

GAMBLING COMMISSION

Money laundering: the prevention of money laundering and combating the financing of terrorism

Guidance for remote and non-remote casinos

Second edition

December 2011

Contents

Part 1: Summary of the guidance	4
Principles to be followed	4
Risk-based approach	4
Senior management responsibility	4
Nominated officer	5
Casino employees	5
Customer due diligence	5
Record keeping	6
Suspicious activity reports	6
Offences	7
Part 2: The guidance	8
1 Introduction	8
How should the guidance be used?	9
Content of the guidance	9
Status of the guidance	10
2 Risk-based approach	11
Introduction	11
Identifying and assessing the risks faced by the operator	11
Risk management is dynamic	12
Remote casinos – enhanced due diligence	12
3 Senior management responsibility	14
Introduction	14
Obligations of all operators	14
Policies and procedures	14
Training	15
4 Nominated officer	16
Standing of the nominated officer	17
Internal and external reports	17
5 Customer due diligence	18
Introduction	18
Threshold approach	18
Identification and verification on entry	24
Identification and verification	24
Electronic verification	25
Criteria for use of an electronic data provider	26
Documentary evidence	27
Politically exposed persons	28
Failure to complete checks	29
Requirements for remote casinos	30
Existing customers	30

	List of persons subject to financial restrictions	30
6	Record keeping	32
	General legal and regulatory requirements	32
	Business relationships	32
	Occasional transaction	33
	Other casino customers	33
	Customer information	33
	Supporting records – non-remote casinos	35
	Supporting records – remote casinos	35
	Supporting records – gaming machines	35
	Retention period	36
	Form in which records have to be kept	36
7	Suspicious activities and reporting	37
	Introduction	37
	What is meant by knowledge and suspicion?	37
	What is meant by reasonable grounds to know or suspect?	39
	Internal reporting	39
	Evaluation and determination by the nominated officer	41
	External reporting	41
	Submission of suspicious activity reports	41
	Appropriate consent	42
	Applying for appropriate consent	45
	Failing to report	45
	After a report has been made	45
	Tipping off, or prejudicing an investigation	46

Figures

	Figure 1 – Risk-based approach	13
	Figure 2 – Customer due diligence	19
	Figure 3 – Determining when the threshold is reached (non-remote casinos) – chips and gaming machines	21
	Figure 4 – Determining when the threshold is reached (non-remote casinos) – casino account	22
	Figure 5 – Determining when the threshold is reached (remote casinos)	23
	Figure 6 – Record keeping	34
	Figure 7 – Reasonable grounds to suspect (objective test)	38
	Figure 8 – Knowledge or suspicion of money laundering or terrorist financing (subjective test)	40
	Figure 9 – Appropriate consent	43

Annex A – Glossary of terms **49**

Part 1 – Summary of the guidance

Principles to be followed

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

Risk-based approach

- ii The Regulations require operators to have a policy and procedure in relation to risk assessment and management. The risk-based approach involves a number of discrete steps in assessing the most proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the operator. These steps require the operator to:
 - identify the money laundering and terrorist financing risks that are relevant to the operator;
 - design and implement policies and procedures to manage and mitigate these assessed risks;
 - monitor and improve the effective operation of these controls; and
 - record what has been done, and why.
- iii A risk-based approach focuses the effort where it is most needed and will have most impact. It requires the full commitment and support of senior management, and the active co-operation of all employees.
- iv The risk-based approach is discussed in section 2 of this guidance.

Senior management responsibility

- v Senior management must be fully engaged in the processes around an operator's assessment of risks for money laundering and terrorist financing, and must be involved at every level of the decision making to develop the operator's policies and processes to comply with the Money Laundering Regulations 2007 (the Regulations). Disregard for the legal requirements, for example, turning a blind eye to customers spending criminal proceeds, may result in criminal or regulatory action.
- vi A member of senior management who consents to, or connives in, the commission of offences under the Regulations, or where the commission of any such offence is attributable to any neglect on his part, will be individually liable for the offence.

- vii Operators must establish and maintain appropriate written risk-sensitive policies and procedures relating to:
- customer due diligence (CDD) measures and ongoing monitoring;
 - reporting;
 - record keeping;
 - internal control;
 - risk assessment and management;
 - training; and
 - the monitoring and management of compliance with, and the internal communication of, such policies and procedures.
- viii Senior management responsibility is discussed in section 3 of this guidance.

Nominated officer

- ix Nominated officers have responsibility for:
- making reports to senior management on anti-money laundering (AML) and countering terrorist financing (CTF) activity;
 - receiving internal disclosures under Part 7 of the Proceeds of Crime Act 2002 (POCA) and Part 3 of the Terrorism Act 2000 (the Terrorism Act);
 - deciding whether these should be reported to the Serious Organised Crime Agency (SOCA); and
 - if appropriate, making such external reports.
- x They must have the authority to act independently in carrying out their responsibilities, and have access to sufficient resources to carry out their duties.
- xi Casinos must have contingency arrangements in place for circumstances where no nominated officer is in post, for example, if on annual leave, long-term sick leave or if the nominated officer leaves the employ of the casino.
- xii The responsibilities of the nominated officer are discussed in section 4 of this guidance.

Casino employees

- xiii Employees must report to their nominated officer any knowledge or suspicion of money laundering whether by customers, guests or other employees.
- xiv Employees must follow casino policies and procedures for:
- CDD, including enhanced requirements for high risk customers, which includes politically exposed persons (PEPs);
 - reporting suspicious activity to the nominated officer
 - where necessary, seeking appropriate consent to allow participation in gaming and to conduct gaming and other business transactions; and
 - record keeping for those who exceed the threshold or who have a business relationship.
- xv The duties of casino employees are discussed throughout sections 4, 5, 6 and 7 of this guidance.

Customer due diligence

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

- xvii Operators must conduct their CDD on the basis of risk assessment, including simplified due diligence and enhanced due diligence (which includes PEPs). Operators are also required to identify the beneficial owner of a customer and they will also need to have evidence of identity in place for all customers.
- xviii Operators should note that CDD is ongoing and may need updating for changes in the customer's circumstances and personal details.
- xix Customer due diligence is discussed in section 5 of this guidance.

Record keeping

- xx The purpose of the record keeping requirement is to ensure that there is an audit trail that could assist in any financial investigation by a law enforcement body.
- xxi The operator's record keeping policy and procedure should cover records in the following areas:
 - details of how compliance has been monitored by the nominated officer;
 - delegation of AML/CTF tasks by the nominated officer;
 - nominated officer reports to senior management;
 - information not acted upon by the nominated officer, with reasoning why no further action was taken;
 - customer identification and verification information;
 - supporting records in respect of business relationships or occasional transactions;
 - employee training records;
 - internal and external suspicious activity reports (SARs); and
 - contact between the nominated officer and law enforcement or SOCA, including records connected to appropriate consent.
- xxii Record keeping is discussed in section 6 of this guidance.

Suspicious activity reports

- xxiii Employees in casinos are required to make a report in respect of information that comes to them within the course of business:
 - where they know; or
 - where they suspect; or
 - where they have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing.
- xxiv Operators must ensure that any employee reports to the nominated officer where they have grounds for knowledge or suspicion that a person or customer is engaged in money laundering or terrorist financing. The operator's nominated officer must consider each report, and determine whether it gives grounds for knowledge or suspicion.
- xxv If the nominated officer determines that a report does give rise to grounds for knowledge or suspicion, he must report the matter to SOCA. Under POCA, the nominated officer is required to make a report to SOCA as soon as is practicable if he has grounds for suspicion that another person, whether or not a customer, is engaged in money laundering. Under the Terrorism Act, similar conditions apply in relation to disclosure where there are grounds for suspicion of terrorist financing.
- xxvi Suspicious activities and reporting requirements are discussed in section 7 of this guidance.

Offences

- xxvii POCA and the Terrorism Act create offences of failing to report suspicious activity. Where a person fails to comply with the obligations to make disclosures to a nominated officer, or the nominated officer to SOCA, as soon as practicable after the information giving rise to the knowledge or suspicion comes to the employee, they are open to criminal prosecution.
- xxviii In certain circumstances, a person also commits an offence under POCA if he discloses information that a SAR has been submitted that is likely to prejudice any investigation, or discloses information that an investigation into allegations that an offence under the Regulations has been committed, that is likely to prejudice the investigation.
- xxix A person in the regulated sector also commits an offence if he knows or suspects that an appropriate officer or, in Scotland, a proper person is acting (or proposing to act) in connection with a confiscation investigation, a civil recovery investigation, a detained cash investigation or a money laundering investigation which is being or is about to be conducted, and falsifies, conceals, destroys or disposes of, or causes or permits the falsification, concealment, destruction or disposal of, documents which are relevant to the investigation.
- xxx The offences are discussed in section 7 of this guidance.

Part 2 – The guidance

1 Introduction

- 1.1** The law concerning money laundering is based on the general and wide ranging prevention and detection of the use of any proceeds of crime, the prevention and detection of terrorist financing, and for some businesses (including casinos) the more specific requirements of the business and its employees to have policies and procedures in place covering the risks it faces from money laundering.
- 1.2** Money laundering is a term that is often misunderstood. It is defined in section 340 of POCA and covers wide ranging circumstances involving any activity concerning the proceeds of any crime. This includes:
- 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;
 - possessing or transferring stolen goods;
 - being directly involved with any criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property; and
 - criminals investing the proceeds of their crimes in the whole range of financial products.
- 1.3** Using money in casinos, regardless of the amount, that is the proceeds of any crime can amount to money laundering if the person using or taking the money knows or suspects that it is the proceeds of crime. Money laundering offences can be committed by both the customer and casino employees, depending on respective levels of knowledge or suspicion.
- 1.4** The Regulations came into effect on 15 December 2007 and replaced the Money Laundering Regulations 2003 (the 2003 Regulations). Both remote and non-remote casinos licensed by the Commission are covered by the Regulations.
- 1.5** The Regulations are generated from the Third European Union Directive (2005) that was adopted in October 2005. This directive represents Europe’s ongoing commitment to tackle the international problem of money laundering and terrorist financing by implementing the global standards produced by the Financial Action Task Force (FATF) in 2003.
- 1.6** The FATF recommendations that set the global standards single out the business sectors where there are believed to be the highest risks of money laundering and terrorist financing. This includes remote and non-remote casinos.
- 1.7** Criminal offences of money laundering were first introduced in the United Kingdom (UK) in the Criminal Justice Act 1988 and the Drug Trafficking Offences Act 1986. POCA consolidated, updated, and reformed, the criminal law relating to money laundering to include any dealing in ‘criminal property’, which is defined widely as the proceeds of any type of crime, however small the amount. POCA created three principal offences that between them criminalise any involvement in the proceeds of any crime if the person knows or suspects that the property is the proceeds of crime.¹
- 1.8** These are wide offences that can be committed by any person, including a casino employee, who has actual knowledge or suspicion that a customer is using the proceeds of crime, or has possession of the proceeds of criminal activity.

¹ Sections 327, 328 and 329 of POCA.

- 1.9** Specific obligations to report suspected terrorist financing were included in the Terrorism Act, as amended by the Anti Terrorism Crime and Security Act 2001. This legislation creates criminal offences, most of which can be committed by anyone in the UK. Some of the offences are specific to people working in firms covered by the Regulations, and who are therefore in the regulated sector, which includes casinos.
- 1.10** The Regulations cover a range of businesses and professions, including remote and non-remote casinos licensed by the Commission. This guidance sets out how casino operators can and must comply with the law, which at times is complex and demanding. The law places responsibilities on the Commission as the supervisory authority for casinos. The Commission should produce guidance that helps casino operators to meet the requirements of the law, is workable in the remote and non-remote casino environments and is approved by HM Treasury. This guidance covers the full requirements of the UK law as it affects casinos.
- 1.11** The purpose of this guidance is to:
- outline the legal framework for AML and CTF requirements and systems across the remote and non-remote casino sector;
 - summarise the requirements of the relevant law and regulations, and how they may be implemented in practice;
 - indicate good industry practice in AML/CTF procedures through a proportionate risk-based approach;
 - assist operators to design and implement the policies and procedures necessary to mitigate the risks of being used in connection with money laundering and the financing of terrorism.
- 1.12** This guidance sets out what will be expected of casino operators and their employees in relation to the prevention of money laundering and terrorist financing, but allows them some discretion as to how they apply the requirements of the AML/CTF regime in the particular circumstances of their business.
- 1.13** This guidance will be of direct relevance to senior management and nominated officers in remote and non-remote casinos.

How should the guidance be used?

- 1.14** The purpose is to give guidance to those who set operators' risk management policies and procedures for preventing money laundering and terrorist financing. This guidance aims to assist operators with detail about how to comply with the Regulations and the wider legal requirements, and is intended to allow operators flexibility as to how they comply. Operators will need to establish their own, more detailed and more specific internal arrangements directed by senior management and nominated officers to reflect the risk profile of their business.
- 1.15** When provisions of the statutory requirements or the Commission's regulatory requirements are directly described in the text of the guidance and are obligatory, the guidance uses the term 'must', indicating that these provisions are mandatory. Where the guidance is merely advisory, the term 'should' is adopted. References to 'must' and 'should' in the text should therefore be construed accordingly.
- 1.16** This guidance is not intended to be a substitute for legal advice or operators' individual risk management plans. Operators should refer to the Regulations and associated legislation in making decisions in relation to the Regulations.

Content of the guidance

- 1.17** This guidance emphasises the responsibility of senior management to manage the operator's money laundering and terrorist financing risks, and how this should be carried

out on a risk-based approach. It sets out a standard approach to the identification of customers and verification of their identities, separating out basic identity from other measures relating to customer due diligence, including the obligation to monitor customer activity.

- 1.18** It is accepted that a proportionate risk-based approach has to meet a variety of scenarios and, as such, has to be based on an understanding of how the business is designed to operate. There is, therefore, a need for ongoing and repeated assessments of risk to meet changing circumstances.
- 1.19** The guidance contains the following sections:
- the importance of adopting a risk-based approach
 - the importance of senior management taking responsibility for effectively managing the money laundering and terrorist financing risks faced by the operator's businesses;
 - the role and responsibilities of the nominated officer;
 - the proper carrying out of the CDD obligations, including monitoring customer transactions and activity;
 - record keeping; and
 - the identification and reporting of suspicious activity.

Status of the guidance

- 1.20** POCA requires a court to take account of industry guidance, such as this, that has been approved by a Treasury minister when considering whether a person within the regulated sector has committed the offence of failing to report. Similarly the Terrorism Act requires a court to take account of such approved industry guidance when considering whether a person has failed to report under that Act. The Regulations state that a court must consider whether someone has followed this guidance if they are prosecuted for failing to comply with the Regulations.² The first edition of this guidance was approved by HM Treasury on 27 July 2010.
- 1.21** Operators must be able to demonstrate that they have taken all reasonable steps to comply with all the AML requirements. If they can demonstrate to a court and/or the Commission that they have followed this guidance then the court or the Commission is obliged to take that into account.
- 1.22** The Commission is not a 'designated authority' under the Regulations and therefore has no powers to take action against operators that breach the Regulations.³ However, an ordinary code provision within the Licence Conditions and Codes of Practice requires casino operators to act in accordance with this guidance. Should operators not follow the code provision, the Commission may consider reviewing the suitability of the operator to carry on the licensed activities. This could result in the suspension or revocation of the operator's licence under sections 118 and 119 of the Gambling Act 2005 (the Act).
- 1.23** The Commission also has employees who have the powers of accredited financial investigators under POCA in England and Wales.⁴ This means that the Commission can apply for orders and warrants in relation to money laundering, for the purpose of:
- requiring a specified person to produce certain material
 - permitting the search of and seizure of material from specified premises
 - requiring a financial institution to provide customer information relating to a specified person.
- 1.24** The guidance provides a sound basis for operators to meet their legislative and regulatory obligations when tailored by operators to their particular business risk profile. Departures

² Sections 330 and 331 of POCA and Regulation 45.

³ Regulation 42.

⁴ See Statutory Instrument No 2009/975.

from this guidance, and the grounds for doing so, should be documented and may have to be justified, for example, to the Commission.

2 Risk-based approach

Introduction

- 2.1** The Regulations impose compulsory compliance requirements and a breach can constitute a criminal offence.⁵ However, within this legal framework of requirements, casinos have flexibility to devise policies and procedures which best suit their assessment of the money laundering and terrorist financing risks faced by their business. The Regulations require a policy and procedure in relation to risk assessment and management.⁶
- 2.2** Operators are already expected to manage their operations with regard to the risks posed to the licensing objectives in the Act, and measure the effectiveness of the policies and procedures they have put in place to manage those risks. The approach to managing the risks of the operator being used for money laundering or terrorist financing is consistent with the existing regulatory requirements.
- 2.3** The risk-based approach involves a number of discrete steps in assessing the most proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the operator. These steps require the operator to:
- identify the money laundering and terrorist financing risks that are relevant to the operator;
 - design and implement policies and procedures to manage and mitigate these assessed risks;
 - monitor and improve the effective operation of these controls; and
 - record what has been done, and why.
- 2.4** A risk-based approach will serve to balance the burden placed on operators and their customers with a realistic assessment of the threat of the operator being misused in connection with money laundering or terrorist financing. It focuses the effort where it is most needed and will have most impact. It is not a blanket one size fits all approach, and therefore operators have a degree of flexibility in their methods of compliance.
- 2.5** A risk-based approach requires the full commitment and support of senior management, and the active co-operation of all employees. Senior management should ensure that the risk-based approach is part of the operator's philosophy and reflected in its policies and procedures. There needs to be a clear communication of the policies and procedures across the operator, along with robust mechanisms to ensure that they are carried out effectively, weaknesses are identified, and improvements are made wherever necessary.

Identifying and assessing the risks faced by the operator

- 2.6** The operator should assess its risks in the context of how it is most likely be involved in money laundering 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?
 - 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 and mitigate any money laundering potential?

⁵ Regulation 45.

⁶ Regulation 20(1)(e).

- Is the business local with regular and generally well known customers?
- Are there a large proportion of overseas customers using foreign currency or overseas based bank cheque or debit cards?
- Are customers likely to be individuals who hold public positions in countries which carry a higher exposure to the possibility of corruption, that is, a PEP?
- 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?

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

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

2.9 Where a customer is assessed as presenting higher risk it will be necessary to seek additional information in respect of the customer. This will help the operator judge whether the higher risk that the customer is perceived to present is likely to materialise. Such additional information may include an understanding of where the customer's funds and wealth have come from.

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

2.11 In order to be able to detect customer activity that may be suspicious, it is necessary to monitor transactions or activity.⁷ Monitoring customer activity should be carried out using the risk-based approach, with higher risk customers being subjected to an appropriate frequency and depth of scrutiny, which is likely to be greater than may be appropriate for lower risk customers.

Risk management is dynamic

2.12 A money laundering/terrorist financing risk assessment is not a one-off exercise. Operators must therefore ensure that their policies and procedures for managing money laundering and terrorist financing risks are kept under regular review.

Remote casinos – enhanced due diligence

2.13 The Regulations view situations where a customer is not physically present for identification purposes as higher risk for money laundering and require an operator to take specific and adequate measures to compensate for the higher risk (referred to as

⁷ Regulation 8.

enhanced customer due diligence and ongoing monitoring in the Regulations), for example, by applying one or more of the following measures:⁸

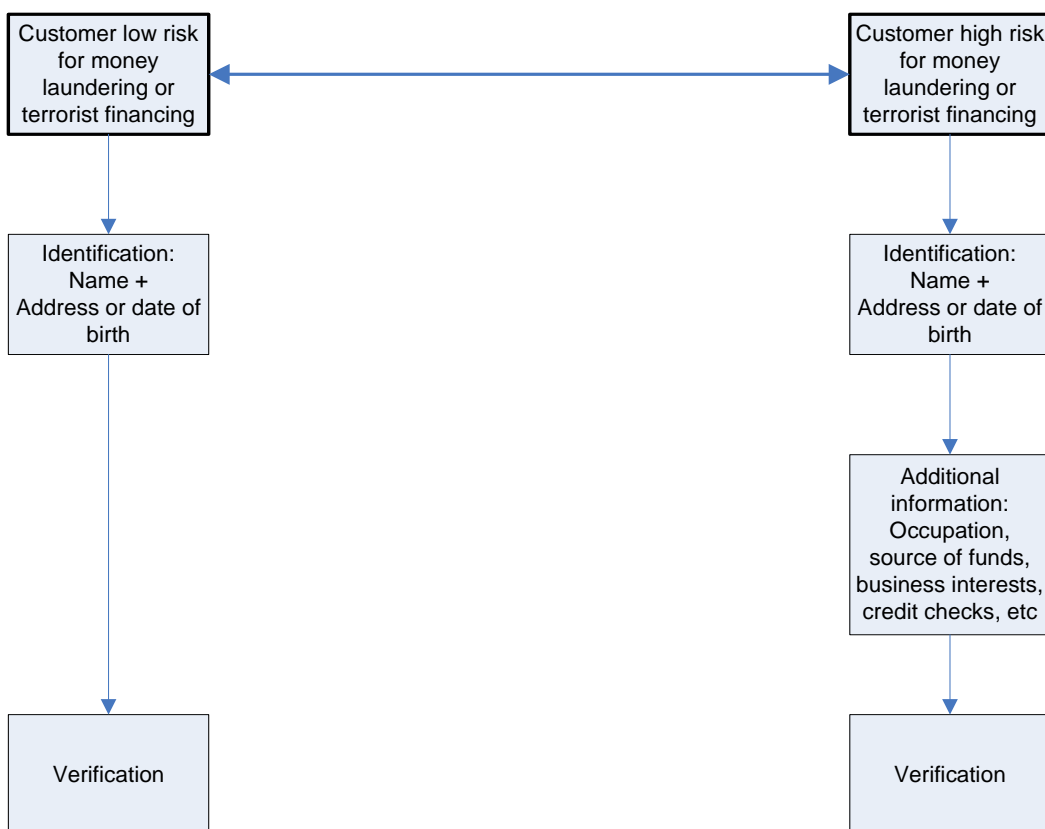
- (a) ensuring that the customer's identity is established by additional documents, data or information;
- (b) supplementary measures to verify or certify the documents supplied, or confirmatory certification by a credit or financial institution which is subject to the money laundering directive; or
- (c) ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution.

2.14 Option (c) above will fit with remote casinos business methods where it is necessary for a customer to have a bank or credit card account, which must be in his name.

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

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

Figure 1: Risk-based approach



Note:

Casino operators should undertake risk assessments of each premises and each remote site and:

- (a) look at the average drop/win per customer, and
- (b) risk assess each customer.

See paragraphs 2.1 to 2.16 of this guidance for more detail on assessing risk.

⁸ Regulation 14.

3 Senior management responsibility

Introduction

- 3.1** Senior management must be fully engaged in the processes around an operator's assessment of risks for money laundering and terrorist financing, and must be involved at every level of the decision making to develop the operator's policies and processes to comply with the Regulations. Disregard for the legal requirements, for example, turning a blind eye to customers spending criminal proceeds, may result in criminal or regulatory action.
- 3.2** It is considered best practice, and is explicit in parts of the Regulations, that a risk-based approach should be taken to tackling money laundering and terrorist financing.
- 3.3** Operators, using a risk-based approach, should start from the premise that most customers are not money launderers or terrorist financiers. However, operators should have policies and procedures in place to highlight those customers who, according to criteria established by the operator, may present a higher risk. The policies and procedures should be proportionate to the risks involved.

Obligations on all operators

- 3.4** An officer of a licensed operator which is subject to the Regulations (that is, a director, manager, secretary, chief executive, member of the management committee, or a person purporting to act in such a capacity) who consents to, or connives in, the commission of offences under the Regulations, or where the commission of any such offence is attributable to any neglect on his part, will be individually liable for the offence.⁹
- 3.5** The nominated officer should compile an annual report covering the operation and effectiveness of the operator's policies and procedures to combat money laundering. In practice, senior management should determine the depth and frequency of information they feel is necessary to discharge their responsibilities. The nominated officer may also wish to report to senior management more frequently than annually, as circumstances dictate. The nominated officer may not need to provide the names of suspected persons in any report.

Policies and procedures

- 3.6** Operators must establish and maintain appropriate written risk-based policies and procedures relating to:
- CDD measures and ongoing monitoring;
 - reporting;
 - record keeping;
 - internal control;
 - risk assessment and management;
 - training; and
 - the monitoring and management of compliance with, and the internal communication of, such policies and procedures.¹⁰
- 3.7** The operator's policies and procedures should cover:
- the arrangements for nominated officer reports to senior management;
 - the systems for customer identification and verification, including enhanced arrangements for high risk customers, which includes PEPs;
 - the circumstances in which additional information in respect of customers will be sought in the light of their activity;

⁹ Regulation 47.

¹⁰ Regulation 20.

- the procedures for handling SARs, covering both reporting by employees and transmission to SOCA;
- the mechanisms for contact between the nominated officer and law enforcement or SOCA, including the circumstances in which appropriate consent should be sought;
- the arrangements for recording information not acted upon by the nominated officer, with reasoning why no further action was taken;
- the monitoring and management of compliance with internal policies and procedures;
- the communication of such policies and procedures, including details of how compliance is monitored by the nominated officer, and the arrangements for communicating the policies and procedures to all relevant employees;
- employee training records; and
- supporting records in respect of business relationships, and the retention period for the records.

Training

- 3.8** The Regulations require that all relevant employees of casinos must be trained on the prescribed AML and CTF topics. Operators must ensure that their employees understand the Regulations and apply the operator's policies and procedures, including the requirements for CDD, record keeping and SARs.
- 3.9** One of the most important controls over the prevention and detection of money laundering is to have employees who are alert to the risks of money laundering and terrorist financing, and who are well trained in the identification of unusual activities or transactions which appear to be suspicious. The effective application of even the best designed control systems can be quickly compromised if the employees applying the systems are not adequately trained. The effectiveness of the training will therefore be important to the success of the operator's AML/CTF strategy.
- 3.10** Operators should devise and implement a clear and well articulated policy and procedure for ensuring that relevant employees are aware of their legal obligations in respect of the prevention of money laundering and terrorist financing, and for providing them with regular training in the identification and reporting of anything that gives grounds for suspicion of money laundering or terrorist financing.
- 3.11** Under POCA and the Terrorism Act, individual employees face criminal penalties if they are involved in money laundering or terrorist financing. If they do not make an internal report to their nominated officer when necessary they may also face criminal sanctions. It is important, therefore, that employees are made aware of their legal obligations, and are given training in how to discharge them.
- 3.12** The Regulations require operators to take appropriate measures so that all relevant employees are:
- made aware of the law relating to money laundering and terrorist financing; and
 - regularly given training in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing.¹¹
- 3.13** 'Relevant employees' includes the holders of personal management licences and personal functional licences issued by the Commission as well as employees responsible for completing CDD measures. It does not include any ancillary employees such as catering and bar staff.
- 3.14** The content of any training, the regularity of training and the assessment of competence following training are matters for each operator to assess and decide in light of the money laundering risks they identify. The Commission will expect such issues to be covered in each operator's policies and procedures. This should make provision for the attainment of

¹¹ Regulation 21.

an appropriate competence level by the relevant employees identified in paragraph 3.13, prior to them undertaking the duties for which they will be responsible. This may, for example, be achieved by the attainment of an appropriate pass rate in a competency test following training.

- 3.15** Operators should also ensure that relevant employees are aware of and understand:
- their responsibilities under the operator's policies and procedures for the prevention of money laundering and terrorist financing;
 - the money laundering and terrorist financing risks faced by an operator and each of its casino premises;
 - the operator's procedures for managing those risks;
 - the identity, role and responsibilities of the nominated officer, and what should be done in his absence;
 - the potential effect of a breach upon the operator and upon its employees;
 - how the casino will undertake CDD;
 - how the casino will track customers when CDD is not undertaken on entry to the casino; and
 - how PEPs will be identified
- 3.16** There is no single solution when determining how to deliver training and a mix of training methods may, therefore, be appropriate. On-line training systems can provide a solution for many employees, but this approach may not be suitable for all employees. Classroom training can be more effective in these circumstances.
- 3.17** Procedure manuals, whether paper or electronic, are useful in raising employee awareness and can supplement more dedicated forms of training, but their main purpose is generally to provide ongoing reference rather than being written as training material.
- 3.18** Ongoing training should be given to all relevant employees at appropriate intervals. Records should be maintained to monitor who has been trained, when they received the training, the nature of the training and the effectiveness of the training.
- 3.19** The nominated officer should be heavily involved in devising and managing the delivery of such training, taking particular care to ensure that systems are in place to cover all part-time or casual employees.
- 3.20** SOCA publishes a range of material at www.soca.gov.uk, such as threat assessments and risk profiles, of which operators may wish to make their employees aware. The information on this website could usefully be incorporated into operators' training materials.

4 Nominated officer

- 4.1** Licensed casino operators must appoint a nominated officer, who is responsible for:¹²
- receiving internal disclosures under Part 7 of POCA and Part 3 of the Terrorism Act;
 - deciding whether these should be reported to SOCA;
 - if appropriate, making such external reports; and
 - ensuring that appropriate consent is applied as necessary.
- 4.2** A nominated officer should be able to monitor the effectiveness of the day-to-day operation of the operator's AML/CTF policies, and respond promptly to any reasonable request for information made by the Commission or law enforcement bodies.
- 4.3** The term 'nominated officer' is used and defined in the Regulations.

¹² Regulation 20(2)(d)

Standing of the nominated officer

- 4.4** The nominated officer is responsible for the oversight of all aspects of the operator's AML/CTF activities at all premises. They are the focal point for all activity within the operator relating to AML. The individual appointed as nominated officer must have a sufficient level of seniority. The nominated officer must hold a personal management licence (PML) issued by the Commission. The job description of the nominated officer should clearly set out the extent of the responsibilities given to him and his objectives. The nominated officer will need to be involved in establishing the basis on which a risk-based approach to the prevention of money laundering and terrorist financing is put into practice.
- 4.5** The nominated officer must:
- have the authority to act independently in carrying out his responsibilities
 - be free to have direct access to the Commission and appropriate law enforcement agencies, including SOCA
 - be free to liaise with SOCA on any question of whether to proceed with a transaction in the circumstances, that is, in relation to appropriate consent.
- 4.6** Senior management of the operator must ensure that the nominated officer has sufficient resources available to him, including appropriate employees and technology. This should include arrangements that apply in his temporary absence.
- 4.7** Where a nominated officer is temporarily unavailable, another PML holder may deputise. Operators should consider the appointment of a permanent deputy nominated officer.
- 4.8** Where AML/CTF tasks are delegated by an operator's nominated officer, the Commission will expect the nominated officer to take ultimate managerial responsibility and they are likely to remain liable for the commission of any criminal offences relating to POCA, the Terrorism Act or the Regulations. The Commission strongly recommends that in such circumstances:
- the fact, date and time of such delegation be entered contemporaneously in a written record;
 - the delegate counter-signs by way of acceptance of responsibility; and
 - all employees who need to be aware of such delegation, are notified immediately.

Internal and external reports

- 4.9** An operator must require that anyone working for the operator, to whom information or other matter comes in the course of business, as a result of which they know or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing must make an internal report to their nominated officer. Whilst disclosure to another of the fact that a person may be engaged in money laundering is generally an offence, such disclosures to a 'nominated officer' are specifically protected, where they are made as soon as is practicable and in the course of the discloser's employment.¹³ It is recommended that employees be made aware that they have a legal defence to prosecution if they make an internal report to the nominated officer as soon as is reasonably practicable after the information or other matter comes to their attention.
- 4.10** Any internal report should be considered by the nominated officer, in the light of all other relevant information, to determine whether or not the information contained in the report leads them to form knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of money laundering or terrorist financing.
- 4.11** The nominated officer should consider any information held about the customer's personal circumstances that might be available to the operator; and review other transaction

¹³ Section 337 of POCA.

patterns and volumes through the account or accounts in the same name, the length of the business relationship and identification records held.

4.12 The nominated officer must be fully conversant with his legal obligations to make external reports to SOCA.

4.13 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 SOCA.

5 Customer due diligence

Introduction

5.1 A key requirement in the Regulations is the requirement to make checks on customers, known as customer due diligence or CDD.¹⁴ Casino operators may take one of two approaches; identifying and verifying the identity of all customers on entry to the casino's licensed premises or undertaking identification and verification when a customer approaches the threshold set out in the Regulations.

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

5.3 The Regulations define casino as 'the holder of a casino operating licence'.¹⁵ CDD therefore may be conducted just once by the holder of an operating licence and does not need to be repeated each time a customer visits another casino operated by that licensee. CDD records held by a casino operator will need to be available across the operator's different casino premises and the policies and procedures must include details of how the operator will manage this. Operators should note that CDD is ongoing and may need updating for changes in the customer's circumstances and personal details.

Threshold approach

5.4 The Regulations set out thresholds which, if customer transactions approach this level, require the casino operator to verify the identity of the customer. These limits are:

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

5.5 The gaming machine limits only apply in premises based casinos. By separating the purchase or exchange of chips from the payment to use gaming machines there is the potential for customers to spend up to €2,000 in the machines in addition to the purchase or exchange of chips up to €2,000. It should be noted that for the purpose of this guidance 'gaming machine' and 'stake' have the same meaning as that in the Act

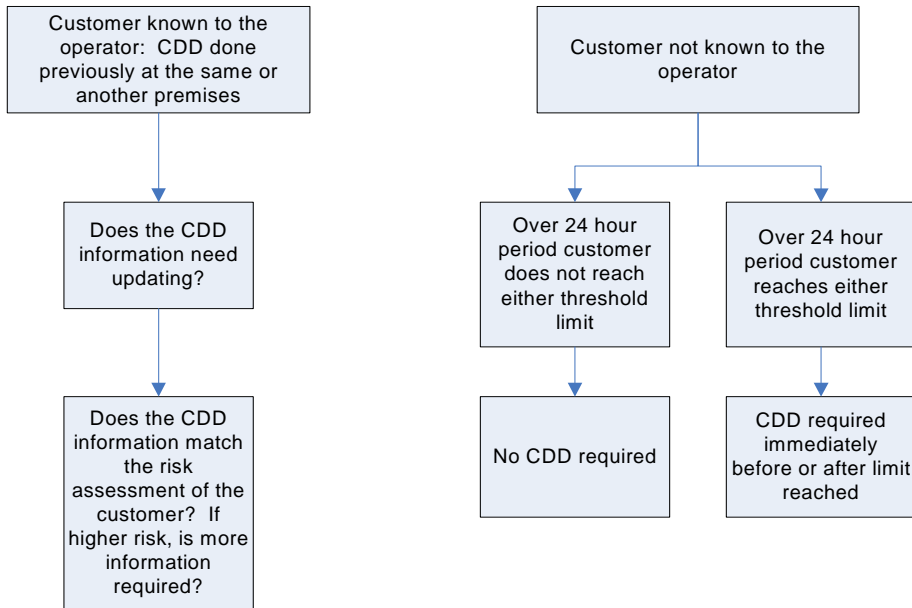
5.6 In premises based casinos automated and semi-automated table games such as touch-bet roulette are not defined as gaming machines and therefore the take in these games should be counted towards the threshold approach for chips.

¹⁴ Regulation 10.

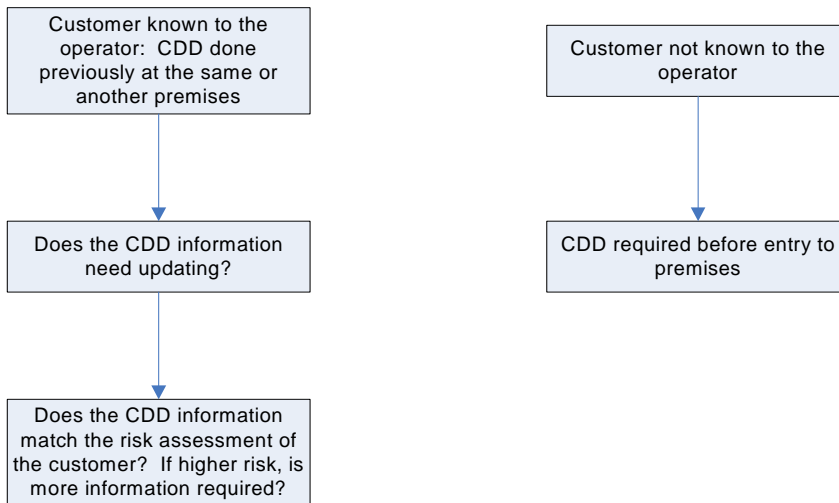
¹⁵ Regulation 3(13).

Figure 2: Customer due diligence

Threshold model



On entry model

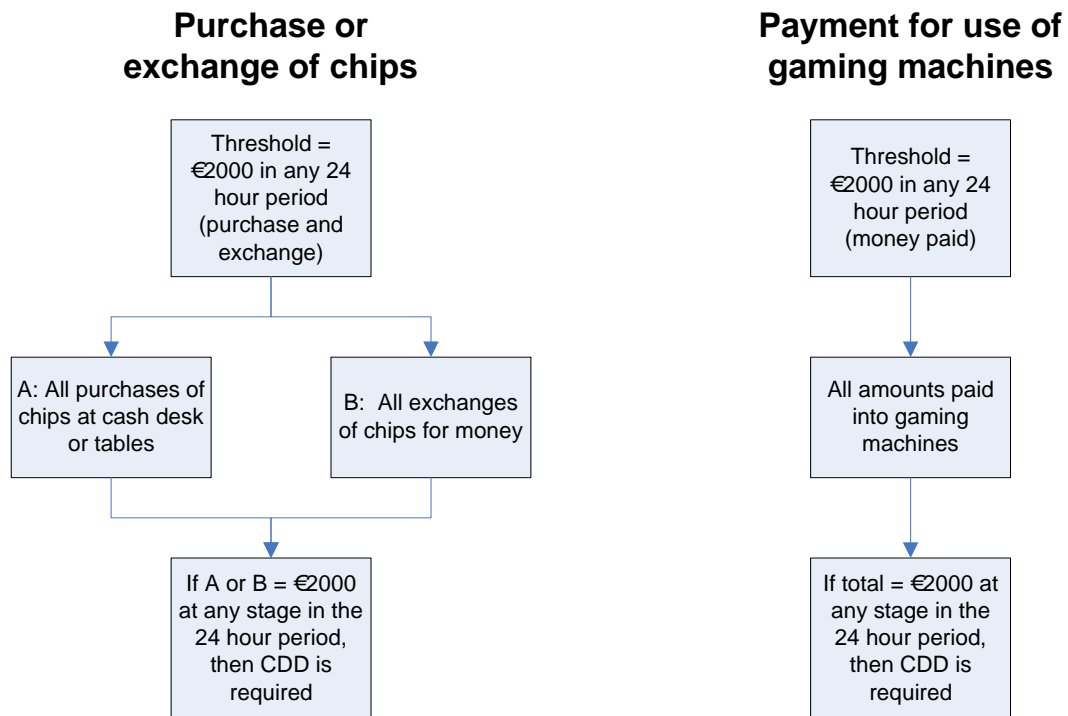


Notes:

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.

- 5.7** If casinos wish to adopt the threshold approach, the following two conditions must be satisfied:
- it must verify the identity of each customer before, or immediately after, the customer purchases, exchanges, pays or stakes €2,000 or more; and
 - the Commission must be satisfied that the casino operator has appropriate procedures in place to monitor and record the total value of chips purchased from or exchanged with the casino, the total money paid for the use of gaming machines, or the total money paid or staked in connection with facilities for remote gaming by each customer.
- 5.8** Casino operators will have to satisfy the Commission that they have the mechanisms in place that are appropriate for the spend profile in each premises. For example, a casino with a customer drop/win average considerably below the threshold will need mechanisms in place to monitor customer transactions to be sure that any customer reaching either of the threshold levels is picked up in good time to allow CDD to be completed. Where the operator has a number of premises, the Commission will consider the use of the threshold approaches for each casino premises rather than for an operator.
- 5.9** Casinos adopting the threshold approach should think carefully about whether they wish to defer both identification and verification until the threshold is reached, or whether identification will be conducted on entry but verification deferred until the threshold is reached. For example, a premises based casino may operate a membership scheme where customers are identified on admission but verification only occurs once the threshold is approached. Similarly, remote casinos may require customers to identify themselves (and undertake age verification) on registering with the casino but only require verification of identity if the threshold is approached.
- 5.10** There may be significant advantages in asking customers for their identification on entry, even if verification of this information is deferred until the threshold is reached, for example, identifying customers on entry means it will not be necessary to interrupt the customer's gambling once the threshold is reached, and verification becomes necessary.
- 5.11** Casinos have to monitor both purchase and exchange of chips. If either hits the threshold CDD will be necessary.
- 5.12** A key challenge for casinos wishing to adopt the threshold approach is keeping track of the level of all an individual customer's purchases and exchanges of chips, and spends on the gaming machines. However, it is appropriate to do so in light of the known spend patterns in each premises.
- 5.13** Should casino operators choose to adopt the threshold approach, they must satisfy the Commission, on a premises-by-premises basis, that they have the appropriate procedures in place to manage the threshold in light of the assessed money laundering risk and spending profile at each premises.

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

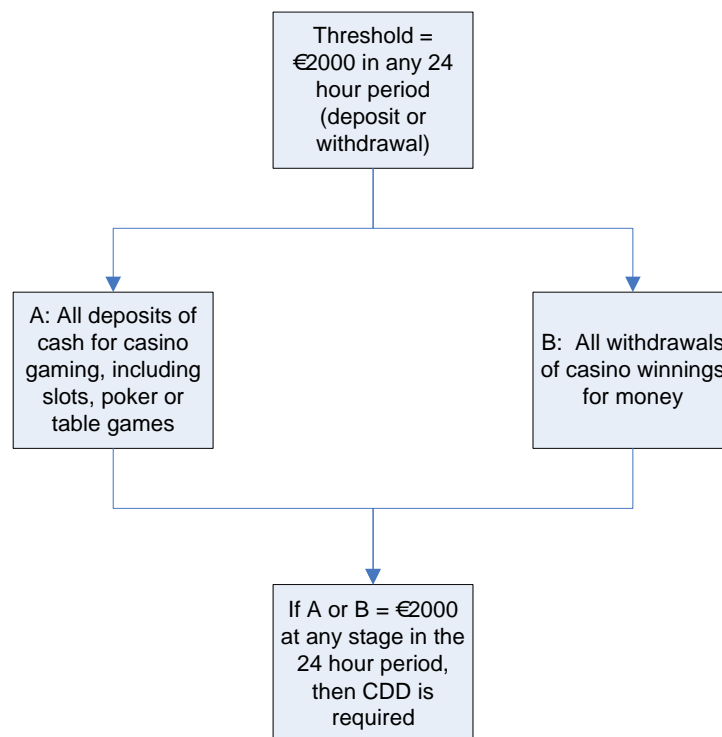


Notes:

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

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

**Depositing or withdrawing
casino account funds**

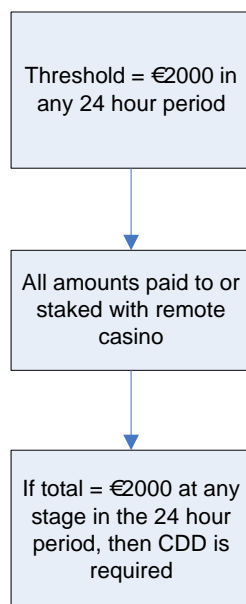


Notes:

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

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

Payment to remote casino



Notes:

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

- 5.14** Some remote casinos operate a ‘wallet’ system which allows customers to use the money in their wallet in different parts of the operator’s site. An operator’s site may include some casino games as well as other games. It is only when a customer first enters the casino part of an operator’s website and stakes money or chips that the CDD requirements apply. The Regulations do not apply to people ‘window shopping’ in a remote casino’s website, it applies only when money is staked. Where an operator is unsure of what the funds in the wallet will be used for (for example, casino or sports betting) they should consider applying these controls to all customers.
- 5.15** Casinos using the ‘threshold approach’ must be sure that they are able to end transactions with a customer who reaches the threshold if they are unable to comply with the CDD requirements.
- 5.16** The Commission has not determined the start of a 24 hour period for the purposes of the Regulations. Casino operators are free to choose the start time of their 24 hour period (previously referred to as the ‘business day’) to meet the demands of their business.

Identification and verification on entry

- 5.17** The ‘on entry’ approach requires casinos to identify and verify the identity of the customer before entry to any premises where gaming facilities are provided, or before access is given to remote gaming. Once the customer’s identity is verified he may commence gaming.
- 5.18** If a casino using the ‘on entry’ approach to CDD is unable to complete the appropriate CDD they must not allow the customer access to the premises or to the remote gaming. This puts a stop, in non-remote casinos, to the current practice of allowing guests of known customers a single entry without undertaking CDD. However, operators should consider using variations of the threshold CDD approach for guests of casino members.

Identification and verification

- 5.19** Applying CDD measures involves several steps. The operator is required to identify customers and then verify their identities, either upon entry or when reaching the threshold. Identification of a customer is being told or coming to know of the customer’s identifying details, such as their name and address. Verification is obtaining some evidence which supports this claim of identity. The operator *identifies* the customer by obtaining a range of information about him. The *verification* of the identity consists of the operator verifying some of this information against documents, data or information obtained from a reliable and independent source.
- 5.20** Identification of customers consists of a number of aspects, including the customer’s name, current and past addresses, date of birth, place of birth, physical appearance, employment and financial history, and family circumstances.
- 5.21** Casino operators may identify their customers simply by asking them for personal information, including name, home address and date of birth. Other sources of identity can include:
- identity documents such as passports and photocard driving licences presented by customers
 - other forms of confirmation, including assurances from persons within the regulated sector (for example, banks) or employees within the same casino or casino group who have dealt with the customer for some time.

Some or all of this information will need to be verified. It may also be helpful to obtain information on customers’ source of funds and level of legitimate income, for example occupation. This information may assist casinos with their assessments about whether a customer’s level of gambling is in profile for their approximate income, or whether it is suspicious.

- 5.22** Information about customer identity must then be verified through documents, data and information which come from a reliable and independent source. There are a number of ways that a person's identity can be verified, including:
- obtaining or viewing original documents
 - conducting electronic verification
 - obtaining information from another person in the regulated sector (for example, banks).

No method of verification, either documentary or electronic, can conclusively prove that the customer definitely is who they claim to be. However, the Commission expects casinos to be reasonably satisfied following appropriate inquiry that customers are who they claim to be.

- 5.23** It is generally considered good practice to require either:
- one government document which verifies either name and address, or name and date of birth
 - a government document which verifies the customer's full name and another supporting document which verifies their name and either their address or date of birth.

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

Electronic verification

- 5.25** Increasingly casinos use reliable electronic systems to help with verification. Some of these systems also have the advantage of assisting in the identification of PEPs. The amount of electronic information available about individuals will vary, depending on the extent of their electronic 'footprint'.
- 5.26** Electronic data sources can provide a wide range of confirmatory material without necessarily requiring the customer to produce documents. Electronic sources can be a convenient method of verification. They can be used either as the sole method of verification, or in combination with traditional document checks, on a risk basis. For an electronic check to provide satisfactory evidence of identity on its own it must use data from multiple sources, and across time, or incorporate qualitative checks that assess the strength of the information supplied. An electronic check that accesses data from a single source (for example, a single check against the electoral roll) is not enough on its own to verify identity.
- 5.27** Where such sources are used for a credit check, the customer's permission is required under the Data Protection Act 1998 (the Data Protection Act). Credit checks can provide inexpensive information on which to assess a customer's access to funds and to obtain a credit profile to match against spending patterns. For example, a criminal spending large amounts of criminal property would most likely not match his or her credit profile. A search for identity verification for AML/CTF purposes, however, leaves a different 'footprint' on the customer's electronic file, and the customer's permission is not required, but they must be informed that this check is to take place. There are systems available that give typical financial and lifestyle profiles of people in a given postcode, such systems do not amount to credit check and do not require the use of personal information but can provide helpful indicators of someone's expected financial profile.

- 5.28** Some external electronic databases are accessible directly by casinos but it more likely they will be purchased from an independent third party organisation. The size of the electronic 'footprint' in relation to the depth, breadth and quality of data, and the degree of corroboration of the data supplied by the customer may provide a useful basis for an assessment of the degree of confidence in the product.
- 5.29** A number of commercial agencies which access many data sources are accessible online by operators, and may provide operators with a composite and comprehensive level of electronic verification through a single interface. Such agencies use databases of both positive and negative information, and many also access high-risk alerts that utilise specific data sources to identify high-risk conditions, for example, known identity frauds or inclusion on a sanctions list.
- 5.30** Positive information (relating to full name, current address, date of birth) can prove that an individual exists, but some can offer a higher degree of confidence than others. Such information should include data from more robust sources – where an individual has to prove their identity, or address, in some way in order to be included, as opposed to others, where no such proof is required.
- 5.31** Negative information includes consideration of lists of individuals known to have committed fraud, including identity fraud, and registers of deceased persons. Checking against such information may be appropriate where other factors suggest an increased risk of impersonation fraud.

Criteria for use of an electronic data provider

- 5.32** Before using a commercial agency for electronic verification, operators should be satisfied that information supplied by the data provider is considered to be sufficiently extensive, reliable and accurate. This judgement may be assisted by considering whether the provider meets all the following criteria:
- it is recognised, through registration with the Information Commissioner's Office, to store personal data;
 - it uses a range of positive information sources that can be called upon to link an applicant to both current and previous circumstances;
 - it accesses negative information sources, such as databases relating to identity fraud and deceased persons;
 - it accesses a wide range of alert data sources; and
 - it has transparent processes that enable the operator to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject.
- 5.33** In addition, a commercial agency should have processes that allow the enquirer to capture and store the information they used to verify identity.
- 5.34** It is important that the process of electronic verification meets a standard level of confirmation before it can be relied on. The standard level of confirmation, in circumstances that do not give rise to concern or uncertainty, is:
- one match on an individual's full name and current address, and
 - a second match on an individual's full name and either his current address or his date of birth.
- 5.35** Commercial agencies that provide electronic verification use various methods of displaying results – for example, by the number of documents checked, or through scoring mechanisms. Operators should ensure that they understand the basis of the system they use, in order to be satisfied that the sources of the underlying data meet the required standard.

Documentary evidence

- 5.36** If verification is undertaken using documents, casino operators should usually rely upon documents issued by government departments.
- 5.37** 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 SOCA. Casino operators should also be aware that even if documents appear to be legitimate and issued by a government department they may be false, for example, the European driving permit that is 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.
- 5.38** If documents are in a foreign language appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity, for example, a translation of the relevant sections.
- 5.39** Documentation purporting to offer evidence of identity may emanate from a number of sources. These documents differ in their integrity, reliability and independence. Some are issued after CDD on the holder of the document is carried out by the issuing authority. There is a broad hierarchy of documents.
- 5.40** Documents issued by government departments and agencies that contain a photograph may be considered reliable. In practical terms, for face-to-face verification conducted by non-remote casinos, production of a valid passport or photocard driving licence should enable most individuals to meet the identification requirement for AML/CTF purposes. These documents will also confirm either residential address or date of birth.
- 5.41** Alternatively government issued documents without a photograph may be used which incorporates the customer's full name, supported by a second document, which is ideally also government issued, or issued by a public sector body or authority. This second document must also include the customer's full name and either his residential address or his date of birth.
- 5.42** The following sources may, therefore, be useful for verification of UK-based customers:
- current signed passport
 - birth certificate
 - current photocard driving licence
 - current EEA member state identity card
 - current identity card issued by the Electoral Office for Northern Ireland
 - residence permit issued by the Home Office
 - firearms certificate or shotgun licence
 - benefit book or original notification letter from the Department of Works and Pensions confirming the right to benefits
 - council tax bill
 - utility bill or statement (but not ones printed off the internet), or a certificate from a utilities supplier confirming an arrangement to pay services on pre-payment terms
 - bank, building society or credit union statement or passbook containing current address (but not statements printed off the internet) - bank or credit cards alone will not be sufficient as these do not provide either residential address or date of birth
 - confirmation from an electoral register that a person of that name lives at that address
 - recent original mortgage statement from a recognised lender

- solicitor's letter confirming recent house purchase or land registry confirmation of address
- local council or housing association rent card or tenancy agreement
- HM Revenue and Customs (HMRC) self-assessment statement or tax demand
- house or motor insurance certificate.

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

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

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

Politically exposed persons

Definition

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

- heads of state, heads of government, ministers and deputy or assistant ministers
- members of parliament
- members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances
- members of courts of auditors or of the boards of central banks
- ambassadors, charge d'affaires and high ranking officers in armed forces
- members of the administrative, management or supervisory bodies of state-owned enterprises.¹⁶

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

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

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

Risk-based approach to PEPs

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

¹⁶ Regulation 14(5) and Schedule 2.

- 5.47** Establishing whether individuals are PEPs is not always straightforward and can present difficulties. Where operators need to carry out specific checks, they may be able to rely on an internet search engine, or consult relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations. Resources such as the Transparency International Corruption Perceptions Index, which ranks approximately 150 countries according to their perceived level of corruption, may be helpful in assessing the risk. This can be found at www.transparency.org/policy_research/surveys_indices/cpi. If there is a need to conduct more thorough checks, or if there is a high likelihood of an operator having PEPs for customers, subscription to a specialist PEP database may be the only adequate risk mitigation tool.
- 5.48** 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, if they change their job or retire. The operator should, as far as practicable, be alert to public information relating to possible changes in the status of its customers with regard to political exposure. Casino operators should be alert to situations which suggest that the customer is a PEP. These situations include:
- receiving funds from a government account
 - correspondence on an official letterhead from the customer or a related person
 - general conversation with the customer or related person linking the person to a PEP
 - news reports suggesting that your client is a PEP or is linked to one.
- 5.49** Although under the definition of a PEP an individual ceases to be so regarded after he has left office for one year, operators are encouraged to apply a risk-based approach in determining whether or when they should cease carrying out appropriately enhanced monitoring of transactions. In many cases, a longer period might be appropriate, in order to ensure that the higher risks associated with the individual's previous position have adequately abated.
- 5.50** Each operator's policies and procedures should cover when and how customers will be checked for PEP status.

PEPs requirements

- 5.51** An operator who proposes to allow a PEP to be a customer must:
- have approval from its senior management for establishing a business relationship with that person;
 - take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship; and
 - where a business relation is entered into, conduct enhanced ongoing monitoring of the relationship.
- 5.52** Each operator's policies and procedures should cover how and when senior management approval will be sought and provided, and deal with how the customer will be dealt with if there is any delay to approval being provided.

Failure to complete checks

- 5.53** Where a casino operator is unable to comply with the required CDD measures in relation to a customer, the operator:
- must not carry out a transaction with or for the customer through a bank account;
 - must not establish a business relationship or carry out an occasional transaction with the customer;
 - must terminate any existing business relationship with the customer; and

- must consider making a report to SOCA.¹⁷

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

Requirements for remote casinos

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

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

Existing customers

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

List of persons subject to financial sanctions

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

¹⁷ Regulation 11.

- 5.59** Financial restrictions in the UK are governed by various pieces of legislation. The purpose of imposing financial restrictions is to restrict the access to finance by designated persons and to prevent the diversion of funds to terrorism and terrorist purposes. In all circumstances, where an asset freeze is imposed, it is unlawful to make payments to or allow payments to be made to designated persons.
- 5.60** A list of all financial restrictions currently in force in the UK is maintained by the Treasury's Asset Freezing Unit. The Consolidated List of persons designated as being subject to financial restrictions can be found on the HM Treasury web site at: www.hm-treasury.gov.uk/financialsanctions. Further information on financial restrictions can also be found via this website. The purpose of the HM Treasury list is to draw together, in one place, all the names of designated persons for the various financial restrictions regimes effective in the UK.
- 5.61** Under the relevant legislation, it is a criminal offence for any natural or legal person to:
- deal with the funds of designated persons;
 - make funds and economic resources, and in the case of terrorism financial services, available, directly or indirectly to or for the benefit of designated persons; or
 - knowingly and intentionally participate in activities that would directly or indirectly circumvent the financial restrictions or enable or facilitate the commission of an offence relating to the above.
- 5.62** In this context, “deal with” means:
- in respect of funds, to use, alter, move, allow access to or transfer;
 - in respect of funds, deal with in any other way that would result in any change in volume, amount, location, ownership, possession, character or destination; or
 - in respect of funds, make any other change that would enable use, including portfolio management; and
 - in respect of economic resources, to use to obtain funds, goods or services in any way, including (but not limited to) by selling, hiring or mortgaging the resources.
- 5.63** HM Treasury has the power to grant licences exempting certain transactions from the financial restrictions. Requests to disapply the financial restrictions in relation to a designated person are considered by the Treasury on a case-by-case basis to ensure that there is no risk of funds being diverted to otherwise restricted purposes. To apply for a licence, the Asset Freezing Unit at HM Treasury can be contacted using the contact details provided below.
- 5.64** Operators need to have the necessary policies and procedures in place to monitor financial transactions so that payments are not made to designated persons, thereby preventing breaches of the financial restrictions legislation. For manual checking, operators can register with the HM Treasury Asset Freezing Unit update service (directly or via a third party). If checking is automated, operators will need to ensure that the relevant software includes checks against the latest Consolidated List.
- 5.65** The Asset Freezing Unit may also be contacted to provide guidance and to assist with any concerns regarding financial restrictions at:
- Asset Freezing Unit
Tel: 020 7270 5664/5454
Fax: 020 7451 7677
Email: assetfreezingunit@hmtreasury.gsi.gov.uk
- 5.66** In the event that a customer or a payee is identified as a designated person, payments must not proceed unless a licence is granted by the Treasury, as this would be a breach of the financial restrictions. The Treasury should be informed immediately and the transaction suspended pending their advice. No funds should be returned to the

designated person. The firm may also need to consider whether there is an obligation also to report to SOCA under POCA or the Terrorism Act.

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

6 Record keeping

General legal and regulatory requirements

6.1 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.

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

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

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

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

Business relationships

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

6.5 Casinos are likely to form a business relationship when:

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

6.6 'Ongoing monitoring of business relationships' is a requirement for casino operators and includes scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, his business and risk profile.¹⁸

6.7 Casinos are expected to approach this requirement on a risk basis. Dependent on how frequently a casino forms 'business relationships' it may be good practice to apply ongoing monitoring more widely. Regular players should be the subject of closer scrutiny and their level of play should be assessed with reference to the information already known about

¹⁸ Regulation 8(1)

them, and where necessary, additional information must be collected and retained about the source of their funds.

Occasional transaction

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

Other casino customers

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

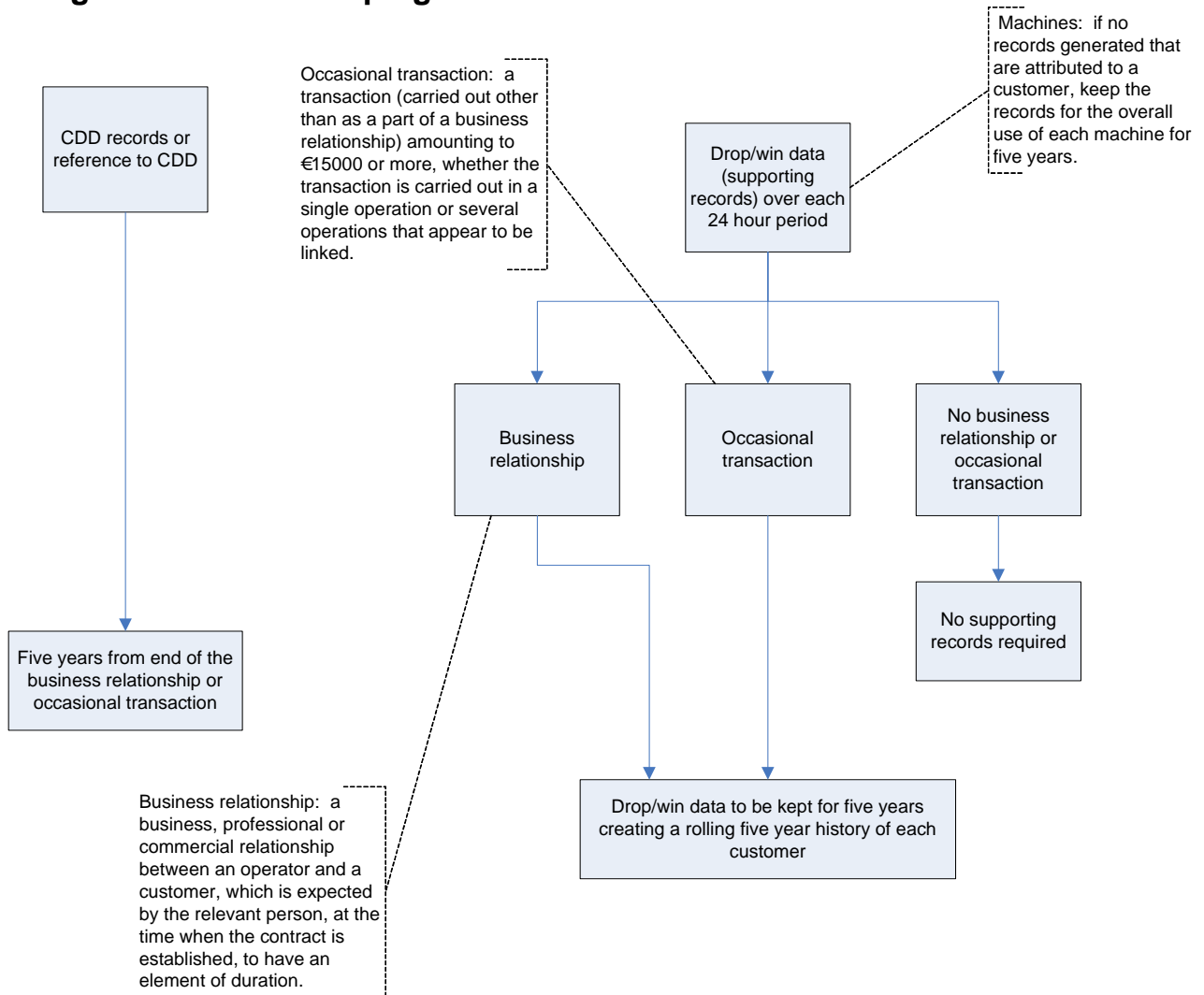
Customer information

- 6.10** In relation to the evidence of a customer's identity, operators must keep a copy of, or the references to, the verification evidence of the customer's identity obtained during the application of CDD measures.¹⁹
- 6.11** An operator may often hold additional information beyond identity in respect of a customer for the purposes of wider customer due diligence. As a matter of best practice this information and any relevant documents should also be retained.
- 6.12** There is a separate requirement in the Regulations to ensure that documents, data or information held by casinos are kept up to date.²⁰ A trigger event for refreshing and extending CDD may be if a customer returns to a casino after a period of non-attendance. Refreshing information about existing customers will ensure that matters such as change of address, or a customer being appointed into a role which attracts PEP status, will be picked up. Keeping information up to date is also a requirement under the Data Protection Act. How these issues which will be dealt with in practice should be covered in the casino's policies and procedures.

¹⁹ Regulation 19(2).

²⁰ Regulation 8(2)(b).

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 .

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

Supporting records – non-remote casinos

- 6.14** The requirement to keep supporting records is linked to 'business relationships' and 'occasional transactions' which are defined in the Regulations²¹ and the extent and nature of records created. In many casinos customers, regardless of whether or not they have formed a business relationship, or are part of an occasional transaction, purchase chips with cash at the gaming tables where, in low risk situations, no records are created and therefore not available to be kept.
- 6.15** The Commission expects casino operators to use reasonable endeavours to create and keep supporting records and to make it clear in their policies and procedures what records will be created in light of the known spending patterns and the assessed money laundering and terrorist financing risks at each premises.
- 6.16** Casinos currently undertake a process at the end of each business day to count the total drop (cash used to purchase chips) to compare against the total amount recorded through tracking individual customer spending. The difference between the two figures is the amount of drop that is not attributable to particular customers. This in turn can be calculated against known attendance figures and the number of customers tracked to give an average amount of money used to purchase chips per customer that has not been tracked, and therefore with no supporting records. This process should continue and should form part of the on-going risk-assessment for each premises. The records created during this process should be retained.
- 6.17** Any casino operator devising its record keeping policy and procedure should decide how its business fits within the definitions of 'business relationship' or 'occasional transaction'. The variation in the record-keeping requirements for different circumstances illustrates the flexibility available to casinos which allows them to focus their resources on higher money laundering risk situations.
- 6.18** For the purposes of supporting records, the Commission takes the view that in most cases this will consist of records covering the drop/win figures, subject to paragraph 6.9, for each customer for each 24 hour period. There is no requirement to keep detailed records for each customer for each table or game for AML purposes. However, HMRC may require operators to maintain records for each table or game but not broken down by each customer's transactions.

Supporting records – remote casinos

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

Supporting records – gaming machines

- 6.20** 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

²¹ Regulation 2(1).

retained by the casino. However, 'ticket in, ticket out' (TITO) and 'smart card' technology may mean that, in the future, machines produce supporting records that can be attributed to a customer who falls within the record keeping requirements, in which case such records must be retained in accordance with the Regulations.

- 6.21** The essentials of any system of monitoring are that:
- it flags up transactions and/or activities for further examination;
 - these reports are reviewed promptly by the nominated officer; and
 - appropriate action is taken on the findings of any further examination.
- 6.22** Monitoring can be either:
- in real time, in that transactions and/or activities can be reviewed as they take place or are about to take place; or
 - after the event, through the nominated officer's review of the transactions and/or activities that a customer has undertaken.
- In either case, unusual transactions or activities should be flagged for further examination.
- 6.23** In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer risk.
- 6.24** Monitoring is not a mechanical process and does not necessarily require sophisticated electronic systems. The scope and complexity of the process will be influenced by the operator's business activities, and whether the operator is large or small. The key elements of any system are having up-to-date customer information, on the basis of which it will be possible to spot the unusual, and asking pertinent questions to elicit the reasons for unusual transactions or activities in order to judge whether they may represent something suspicious.

Retention period

- 6.25** Records of identification and verification of customers must be kept for a period of at least five years after the relationship with the customer has ended.²² The date the relationship with the customer ends is the last date on which they visit or use a casino.
- 6.26** Supporting records must be retained for a period of five years beginning on the date any transaction is completed where the records relate to a particular transaction. This creates a rolling five year history of drop/win data. Records of internal and external reports on suspicious activity should be retained for five years from when the report was made.²³

Form in which records have to be kept

- 6.27** Most operators have record keeping procedures which they keep under review, and will seek to reduce the volume and density of records which have to be stored, whilst still complying with statutory requirements. Retention may therefore be:
- by way of original documents;
 - by way of photocopies of original documents;
 - on microfiche;
 - in scanned form; or
 - in computerised or electronic form.
- 6.28** Records relating to ongoing investigations should, where possible, be retained until the relevant law enforcement agency has confirmed that the case has been concluded.

²² Regulation 19(3).

²³ Regulation 19(3).

- 6.29** 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.

7 Suspicious activities and reporting

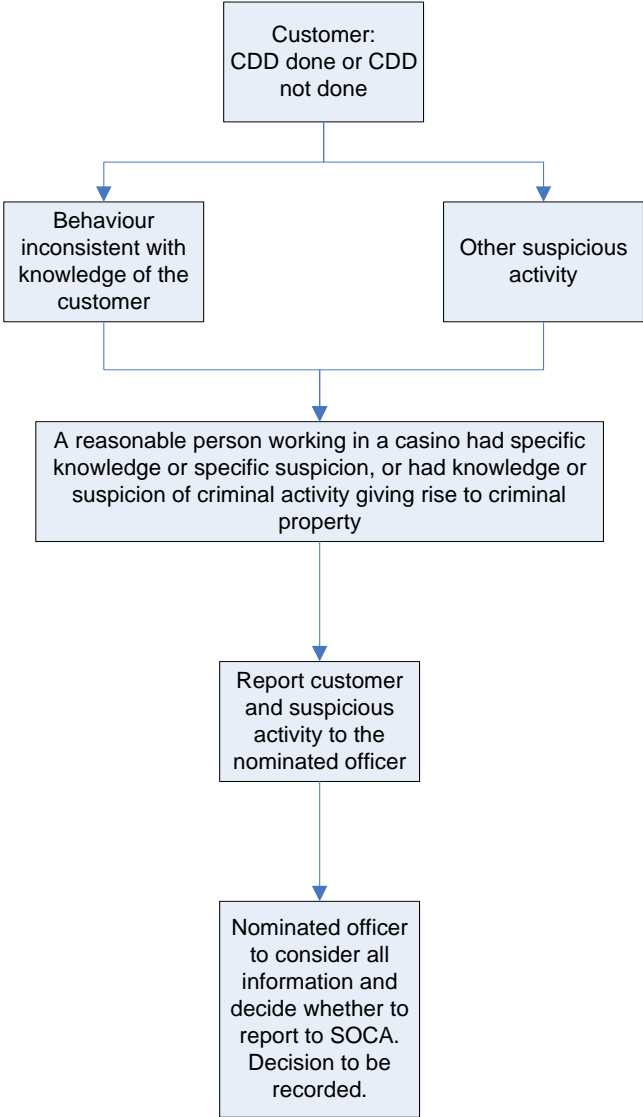
Introduction

- 7.1** Employees in casinos are required to make a report in respect of information that comes to them within the course of their business:
- where they know; or
 - where they suspect; or
 - where they have reasonable grounds for knowing or suspecting,
- that a person is engaged in money laundering or terrorist financing. Within this guidance, the above obligations are collectively referred to as 'grounds for knowledge or suspicion'.
- 7.2** In order to provide a framework within which suspicion reports may be raised and considered:
- each operator must ensure that any employee reports to the operator's nominated officer where they have grounds for knowledge or suspicion that a person or customer is engaged in money laundering or terrorist financing;
 - the operator's nominated officer must consider each such report, and determine whether it gives grounds for knowledge or suspicion;
 - operators should ensure that employees are appropriately trained in their obligations, and in the requirements for making reports to their nominated officer.
- 7.3** If the nominated officer determines that a report does give rise to grounds for knowledge or suspicion, he must report the matter to SOCA. Under POCA, the nominated officer is required to make a report to SOCA as soon as is practicable if he has grounds for suspicion that another person, whether or not a customer, is engaged in money laundering. Under the Terrorism Act, similar conditions apply in relation to disclosure where there are grounds for suspicion of terrorist financing.

What is meant by knowledge and suspicion?

- 7.4** Having knowledge means actually knowing something to be true. In a criminal court, it must be proved that the individual in fact knew that a person was engaged in money laundering. That said, knowledge can be inferred from the surrounding circumstances, so, for example, a failure to ask obvious questions may be relied upon by a jury to infer knowledge. The knowledge must, however, have come to the operator (or to the employee) in the course of casino business or (in the case of a nominated officer) as a consequence of a disclosure under section 330 of POCA. Information that comes to the operator or employee in other circumstances does not come within the scope of the regulated sector obligation to make a report. This does not preclude a report being made should employees choose to do so. Employees may also be obliged to make a report by other parts of the Act.

Figure 7: Reasonable grounds to suspect (objective test)



- 7.5** 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.
- 7.6** Whether you hold suspicion or not is a subjective test. If you think a transaction is suspicious you are not expected to know the exact nature of the criminal offence or that particular funds are definitely those arising from the crime. You may have noticed something unusual or unexpected and, after making enquiries, the facts do not seem normal or make commercial sense. You do not need to have evidence that money laundering is taking place to have suspicion.
- 7.7** 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 SOCA. The nominated officer is required to assess all of the circumstances and, in some cases, it may be helpful to ask the customer or others more questions. The choice depends on what is already known about the customer and the transaction, and how easy it is to make enquiries.
- 7.8** 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.

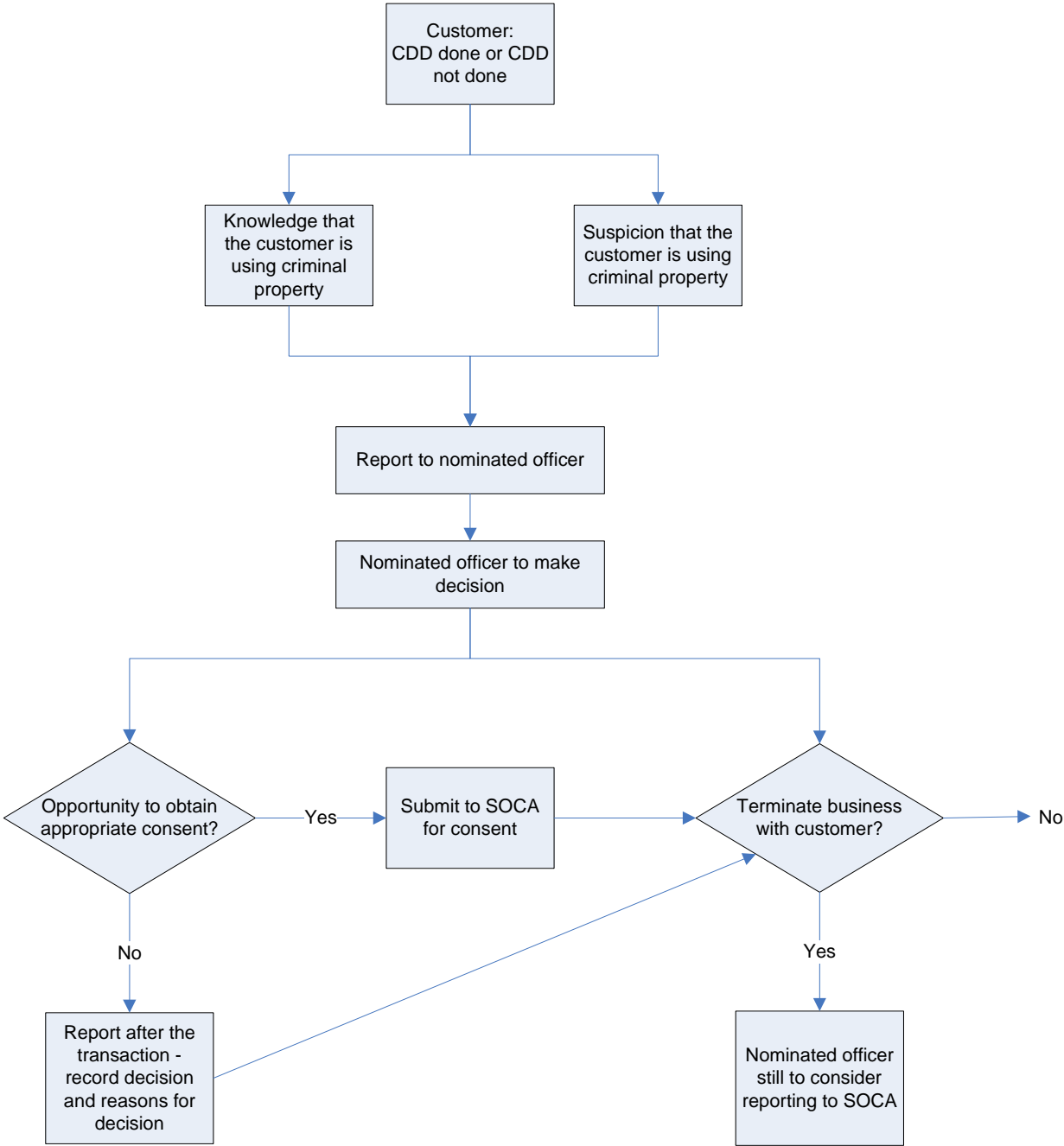
What is meant by reasonable grounds to know or suspect?

- 7.9** In addition to establishing a criminal offence relating to when suspicion or actual knowledge of money laundering, POCA creates criminal liability for failing to disclose information when reasonable grounds exist for knowing or suspecting that a person is engaged in money laundering or terrorist financing. This lower test, which introduces an *objective* test of suspicion, applies to all businesses covered by the Regulations, including remote and non-remote casinos. The test would likely be met when there are demonstrated to be facts or circumstances, known to the employee in the course of business, from which a reasonable person engaged in a casino business, would have inferred knowledge, or formed a suspicion, that another person was engaged in money laundering or terrorist financing.
- 7.10** 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.

Internal reporting

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

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



- 7.12** 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. 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.
- 7.13** Once an employee has reported his suspicion to the nominated officer, or to an individual to whom the nominated officer has delegated the responsibility to receive such internal reports, he has fully satisfied his statutory obligation.

Evaluation and determination by the nominated officer

- 7.14** The operator's nominated officer must consider each report and determine whether it gives rise to grounds for knowledge or suspicion. The operator must permit the nominated officer to have access to any information, including CDD information, in the operator's possession that could be relevant. The nominated officer may also require further information to be obtained, from the customer if necessary. Any approach to the customer should be made sensitively and probably by someone already known to the customer, to minimise the risk of alerting the customer or an intermediary that a disclosure to SOCA is being considered.
- 7.15** If the nominated officer decides not to make a report to SOCA, the reasons for not doing so should be clearly documented or electronically recorded, and retained. These records should be kept separately by the nominated officer in order that the information therein is not disclosed accidentally.

External reporting

- 7.16** To avoid committing a failure to report offence, the nominated officer must make a disclosure to SOCA where he decides that a report gives rise to grounds for knowledge or suspicion. The national reception point for the disclosure of suspicions, and for seeking consent to continue to proceed with the transaction or activity, is the UK Financial Intelligence Unit (UKFIU) within SOCA.
- 7.17** The nominated officer must report to SOCA any transaction or activity that, after his evaluation, he knows or suspects, or has reasonable grounds to know or suspect, may be linked to money laundering. Such reports must be made as soon as is reasonably practicable after the information comes to the nominated officer.
- 7.18** The Secretary of State may by order prescribe the form and manner in which a disclosure under section 330, section 331, section 332, or section 338, may be made. A consultation paper on the form and manner of reporting was issued by the Home Office in the summer of 2007, however, the Home Office decided not to proceed with the introduction of a prescribed form and manner for reporting.

Submission of suspicious activity reports

- 7.19** SOCA accepts the submission of SARs in three main ways:
- **Paper based reporting** using the standard SOCA Suspicious Activity Report Form. SOCA prefers submissions to be typed to enable it to be scanned and prevent errors in data entry. The form is available from the SOCA website at: www.soca.gov.uk/financialintel/suspectactivity.html#forms. Guidance on using the form can be found at www.soca.gov.uk/financialintel/formsguide.html

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

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

- **SAR Online** is a secure web based reporting system for small or medium sized reporting entities with access to the internet, which allows SARs to be submitted electronically through <https://www.ukfiu.gov.uk/saronline.aspx>. Reporters must register themselves as a source (reporting entity) on the system once, and then submit SARs by completing linked electronic screens that reflect the fields included in the paper based reports.

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

SAR Online is SOCA's preferred method for small and medium sized reporters to submit SARs. The benefit to the reporter is 24/7 reporting, an automatic acknowledgment of receipt with the ELMER reference number, an initial feedback report on the quality of the SARs submitted after 6 months, and investigators are able to access the information more rapidly.

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

7.20 Operators should include in each SAR as much relevant information about the customer, transaction or activity that it has in its records. SOCA has published a glossary of terms which they prefer operators to use when completing SARs (www.soca.gov.uk/financialIntel/SARglossary.html). This will assist in consideration of the report by SOCA.

7.21 In order that an informed overview of the situation may be maintained, all contact between operators and law enforcement agencies should be controlled through, or reported back to, the nominated officer or a deputy acting in the absence of the nominated officer.

Appropriate consent

7.22 If operators handle any proceeds of crime they may commit one of the POCA principal money laundering offences. However if the nominated officers makes a report to SOCA this can amount to a defence. The 'reporting defence' includes the statutory mechanism which allows SOCA either to agree to the transaction going ahead, or to prevent the suspected money laundering going ahead. This statutory mechanism is called 'appropriate consent'.

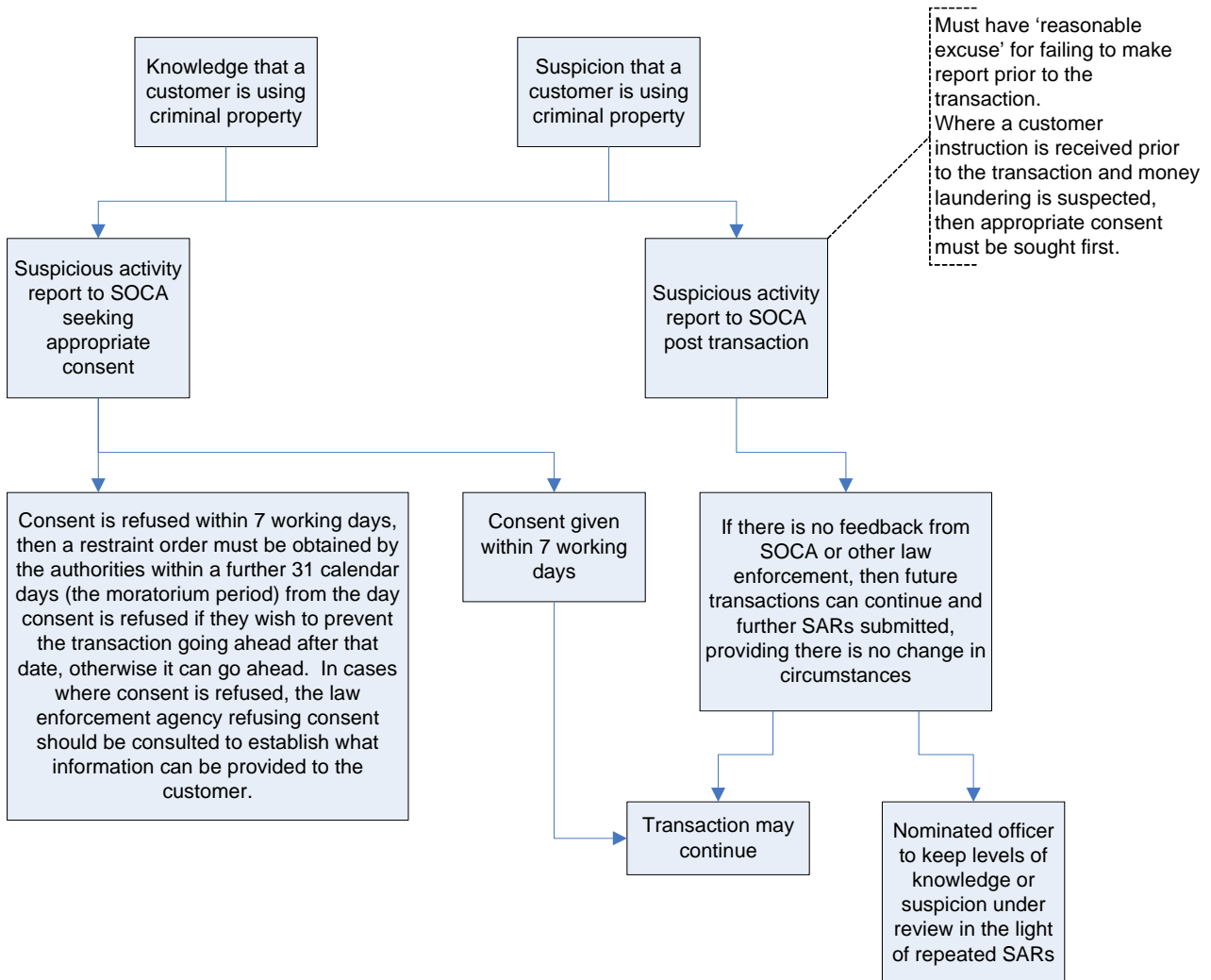
7.23 The nominated officer needs to consider how he will approach his reporting obligations and consider:

- the timing of the report(s) – particularly second or subsequent reports; and
- whether the operator wishes to continue to do business with the customer.

7.24 A nominated officer, police constable, SOCA employee or customs officer can give a person (which may include, for example, a casino employee) *actual* 'appropriate consent' to a suspect transaction proceeding. However, it should be noted that SOCA is the only

body able to issue formal notification of consent by means of an official SOCA letter, which the nominated officer can then retain for his records.

Figure 9: Appropriate consent



- 7.25** Alternatively, such a person will be *treated* as having the appropriate consent if notice is given to a police constable or customs officer (but not the nominated officer) and either:
- consent is not refused within seven working days (beginning with the day after the notice is given); or
 - 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.
- 7.26** However, the Act provides that a nominated officer *must not* give the appropriate consent unless he has himself already made a disclosure to an authorised officer of SOCA and, either:
- the SOCA employee has consented to the transaction; or
 - consent is not refused within seven working days (beginning with the day after the notice is given); or
 - 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.
- 7.27** Reporting suspicious activity before or reporting after the event are not equal options which an operator can choose between. 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. Where a customer instruction is received prior to a transaction or activity taking place, or arrangements being put in place, and there are grounds for knowledge or suspicion that the transaction, arrangements, or the funds/property involved, may relate to money laundering, a report must be made to SOCA and consent sought to proceed with that transaction or activity. In such circumstances, it is an offence for a nominated officer to consent to a transaction or activity going ahead within the seven working day notice period from the working day following the date of disclosure, unless SOCA gives consent.
- 7.28** In the casino environment business is often conducted out of normal office hours and in circumstances where it is not feasible to obtain appropriate consent prior to or during a transaction. Grounds for knowledge or suspicion may be triggered after a customer has completed the three stages of a gambling transaction; that is, they have bought in, they have played and they have cashed out. Under these circumstances it would be reasonable to report after the transaction. However, the defence of ‘reasonable excuse’ when reporting after the transaction is untested by case law, and would need to be considered on a case-by-case basis.
- 7.29** Casinos should include in their policies and procedures details on how they will manage circumstances where there is grounds for knowledge or suspicion of money laundering or terrorist financing. If knowledge or suspicion is present then there must be a mechanism for involvement of the senior manager on duty and contact with the nominated officer as soon as is practicable. If the circumstances amount to reasonable grounds to suspect, then reporting the matter to the nominated officer should be sufficient, and for the nominated officer to receive the matter at the earliest practicable opportunity.
- 7.30** The nominated officer will need to think very carefully about whether or not he wishes to continue to do business with the suspected customer. Relevant considerations should be the potential commission of criminal offences under POCA or the Terrorism Act, as well as potential damage to reputation and other commercial factors.
- 7.31** 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. If patterns of gambling lead to a steadily increasing level of suspicion of money laundering, or even to actual knowledge of money laundering, operators will no doubt seriously consider whether they wish to allow the customer to continue using their gaming facilities. Operators are of course free to terminate their business relationships if they wish, and provided this is handled sensitively there will be no risk of ‘tipping off’. However, given that the nominated

officers will have previously reported the customer to SOCA they should liaise with the agency about the best approach to turning the customer away.

- 7.32** How customers suspected of money laundering will be dealt with is an important area of risk management for all operators. Casinos should deal with the issue in their policies and procedures under the Regulations and, as all gambling operators are at risk of committing the principal offences, it is advisable for operators to consider these issues carefully before they arise in practice.
- 7.33** Although one transaction may be suspicious and be reported as such, there may be less concern that all of an individual's future transactions will be suspicious. In these circumstances, each transaction should be considered on a case-by-case basis and reports made accordingly. Where subsequent reports are also made after actual or suspected money laundering has taken place or appears to have taken place, the nominated officer is encouraged to keep records about why reporting was delayed, and about why appropriate consent was not requested before the suspected money laundering took place.

Applying for appropriate consent

- 7.34** When consent is needed reports should be faxed to the SOCA UKFIU Consent Desk (see SOCA website www.soca.gov.uk) or, where SAR Online is used, by checking the box requesting consent. The Consent Desk will apply the Association of Chief Police Officers (ACPO) agreed consent criteria to each request for consent, carry out the necessary internal enquiries, and will contact the appropriate law enforcement agency, where necessary, for a consent recommendation. Once SOCA's decision has been reached, the disclosing operator will be informed of the decision by telephone, and be given a consent number, which should be recorded. A formal consent letter from SOCA will follow.
- 7.35** As indicated, in the event that SOCA does not refuse consent within seven working days (the notice period) following the working day after the report is made, the operator may continue to do business with the customer. However, if consent is refused within that period, SOCA can interrupt business for a further 31 calendar days (the moratorium period) from the day consent is refused.
- 7.36** All consent requests are dealt with by SOCA on a case-by-case basis and while it may take the maximum of seven working days to deal with a consent request, in practice turnaround time for most SARs is about three days.²⁴ Nominated officers should take this into account when deciding whether it is practical and reasonable to request consent prior to the transaction rather than making a report after the transaction or activity.

Failing to report

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

After a report has been made

- 7.38** Depending on the circumstances, an operator being served with a court order in relation to a customer may have cause for suspicion, or reasonable grounds for suspicion, in relation to that customer. In such an event, operators should review the information it holds about

²⁴ SOCA Annual Report 2009/10.

that customer, in order to determine whether or not such grounds exist, and if necessary make a report to SOCA.

7.39 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 disclosure. This contact may also include seeking supplementary information or documentation from the reporting operator and from other sources by way of a court order. The investigating officer will therefore work closely with the nominated officer who will usually receive direct feedback on the stage reached in the investigation. There may, however, be cases when the nominated officer cannot be informed of the state of the investigation, either because of the confidential nature of the enquiry, or because the case is being considered by a court.

Tipping off, or prejudicing an investigation

7.40 Under section 333A of POCA a person commits an offence if:

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

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

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

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

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

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

- does not know or suspect that the documents are relevant to the investigation
- does not intend to conceal any facts disclosed by the documents from any appropriate officer or (in Scotland) proper person carrying out the investigation.²⁵

7.43 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. There are a number of disclosures which are permitted and that do not give rise to these offences (permitted disclosures) – see paragraphs 7.46 to 7.48.

²⁵ Section 342(6) of POCA.

- 7.44** 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.²⁶ Reasonable enquiries of a customer, conducted in a tactful manner, regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity is prudent practice, forms an integral part of CDD measures and should not give rise to tipping off.
- 7.45** Where a confiscation investigation, a civil recovery investigation, a detained cash investigation or a money laundering investigation is being, or is about to be, conducted, it is a criminal offence for anyone to disclose this fact if that disclosure is likely to prejudice the investigation. It is also a criminal offence to falsify, conceal, destroy or otherwise dispose of documents which are relevant to the investigation (or to cause or permit these offences). It is, however, a defence if the person does not know or suspect that disclosure is likely to prejudice the investigation, or if the disclosure is permitted under POCA or the Terrorism Act (see paragraphs 7.46 to 7.48).
- 7.46** An offence is not committed if the disclosure is made to the relevant supervisory authority (the Commission) for the purpose of:
- 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.²⁷
- 7.47** 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.²⁸
- 7.48** A person does not commit an offence under POCA if the person does not know or suspect that the disclosure is likely to prejudice:
- any investigation that might be conducted following a disclosure; or
 - an investigation into allegations that an offence under Part 7 of POCA has been committed, is being contemplated or is being carried out.²⁹
- 7.49** The fact that a transaction is notified to SOCA before the event, and SOCA does not refuse consent within seven working days following the day after disclosure is made, or a restraint order is not obtained within the moratorium period, does not alter the position so far as 'tipping off' is concerned.
- 7.50** This means that an operator:
- cannot, at the time, tell a customer that a transaction is being delayed because a report is awaiting consent from SOCA;
 - cannot, later, tell a customer that a transaction or activity was delayed because a report had been made under POCA or the Terrorism Act, unless law enforcement or SOCA agrees, or a court order is obtained permitting disclosure; and
 - cannot tell the customer that law enforcement is conducting an investigation.
- 7.51** 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*

²⁶ Section 342(3) of POCA.

²⁷ Section 333D of POCA.

²⁸ Section 333B of POCA.

²⁹ Section 333D of POCA.

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 judgements is available at www.soca.gov.uk/about-soca/library/cat_view/84-csar.

- 7.52** The existence of a SAR cannot be revealed to any customer of the casino at any time, whether or not consent has been requested. However, there is nothing in POCA which prevents operators from making normal enquiries about customer transactions in order to help remove any concerns about the transaction and enable the operator to decide whether to proceed with the transaction. These enquiries will only constitute tipping off if the operator discloses that a SAR has been made to SOCA or a nominated officer, or that a money laundering investigation is being carried out or is being contemplated.
- 7.53** The combined effect of these two offences is that one or other of them can be committed before or after a disclosure has been made.
- 7.54** 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.
- 7.55** There is also a specific offence of failure to disclose terrorist financing which was added to the Terrorism Act through the Anti Terrorism Crime and Security Act 2001. This offence is limited to the regulated sector, which includes casinos. The offence can be committed if a person forms knowledge or suspicion of terrorist financing or reasonable grounds for suspecting terrorist financing, during the course of working for a casino, but does not make a report. Guidance issued by the Commission and approved by Treasury must be taken into consideration by any court considering whether this offence has been committed.

Annex A – Glossary of terms

AML	Anti-money laundering.
Business relationship	A business, professional or commercial relationship between a casino operator and a customer, which is expected to have an element of duration.
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.
ML	Money laundering.
Money laundering	The process by which criminal or 'dirty' money is legitimised or made 'clean', including any action taken to conceal, arrange, use or possess the proceeds of any criminal conduct. Defined in section 340 of POCA.
Non-remote casinos	Casinos licensed to operate commercial casino premises.
Operators	Firms holding an operator's licence issued by the Commission.
PFL	Personal functional licence.
POCA	The Proceeds of Crime Act 2002, which is intended to reduce money laundering and the profitability of organised crime through the use of tools such as asset recovery.
PML	Personal management licence.
Proceeds of crime	Property from which a person benefits directly or indirectly, by being party to criminal activity, for example, stolen money, money from drug dealing or property stolen in a burglary or robbery.
Remote casinos	Casinos licensed to offer casino games by means of remote communication.
SAR	A suspicious activity report - the means by which suspicious activity relating to possible money laundering or the financing of terrorism is reported to SOCA under POCA.
SOCA	The Serious Organised Crime Agency, which was established by the Serious Organised Crime and Police Act 2005 and came into being on 1 April 2006. SOCA is an intelligence-led agency with law enforcement powers and the responsibility to reduce the harm caused to people and communities by serious organised crime). SOCA is the organisation to which suspicious activity is reported.
Supervisory authorities	Supervisory authorities, which are listed in regulation 23 of the Regulations. The Commission is the supervisory authority for casinos.
The Commission	The Gambling Commission.

The Regulations	The Money Laundering Regulations 2007.
The Terrorism Act	The Terrorism Act 2000.
UKFIU	The United Kingdom Financial Intelligence Unit, which is the unit within SOCA that operates the disclosure regime for money laundering.

Gambling Commission December 2011

Keeping gambling fair and safe for all

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

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

Gambling Commission
Victoria Square House
Victoria Square
Birmingham B2 4BP

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

GUI 11/04