject to less frequent formal review than if was considered high risk(for example, only where it is necessary to update customer due diligence information or where the customer requests a new service or product).*

What measures may firms take in higher risk situations?

2.36 *In the FCA's view, in higher risk situations a firm may take the following measures:*

- *take more intrusive and exhaustive steps to establish the source of wealth and source of funds of PEPs, family members or known close associates of a PEP*
- *oversight and approval of the relationship takes place at a more senior level of management*
- *a business relationship with a PEP (or a PEP's family and close associates) is subject to more frequent and thorough formal review as to whether the business relationship should be maintained*

Long-term insurance contracts

2.37 Firms that provide a customer with a contract of long-term insurance are required to have reasonable measures to determine whether the beneficiaries of the insurance policy or the beneficial owner of a beneficiary of such an insurance policy are a PEP or family members/known close associates of a PEP. This needs to be done before any payment is made under the insurance policy whether the benefit of the insurance policy is assigned in whole or in part from a PEP or a family member or known close associate of a PEP to another person (and vice versa).[38]

2.38 *As with other measures, the nature and extent of the reasonable measures a firm should take will be driven by the overall money laundering or terrorist financing risks a firms*

[38] See Regulation 35(6) and (7)

who offers this type of product has assessed in its risk assessment[39]*and the extent to which a PEP or known close associate/family using such a product raises the risk. Information on the nature of ML/TF risk is available via the UK's National Risk Assessment, ESA guidelines and other information sources. It will also depend on the nature of the life insurance product (for example, the cost of the premiums for the product, or if it can be redeemed or cashed out).*

Beneficial owners of legal entities who are PEPs

2.39 *Firms should identify when a PEP is a beneficial owner*[40] *of a customer. It does not require that a legal entity should be treated as a PEP just because a PEP might be a beneficial owner.*

2.40 *Once a firm is satisfied that a PEP is a beneficial owner then, in line with the risk-based approach, they should assess the risks posed by the involvement of that PEP and, after making this assessment, firms should apply appropriate measures in accordance with this guidance. These could range from applying customer due diligence measures in cases where the PEP is just a figurehead for an organisation (this will vary according to the circumstances of each entity but could be the case even if they sit on the board, including as a non-executive director) through to applying EDD measures, according to the risk assessed in line with this guidance where it is apparent the PEP has significant control or the ability to use their own funds in relation to the entity.*

2.41 *Where a PEP is a beneficial owner of a corporate customer, then a firm should not automatically treat other beneficial owners/shareholders of the customer as a PEP or known close associate under the Regulations, but may do so having assessed the relationship based on information available to the firm.*

[39] Required by Regulation 18
[40] 'beneficial owner' has the meaning set out in Regulation 5(1)