Commission of Inquiry into Money Laundering in British Columbia:

Known Play

British Columbia Lottery Corporation

April 30, 2021

Building a better working world

Building a better working world

Mr. K. Michael Stephens
Hunter Litigation Chambers
personal information

April 30, 2021

Commission of Inquiry into Money Laundering in British Columbia: Known Play

Dear Mr. Stephens,

Attached please find my report for your attention. It may not be used or distributed for any other purpose without my prior consent in writing.

Any portion of this report should be read and used in the context of the entire question to which it relates and in the context of the entire report and should not be used or relied upon in isolation.

I reserve the right to supplement or amend my report upon the receipt of additional information.

Sincerely,

Bob Boyle, CPA, CAMS
Ernst & Young LLP United States
Senior Manager, Forensic & Integrity Services

Building a better working world

Table of Contents

Building a better working world

1.0 Background and purpose of report

1.1 In May 2019, the British Columbia Premier announced the establishment of a Commission of Inquiry into Money Laundering in British Columbia ("the Cullen Commission"). The British Columbia Lottery Corporation ("BCLC") was granted Participant Standing by the Cullen Commission with respect to the gaming and horse racing sector. BCLC has the opportunity to participate in accordance with the Cullen Commission's rules of practice and procedure including to address issues arising from the First and Second German Reports[1] to the extent those reports make recommendations that affect BCLC's interests and/or touch upon BCLC's role with respect to prevention of money laundering in the gaming and horse racing sector.

1.2 Ernst & Young LLP ("EY" or "I") was engaged by Hunter Litigation Chambers ("HLC" or "Counsel") on behalf of its client BCLC in relation to the Cullen Commission to collect, collate, and provide information on historical anti-money laundering ("AML") processes or controls for Land-Based Casinos or AML oversight bodies in other Gaming Jurisdictions globally.[2]

1.3 This report ("Report") was prepared pursuant to EY's engagement agreement dated October 10, 2017 and statement of work dated February 17, 2021 solely for the purpose described above (the "Purpose").

2.0 Instructions and opinions sought

2.1 My formal instructions are set out in a letter from Counsel dated April 28, 2021 which is attached to this Report as Exhibit 1. The nature of the opinion I have been asked to provide is as follows:

Buy-in refusal practices

Question 1: Please describe the concept of 100% known play as utilized in land-based casinos in the Gaming Jurisdictions.

Question 2: Please describe the concept of 100% carded play as utilized in land-based casinos in the Gaming Jurisdictions.

Question 3: Please describe the concept of 100% cashless play as utilized in land-based casinos in the Gaming Jurisdictions.

Practices in Gaming Jurisdictions

Question 4: Please describe the casino operators that you are aware of in the Gaming Jurisdictions regarding how the following are used:

(a) 100% known play; and

(b) 100% known play with 100% carded play.

[1] Dirty Money: An Independent Review of Money Laundering in Lower Mainland Casinos Conducted for the Attorney General of British Columbia, Peter M. German, Q.C., March 31, 2018 ("First German Report"); Dirty Money – Part 2: Turning the Tide – An Independent Review of Money Laundering in B.C. Real Estate, Luxury Vehicle Sales & Horse Racing, Peter M. German, Q.C., March 31, 2019 ("Second German Report")

[2] For the purposes of this Report, Global Jurisdictions include Canada (excluding British Columbia), the United States, the European Union (including the United Kingdom), Macau, Australia, or New Zealand. See Definitions set on in Appendix C to this Report.

Regulatory Practices

Question 5: In answering question four, please advise if you are aware whether:

(a) regulators have indicated they will require 100% known play and/or 100% carded play in the Gaming Jurisdictions;

(b) casino operators in Canadian jurisdictions have indicated if they will adapt changes toward 100% known play or 100% carded play in anticipation of regulatory changes from FINTRAC taking effect in June 2021 (setting a threshold of CAD 3,000 for identification and receipting)

Effects of 100% known, carded, and/or cashless play

Question 6: Please summarize the benefits and detriments (if any) of 100% known play, 100% carded play and/or 100% cashless play in the Gaming Jurisdictions. To your knowledge, please describe if casino operators implemented 100% known play, 100% carded play and/or 100% cashless play following regulations in the Gaming Jurisdictions.

In answering the question, please include practices in Gaming Jurisdictions, including those in North America where high limit play is available.

2.2 I was instructed by Counsel that the Time Period of relevance for the purposes of this Report is January 1, 2014 to December 31, 2020.

2.3 I was further instructed by Counsel to assume for the purposes of my opinion that the facts set out in the Statement of Assumed Facts (attached as Appendix "A" to Exhibit 1) are true. Information indicating assumptions contrary to those or any other assumptions set out elsewhere in this Report will require a review of the opinions contained in this Report.

3.0 Personal information and qualifications

3.1 The professional work to prepare this Report was performed by me, Bob Boyle, CPA, CAMS, of EY, 5 Times Square, New York, NY 10036, United States of America, with the assistance of other EY professionals under my supervision.

3.2 I am a Certified Public Accountant (State of New York) and a Certified Anti-Money Laundering Specialist.

3.3 My area of expertise is financial crime regulations affecting financial institutions globally, including the gaming and casino industry, concentrating on AML and economic sanctions matters.

3.4 I have extensive experience with AML and economic sanctions engagements including conducting risk assessments, program reviews for both compliance and internal audit functions, implementation of policies and procedures, transaction remediation reviews, enhanced due diligence, training of employees, management and board of directors and providing independent quality assurance for AML matters pertaining to regulatory investigations and examinations for global regulatory bodies for the gaming industry.

3.5 My Statement of Qualifications is attached as Appendix A to this Report.

4.0 Scope of work

Information relied on

4.1 In preparing my Report, I relied on the following information:

a) Instruction letter from Counsel dated April 28, 2021 attached to this Report as Exhibit 1 and Statement of Assumed Facts attached as Appendix "A" to Exhibit 1;

b) Documents set out in Appendix B to this Report; and

c) Discussions with Counsel to obtain a background understanding of the opinions sought.

4.2 In responding to each of the questions below, I also relied on publicly available documents published by regulators or on industry body guidance,[3] as well as my industry experience in the Gaming Jurisdictions.[4]

4.3 The regulators for each Gaming Jurisdiction are as follows:

Canada – Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC")[5]

United States – Financial Crimes Enforcement Network ("FinCEN"); and Bank Secrecy Act ("BSA")

European Union –EU Third through Fifth Anti-Money Laundering Directives

United Kingdom – The Gambling Commission

Macau – Direccao de Inspeccao e Coordenacao de Jogos ("DICJ")

Australia – Australian Transaction Reports and Analysis Centre ("AUSTRAC")

New Zealand – Department of Internal Affairs ("DIA")

4.4 Regulations referred to in this report are limited to those regulations listed above.

4.5 The industry bodies for each Gaming Jurisdiction are as follows:

United States – American Gaming Association ("AGA")

Global – Financial Action Task Force ("FATF")[6]

4.6 Capitalized terms and abbreviations not otherwise defined in this Report are defined in Appendix C.

Scope limitation

4.7 In preparing this Report, I have been provided with and have relied upon the information described above (collectively, "the Information"). I have not audited or otherwise attempted to verify the accuracy and completeness of the Information and, accordingly, I express no opinion or other form of assurance in respect of the Information. I assume no responsibility for information furnished by others and such information is believed to be reliable.

---

[3] The significance between regulatory and industry body guidance as used in this Report is that a regulator can impose mandatory rules or penalties on casino operators that do not follow the regulations. An industry body cannot impose mandatory rules or penalties but is often regarded as providing leading practice for AML processes or controls in Land-Based Casino operators.

[4] Although I have experience as it pertains to casino operators in Canada, the United States, the European Union, and Macau, I do not have direct experience as it pertains to casino operators in the United Kingdom, Australia or New Zealand.

[5] Although the Gaming Jurisdictions as defined do not include British Columbia, regulation references pertaining to FINTRAC are applicable to all Canadian provinces and territories.

[6] Global includes Canada, United States, and various countries in the EU. There is no industry body specific or unique to Canada.

4.8 This Report is based on my analysis of the Information available to the date of this Report. I reserve the right (but will not be obligated) to revise this Report in light of any relevant information that comes to my attention after the date of issuance.

4.9 None of this Report will constitute any legal opinion or legal advice. None of this Report will constitute any tax opinion or tax advice.

4.10 None of this Report will constitute commentary or opinions as to whether BCLC's AML procedures are sufficient or appropriate.

4.11 None of this Report will constitute an assessment of BCLC's compliance with the Federal Proceeds of Crime (Money Laundering) and Terrorist Financing Act or against applicable reporting requirements outlined by FINTRAC.

5.0 Opinions

5.1 I have identified the applicable regulations, industry body guidance and operator practices in arriving at my opinion in answer to each of these questions.

5.2 The questions below refer to specific Canadian dollar amounts. As each gaming jurisdiction would have threshold amounts based on its local currency, I answered the questions by identifying processes or procedures with defined amounts in the applicable local currency. I did not convert threshold amounts to Canadian dollars.

General

Question 1: Please describe the concept of 100% known play as utilized in land-based casinos in the Gaming Jurisdictions.

5.3 It is my understanding that 100% known play, as utilized in Land-Based Casinos in the Gaming Jurisdictions, refers to the concept whereby identification, whether stipulated by jurisdiction-specific regulations or individual casino operator policies, is a requirement for entering the casino. For the purposes of CDD, identification of a patron means being told or coming to know of the patron's identifying details, such as their name and address, as well as documentation supporting this information such as a driver license or passport as established in the UK Gambling Commission Guidance in Exhibit 2. For a casino to be operating a 100% known play property, identification must be obtained from individuals prior to entering the casino gaming floor, regardless of whether the individual expects to game.

5.4 Verification of a patron's identification is not required in all cases and is often applied through risk-based criteria. Verification is the process of verifying through documents or information which have been obtained from a reliable source, independent of the person whose identity is being verified. The UK Gambling Commission Guidance in Exhibit 2 states that documents issued or made available by an official body are to be regarded as being independent of a person even if they are provided or made available to the casino operator by, or on behalf of, that person. Based on my experience, identity documentation can also be checked for legitimacy through vendor systems at different locations in the casino such as the cage or pit area for table games or checked against the information that was provided by the patron when they were initially identified by the casino prior to entering the gaming floor. The types of identification required may vary depending on the country or casino policy.

5.5 100% known play means that all individuals who enter the casino have been positively identified, and there are no anonymous patrons, regardless of their level of play, funds spent, or games played. This would include patrons that transact in low dollar amounts or solely in

cash, two instances in which identification may not typically be requested by casino operators that do not use 100% known play.

Question 2: Please describe the concept of 100% carded play as utilized in land-based casinos in the Gaming Jurisdictions.

5.6 It is my understanding that the concept of 100% carded play is not utilized in Land-Based Casinos in the Gaming Jurisdictions. However, the concept of carded play in certain areas within the casino (such as table games or VIP, private or high-limit rooms) is utilized in Land-Based Casinos in the Gaming Jurisdictions.

5.7 The concept of carded play, as utilized in Land-Based Casino operators, refers to patrons gaming in the casino being registered for a player's card (or equivalent). Carded play is triggered by gaming activity, and not by entry to the casino. A player's card often requires the patron's full name, date of birth, address, and supplemental contact information, but it does not have the capabilities of a wagering account or a PGF account, nor does it constitute casino credit.[7] Player's card benefits are typically focused on experience benefits for the patrons such as discounts, complementary items or game play, etc. Patrons present the player's card prior to gaming by either inserting the card at electronic games or providing their card to the table games dealer in order to track their game play.

Question 3: Please describe the concept of 100% cashless play as utilized in land-based casinos in the Gaming Jurisdictions.

5.8 It is my understanding that the concept of 100% cashless play is not utilized in Land-Based Casinos in the Gaming Jurisdictions. However, the concept of cashless play in certain areas of the casino is utilized in Land-Based Casinos in the Gaming Jurisdictions.

5.9 Cashless play, as utilized in Land-Based Casino operators, describes the concept whereby a patron uses casino credit, PGF account or other type of wagering account to engage in transaction activity with a casino operator. Instead of using cash for the buy-in, cash out or account deposit or withdrawal, the patron utilizes their casino credit, PGF account or other type of wagering account to transact. Cashless play often allows patrons to access funds directly from verifiable external sources such as bank or credit card accounts. Cashless play alternatives are available to facilitate play for Mass Gaming Patrons but are generally used in greater capacity as options for Premium Mass Gaming Patrons or VIPs.

Practices in Gaming Jurisdictions

Question 4: Please describe the casino operators that you are aware of in the Gaming Jurisdictions regarding how the following are used:

(a) 100% known play; and

(b) 100% known play with 100% carded play.

5.10 Based on my experience, there are instances of 100% known play among European casino operators. I have observed casino operators within EU countries, such as the Netherlands, Germany and Spain, that use 100% known play. In these instances, casino operators use

[7] Wagering accounts are casino-based accounts that allow customers to transfer, deposit and withdraw money into and out of their casino account. Funds can typically be deposited into a wagering account with cash, personal cheques, cashier's cheques, wire transfers, money orders, transfers from a debit or credit card or through an extension of credit by the licensee. Patron Gaming Fund (PGF) accounts are casino-based accounts that allow patrons to transfer money (over CAD 10,000) between their casino account and their approved Canadian bank account, eliminating the need to bring cash into the casino.

the on-entry approach as outlined in the EU Third and Fourth Anti-Money Laundering Directives (Exhibit 3 and Exhibit 4, respectively) and described below.

5.11 Included in the EU Third Anti-Money Laundering Directive in Exhibit 5 is a requirement that all patrons be identified, and their identity verified if they purchase or exchange gambling chips with a value of EUR 2,000 or more. The EU Third and Fourth Anti-Money Laundering Directives (Exhibit 3 and Exhibit 4, respectively) and the UK Gambling Commission guidance (Exhibit 2) present the option to casino operators to require identification on entry to avoid the need for extensive identification controls prior to exceeding regulatory threshold amounts at the time of gaming. Therefore, casino operators may conduct both identification and verification on entry or conduct identification on entry and defer verification until the threshold amount is triggered.

5.12 When a casino operator elects to use the on-entry approach, they must identify the patron before entry to any premises where gaming facilities are provided. Forms of acceptable identification for EU citizens include original copies of National ID cards or passports; for non-EU citizens, passports are required. Once the patron's identity is recorded, the patron may commence gaming. The casino operator must complete the processes for verification of the patron if they cross the required threshold amount. If a casino operator using the on-entry approach is unable to complete the appropriate CDD, the casino operator must not allow the patron access to the premises. For Land-Based Casino operators electing to use the on-entry approach, guests of known patrons are not allowed entry without undertaking required CDD measures.

5.13 I am also aware of, from my experience, casino operators who use known play in certain areas of the casino, such as gaming salons[8] or other types of private gaming rooms, or premium mass gaming areas. However, this would not constitute 100% known play as the identification of individuals does not apply to the entire casino. I have observed required known play processes implemented for certain areas of the casino, such as salons, by casino operators outside the EU in other Gaming Jurisdictions like the United States. For example, one casino operator that I am aware of in the United States requires each patron and any associates entering a gaming salon to provide valid identification prior to entering the salon for each visit.

5.14 In addition to requiring identification for these types of casino areas, I have also observed casino operators outside of the EU that require known play for certain casino products and services, such as casino credit and PGF accounts. In these instances, patrons are prohibited from opening accounts or conducting prescribed transactions until the patron’s identity is established and verified.

5.15 I have not observed instances and am not aware of casino operators that use 100% known play while also including a 100% carded play requirement.

5.16 In my experience, I have not observed instances in which a casino operator has a 100% carded play requirement for all gaming offerings. For carded play solely applicable to table games, a pit supervisor or other authorized casino employee will prompt patrons when they sit at the table for their player’s card, which will then be used to track the patron’s activity at

[8] Gaming salons are enclosed gaming facilities that are located anywhere on the property of a resort hotel that holds a nonrestricted gaming license, admission to which is based upon the financial criteria of the salon patron as established by the license and approved by the Board. Salons include table games (may include slot machines) and have minimum wagers for any game offered. (i.e. Minimum wagers for slot machines must not be less than $500). Refer to Chapter 463 – Licensing and Control of Gaming from the 2015 Revised Nevada Statutes (Exhibit 5).

the table. Certain Land-Based Casino operators that offer VIP, private or high-limit rooms may require patrons to have a player's card in order to game within those special rooms, but these types of controls and requirements vary by casino operator and type of gaming product offering and would not constitute 100% carded play requirements for the casino operator as a whole.

Regulatory Practices

Question 5: In answering Question 4, please advise if you are aware whether:

(a) regulators have indicated they will require 100% known play and/or 100% carded play in the Gaming Jurisdictions;

(b) casino operators in Canadian jurisdictions have indicated if they will adapt changes toward 100% known play or 100% carded play in anticipation of regulatory changes from FINTRAC taking effect in June 2021 (setting a threshold of CAD 3,000 for identification and receipting)

5.17 I am not currently aware of regulators in the Gaming Jurisdictions that have indicated they will require 100% known play and/or 100% carded play. In my answer to Question 4 above, I noted that regulations in the EU allow for 100% known play as an option, but do not require casino operators to use 100% known play.

5.18 I am not currently aware of casino operators in Canadian jurisdictions that have indicated they will adopt changes toward 100% known play or 100% carded play in anticipation of the June 2021 FINTRAC regulatory changes.

Effects of 100% known, carded, and/or cashless play

Question 6: Please summarize the benefits and detriments (if any) of 100% known play, 100% carded play and/or 100% cashless play in the Gaming Jurisdictions. To your knowledge, please describe the if casino operators implemented 100% known play, 100% carded play and/or 100% cashless play following regulations in the Gaming Jurisdictions.

In answering the question, please include practices in Gaming Jurisdictions, including those in North America where high limit play is available.

<u>Effects of known play</u>

5.19 The benefits to implementing 100% known play may include:

i) Ability to collect information required to identify patrons for regulatory purposes prior to entry, which may reduce the risk of a regulatory breach.

ii) Ability to trace patron transaction activity on the gaming floor such as buy-in, game play and cash out activity through the assistance of surveillance and casino operational department employees (such as slots, table games and cage personnel). The surveillance footage may be used to track when a particular patron entered the casino, and match that to when and what the patron presented as identification. As an illustrative example, Patron A enters the casino at 6:00PM, presents their identification at the entrance of the casino and the identification is scanned and verified. At 8:00PM, Patron A is observed by a slots floor supervisor to be engaging in bill stuffing activity[9] and is observed to not be using a player's card to track their play activity. When the

[9] Bill stuffing activity is when a patron inputs money into a slot machine and requests a cash-out voucher. The patron subsequently redeems the voucher at a kiosk. Bill stuffing could hide the source of the original funds.

slot floor supervisor reports the suspicious activity to surveillance, surveillance can then review camera footage to trace when Patron A initially entered the casino and obtain the information from their scanned identification. This information can then be presented to the appropriate compliance department for review.

iii) Ability to assist security and surveillance team in identifying and barring entry to previously barred patrons. Casino operators that do not require identification upon entrance risk barred patrons entering the casino and gaming in low-value amounts to avoid being asked for identification.

iv) Ability to identify patron relationships in order to identify potential agent play, chip passing, or chip sharing. This applies when a patron passes their chips to a known associate, such as a spouse who is not gaming, to either hold their chips for safekeeping or to cash out the chips on their behalf at the cage. If 100% of the individuals in the casino, regardless of their play activity, have been identified, it is easier to identify where chips came from, and which individuals with limited to no play activity cash out.

5.20 The detriments to a casino operator of adopting 100% known play may include:

i) Decline in foot traffic for mass gaming patrons who do not wish to present their identification if they are entering a casino to observe or game casually. Patrons with higher volume of gaming activity or designated as premium mass or VIP generally have an understanding or expectation that they will be required to present identification and information; however, patrons who come to casinos for lower volume gaming or no gaming may not be as willing to provide such information. Casino operators run the risk of experiencing a decline in casual gaming volumes, or a general decline in patron satisfaction and experience if patrons feel that requiring identification is too much of an inconvenience to partake in casino products and services offered.

ii) Increase in costs to collect information, monitor, and track 100% of individuals entering the casino including wages, and data storage costs.

iii) Increase in risks related to retention of higher volumes of personally identifiable information due to cyber attacks or other data leaks.

5.21 To my knowledge, some casino operators based in the UK have implemented 100% known play after the UK Gambling Commission required casino operators to either apply CDD measures upon entry or at any transaction that amounts to EUR 2,000 or more. To facilitate this requirement, some casino operators elected to require identification and verification on entry. This requirement is described in my response to Question 4 above.

5.22 Additionally, I have observed certain gaming salons and other private or semi-private gaming rooms typically reserved for patrons who engage in higher limit play (premium mass and VIP patrons) in Canada, the EU and the United States where casino operators have requirements for Known Play. However, it should be noted that these appear to be casino operator policy and are risk-based or operational decisions as opposed to regulatory or legislative requirements. Similar to the UK, many regulatory guidance publications, such as the EU Fourth Anti-Money Laundering Directive (Exhibit 4), require CDD for transactions of EUR 2,000 or more. They also provide the option to require identification at the point of entry, provided that the patron can then be linked to transactions they conduct.

Effects of 100% carded play

5.23 The benefits to implementing 100% carded play may include:

i) Ability to identify and track the patrons who are gaming in the casino. This includes insight into a patron's gaming patterns and activity, and the ability to identify significant deviations in their normal playing history or potential suspicious activities. Carded play does not identify all individuals in the casino.

ii) Ability to perform analytics on betting patterns, buy-in and cash out velocity and changes in behavior in gaming activity to identify anomalies.

iii) Ability to determine a patron's total gaming trip timeline, which can be used to determine whether the patron has left the casino with outstanding chips (i.e. chip walking) and whether they have returned with them over the course of a given gaming trip.

iv) Ability to examine a patron's lifetime wins and losses to aid in assessing a patron's risk level; having patron records and insight into patterns of play assists casinos with understanding expected patron volumes, types of gaming, and if applicable, wagering account activity to assess the risk of the patron as it pertains to money laundering or other financial crimes.

v) Ability to compare additional information on the patron outside of their gaming activity, such as demographic and occupation information, to identify high-risk occupations or occupations that normally do not generate income, or to compare total betting activity against standard salary and source of wealth.

vi) Ability to provide their patrons with targeted promotions and advertisements based on their level of play and preferred game(s). For example: Patrons who solely game using slot machines may be sent special jackpot bonuses or credits to game; patrons who prefer poker or other table games can be invited to participate in tournaments, or provided free food, beverage and accommodations to stay at the casino resort in order to play.

5.24 The detriments to a casino operator of adopting 100% carded play may include:

i) Decline in low-dollar value patrons who do not wish to present their identification if they are gaming casually. Patrons with higher volume of gaming activity generally have an understanding or expectation that they will be required to present identification and information; however, patrons who come to casinos for lower volume gaming may not be as willing to provide such information if their intention is to solely spend a few hours or days gaming. Casino operators run the risk of experiencing a decline in casual gaming volumes, or a general decline in patron satisfaction if patrons feel that requiring identification is too much of an inconvenience.

ii) Increase in costs associated with updating slot machines, table games, etc. to include access points that require carded play.

iii) Increase in costs to collect information, monitor and track 100% of patrons including wages, and data storage costs.

iv) Increase in risks related to retention of higher volumes of personally identifiable information due to cyber attacks or other data leaks.

5.25 In my experience, I have not observed any Land-Based Casino operators that require 100% carded play after introduction of regulations in the Gaming Jurisdictions. In the UK, I am aware of some Land-Based Casino operators that require all patrons to present their identification as well as sign up for a membership prior to entry; however, I am unaware whether institutions such as this require all patrons to also present their cards at the table to track their game play, or if the slot machines require the insertion of the membership card to function.

5.26 In my experience, as it pertains to high limit play, such as gaming salons or other types of private gaming rooms or premium mass gaming areas, casino operators are tracking the patron's activity either through formal carded play, separately through a table games or slot management system or through active surveillance. Typically, these areas are exclusive to patrons who hold higher tier player's cards, but in my experience, I am not aware where 100% of high limit play required a player's card to game in these locations.

Effects of 100% cashless play

5.27 The benefits to implementing 100% cashless play may include:

i) Ability to reduce risk for both the patron and the casino operator regarding the movement of larger amounts of cash.

ii) Ability to divert resources from cash monitoring to other monitoring parameters, including the reduction of regulatory filings (i.e. CTR's) in markets that have cash threshold reporting requirements.

iii) Ability to provide the patron with the ease of accessing funds through credit, PGF or other types of wagering accounts.

iv) Ability to track more aspects of the patron transaction lifecycle, such as deposits, game play and withdrawals.

5.28 The detriments to a casino operator of adopting 100% cashless play may include:

i) Decline in Mass Gaming patrons where cash may be a more common option for transacting. The cash option from the patron to buy-in or cash out which could have a negative affect on patron experience and decrease overall foot traffic as it pertains to Mass Gaming patrons.

ii) Increase in costs associated with the investment in technology and the transition to 100% cashless casino management systems. There may also be costs associated to updating slot machines and various table games to facilitate 100% cashless play options.

iii) Increase in costs associated to updating compliance programs to effectively collect, monitor and track 100% cashless play.

iv) Increase in risks related to retention of higher volumes of personally identifiable information due to cyber attacks or other data leaks.

5.29 In my experience, I have not observed any Land-Based Casino operators that require 100% cashless play after introduction of regulations in the Gaming Jurisdictions.

6.0 Restrictions and limitations

6.1 This Report is confidential and may not be reproduced or distributed without EY's prior written consent, except to the extent necessary in connection with the Purpose of our engagement, as set out in the first section of this Report. In the context of the Purpose described above, this Report may be distributed to the Commission and counsel, insofar as it relates to the Purpose stated herein.

6.2 Any portion of this report should be read and used in the context of the entire question to which it relates and in the context of the entire Report and should not be used or relied upon in isolation, as this could be misleading.

6.3 EY or I will not assume any responsibility or liability for losses incurred by any third parties as the result of their reliance on any part of this Report or on verbal advice that may be provided by me, EY or its employees in the course of discussions with them relating to this matter.

6.4 My awareness and understanding of operator practices, regulations, and industry body guidance is current as of the date of this Report. I reserve the right (but will not be obligated) to revise this Report in light of any relevant information that comes to my attention after the date of issuance.

7.0 Certification by Bob Boyle

7.1 I am the person primarily responsible for the opinions contained in this Report.

7.2 I am aware of my duty under Rule 11-2(1) of the British Columbia Supreme Court Civil Rules to assist the Court and not be an advocate for any party. I have prepared this Report in conformity with this duty. If I am called to give oral or written testimony, I will give that testimony in conformity with this duty.

Sincerely,

Bob Boyle, CPA, CAMS
Ernst & Young LLP United States
Senior Manager, Forensic & Integrity Services

Building a better working world

Appendix A – Statement of qualifications

Bob Boyle, CPA, CAMS

Senior Manager, Forensic & Integrity Services
Ernst & Young LLP, New York
[redacted] | [redacted]

Profile

Bob is a senior manager in EY's Forensic & Integrity Services practice in New York where he has led several financial crimes compliance projects for gaming and casino clients. He has over twelve years of experience providing professional advice to clients in connection with investigative and compliance matters. Specifically, Bob focuses on regulations affecting financial institutions globally, including the gaming and casino industry, concentrating on Anti-Money Laundering (AML) and economic sanctions matters.

He has extensive experience with AML and economic sanctions engagements such as conducting risk assessments, program reviews for both compliance and internal audit functions, implementation of policies and procedures, transaction remediation reviews, enhanced due diligence, training of employees, management and board of directors and providing independent quality assurance for AML matters pertaining to regulatory investigations and examinations for global regulatory bodies for the gaming industry.

Bob is a Certified Public Accountant in the State of New York and is also a Certified Anti-Money Laundering Specialist.

Selected professional experience

Bob has experience across multiple gaming jurisdictions in having led numerous compliance engagements with casinos and other companies in the gaming and sports wagering industry:

- Performed AML and sanctions program assessments and process analysis within multiple Canadian provinces for crown corporations in charge of providing government sanctioned lottery games and managing casinos and bingo halls as well as reviews specific to service providers and individual properties. Led the review of policies and procedures, performed walkthroughs and interviews at key casino service provider locations and performed detailed sample-based testing for reports and filings sent to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

- Managed an engagement with a US gaming industry trade association to conduct authoritative research on the gaming sector's level of commitment to combating money laundering and terrorist financing. The trade association's overall objective was to produce a report in advance of

a Financial Action Task Force's ("FATF's") mutual evaluation of the United States' AML regulatory framework

- Performed an independent AML compliance program assessment for a single-property riverboat casino in the United States. The review included an evaluation of the corporate AML program in accordance with the requirements outlined by Title 31 regulation and the Bank Secrecy Act ("BSA"). Additionally, Bob led a team to develop and present enhanced AML training focusing on specific departments where employees are patron facing. This include tailoring training specific to cage and credit operations, table games, poker, surveillance and security, slot operations and marketing. EY delivered 25 separate training presentations over the course of a week schedule to accommodate the shifts of approximately 600 casino employees

- Managed an independent AML and Sanctions compliance program assessment for a large gaming corporation with operations at 35 properties throughout the United States. The review included an evaluation of the corporate AML and Sanctions programs in accordance with the requirements outlined by Title 31 and OFAC as well as a sample of individual property assessments. EY developed and executed a tailored review methodology including policy and procedure reviews, interviews with key corporate compliance and property personnel, walkthroughs at sampled casino property locations and detailed assessments of investigations, regulatory filings and applicable patron documentation

- Performed an assessment of a large Las Vegas strip casino's AML compliance program against applicable regulatory requirements outlined by the BSA and Title 31. EY performed the review at the direction of the casino's internal audit group. The AML review covered policies and procedures, assessment of risks related to money laundering and terrorist financing and regulatory reporting program, training program, and record retention policies and procedures to test their effectiveness

- Led a team in developing an AML and sanctions risk assessment methodology for a leading racetrack and gaming entertainment establishment in Canada. Bob led interviews with key compliance personnel and staff to address key AML and sanctions risk categories. He developed a detailed report and risk heat map diagram to establish where key high-risk areas were identified

- Led a global AML program assessment for a multi-jurisdictional casino operator with properties in Macau, Manila and the European Union. The assessment consisted of working with local EY teams to address local financial crime compliance regulations in addition to global industry practices. Bob and his global team developed a report covering all three applicable jurisdictions as well as global risk and program considerations

Education and professional designations

- Certified Anti-Money Laundering Specialist, 2011

- Certified Public Accountant, 2009

- Bachelor of Science, New York University, 2008

Appendix B – Documents relied upon

In preparing my Report, I relied on the following information. I have accepted information provided by external sources as being accurate and reliable.

1. Instruction letter from Hunter Litigation Chambers and Appendix “A” thereto Statement of Assumed Facts

2. UK Gambling Commission Guidance Fourth Edition March 2018 https://pdf4pro.com/view/the-prevention-of-money-laundering-and-18a0ec.html

3. EU Third Anti-Money Laundering Directive (2005/60/EC) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005L0060

4. EU Fourth Anti-Money Laundering Directive (2015/849) https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32015L0849

5. 2015 Revised Nevada Statutes Chapter 463 – Licensing and Control of Gaming https://law.justia.com/codes/nevada/2015/chapter-463/

Appendix C – Definitions and abbreviations

The following definitions and abbreviations are used throughout the Report:

Defined terms provided by counsel

Gaming Jurisdictions – Canada (excluding British Columbia), United States, European Union ("EU") including the United Kingdom ("UK"), Macau, Australia, or New Zealand

Land-Based Casinos – exclude online gaming

Time Period – January 1, 2014 to December 31, 2020

Additional definitions and abbreviations

AGA – American Gaming Association, gaming industry body in the United States

AML – Anti-Money Laundering

AUD – Australian dollar currency (as of April 29, 2021 AUD 1 = CAD 0.9552 per the Bank of Canada)

AUSTRAC – Australian Transaction Reports and Analysis Centre, regulatory body of Australia

BSA – Bank Secrecy Act, one of the regulatory bodies of the United States (see also *FinCEN*)

Buy-In Amount ("Buy-In") – the amount of cash, chips, or cheques that a Patron uses to initiate gaming activity.

CAD – Canadian dollar currency

CDD – Customer Due Diligence

CTR – Currency Transaction Report

DIA – Department of Internal Affairs, regulatory body of New Zealand

DICJ – Direccao de Inspeccao e Coordenacao de Jogos, regulatory body for Macau

EFT – Electronic Funds Transfer

EU Third through Fifth Anti-Money Laundering Directives – one of the regulatory bodies of the UK (see also *The Gambling Commission*)

EUR – EU currency (as of April 29, 2021, EU 1 = CAD 1.4897 per the Bank of Canada)

FATF – Financial Action Task Force, global gaming industry body

FinCEN – Financial Crimes Enforcement Network, one of the regulatory bodies of the United States (see also *BSA*)

FINTRAC – Financial Transactions and Reports Analysis Centre of Canada, regulatory body for Canada

The Gambling Commission – one of the regulatory bodies of the UK (see also *EU Third through Fifth Anti-Money Laundering Directives*)

Gaming salons – enclosed gaming facilities that are located anywhere on the property of a resort hotel that holds a nonrestricted gaming license, admission to which is based upon the financial criteria of the salon patron. Gaming salons include table games (may include slot machines) and have minimum wagers for any game offered.

GST – Goods and Services Tax

Junket – an arrangement between a casino and a junket tour operator to facilitate a period of gambling by one, or a group, of patrons at a casino. In return for bringing the patrons to the casino, the casino pays the junket tour operator a commission based on the collective gambling activity of patrons on the junket.

KYC – Know Your Customer

Mass Gaming Patrons – Includes the population of patrons who game and transact with a casino operator during the normal course of business and for no defined threshold value

ML/TF – Money Laundering or Terrorist Financing

MOP – Macau pataca currency (as of April 29, 2021, MOP 1 = CAD 0.1537 per the Bank of Canada Hong Kong Dollar rate divided by 1.03 as MOP is not administered by a central bank and is pegged to HKD at rate of 1.03)

MSB – Money Service Business

NIL – Negotiable Instrument Log

NZD – New Zealand dollar currency (as of April 29, 2021 NZD 1 = CAD 0.8900 per the Bank of Canada)

OFAC – The Office of Foreign Assets Control is a financial intelligence and enforcement agency of the U.S. Treasury Department

Patron – an individual who is conducting transaction activity at a casino

PEP – politically exposed person

PGF – Patron Gaming Fund, used in British Columbia casinos. A PGF account is an account opened at the casino for a patron, where the patron can deposit funds for the purpose of gaming. The account can only be opened with a minimum amount of CAD 10,000 of sourced funds in the form of a bank draft. The PGF Patron can withdraw funds from their PGF account at any point

Premium Mass Gaming Patrons – Population of patrons who interact with the casino at specific threshold amounts and are thus tiered above Mass Gaming Patrons. Premium Mass Gaming Patrons may have access to private or semi-private gaming spaces, access to more exclusive benefits as part of the casino's player's card rewards program and may receive personalized interactions with casino marketing and host staff to enhance the patron's experience.

Real ID – Real IDs are a type of state-issued identification card that is an acceptable form of a government-issued photo identification. In USA, all state issued IDs that are compliant with the Real ID Act are sufficient for BSA reporting purposes, even those that contain the disclaimer, 'Not for Federal Identification'

SAR – Suspicious Activity Report, also known outside the United States as Suspicious Transaction Report ("STR")

SOF – Source of Funds

Sourced cash conditions – Patrons must provide evidence of the source of funds, whether through receipt or other supporting documentation, before performing a buy-in with cash. This is a conditional requirement for utilizing cash as an option to transact at the casino.

Sourced chip conditions - Patrons must state where they obtained chips when performing a transaction with the casino and this must be verifiable by the casino through game play or other transaction activity involving chips before the transaction is executed.

SOW – Source of Wealth

STR – Suspicious Transaction Report, also known in the United States as Suspicious Activity Report ("SAR")

TITO – ticket in/ticket out redemptions

TTO – This Trip Only

TTR – Threshold Transaction Report

UFT – Unusual Financial Transaction

USD – United States dollar currency (as of April 29, 2021, USD 1 = CAD 1.2292 per the Bank of Canada)

VIP – Very Important Person. A VIP is generally the highest tier that a patron has with a casino operator and typically benefit from exclusive offers, gaming opportunities (including private gaming), personalized treatment, accommodations and other rewards and discounts. VIPs typically have dedicated casino personnel to assist them throughout their gaming and transaction experience with the casino and generally use a wagering account to conduct transactions.

Building a better working world

Exhibits

Exhibit Ref.	Source Document
Exhibit 1	Instruction letter from Hunter Litigation Chambers
Exhibit 2	UK Gambling Commission Guidance Fourth Edition March 2018 https://pdf4pro.com/view/the-prevention-of-money-laundering-and-18a0ec.html
Exhibit 3	EU Third Anti-Money Laundering Directive (2005/60/EC) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005L0060
Exhibit 4	EU Fourth Anti-Money Laundering Directive (2015/849) https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32015L0849
Exhibit 5	Excerpts from 2015 Nevada Revised Statutes Chapter 463 – Licensing and Control of Gaming https://law.justia.com/codes/nevada/2015/chapter-463/

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization and/or one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

ey.com/ca

Exhibit 1

Hunter Litigation Chambers

KAARDAL/SMART/STEPHENS/OULTON

April 28, 2021

File no: 1027.107

BY EMAIL
PRIVILEGED AND CONFIDENTIAL

Ernst & Young LLP
personal information
[redacted]

Attention: Bob Boyle, Senior Manager, Forensic & Integrity Services

Dear Mr Boyle:

Re: Expert Witness Retainer - 100% Known Play Gaming Jurisdictions
Commission of Inquiry into Money Laundering in British Columbia –
British Columbia Lottery Corporation

As you are aware, we are counsel to the British Columbia Lottery Corporation ("BCLC") which is a participant in the above-captioned Commission of Inquiry (the "Proceeding").

This letter confirms your retainer as an expert in the Proceeding under the Statement of Work dated February 17, 2021. This letter provides you with certain additional assumptions, and describes your expected role as an expert witness.

The Proceeding and Terms of Reference

The Proceeding arises out of Terms of Reference dated May 15, 2019 entitled the "Commission of Inquiry into Money Laundering in British Columbia Order". The Terms of Reference are to conduct hearings and make findings of fact respecting money laundering in British Columbia, including (among other things), the evolution and methods of money laundering in the gaming sector; and the acts or omissions of regulatory authorities or individuals with powers, duties or functions in respect of (among other things) the gaming sector (paragraph 4(1)). The Commission is empowered to, among other things, make recommendations the commission considers necessary and advisable including with respect to the gaming sector (paragraph 4(2)).

In an Interim Report dated November 2020[1], the Commission stated on p.73 that he expected to hear evidence in the Proceeding on mattes including, among other things, "whether any money

[1] Available at: https://cullencommission.ca/files/reports/CullenCommission-InterimReport.pdf

laundering vulnerabilities continue to exist in BC casinos and, if so, what additional steps can and should be taken to address those vulnerabilities."

In addition, on page 77 of the Interim Report the Commissioner stated that Other Jurisdictions were important to fulfilling the Commission's Terms of Reference:

"One of the more significant aspects of the Commission's work has been the study of anti–money laundering strategies in other jurisdictions, including the United Kingdom, Ireland, Australia, New Zealand, the United States, Germany, the Netherlands, and Switzerland. My hope is that the study of these jurisdictions will lay the foundation for recommendations about how to address money laundering in British Columbia. During the overview portion of the evidentiary hearings, I heard evidence with respect to a number of other jurisdictions – most notably, the United Kingdom. I strongly believe that the international comparative evidence will be invaluable in making recommendations with respect to the matters set out in my Terms of Reference."

Expert Services

You have been retained by Hunter Litigation Chambers on BCLC's behalf to provide expert opinion evidence based on your experience regarding 100% known play, 100% carded play and 100% cashless play in the Gaming Jurisdictions.

We enclose for your review as Appendix "A" a "Statement of Assumed Facts".

We ask that you assume for the purposes of your opinion that the facts set out in the "Statement of Assumed Facts" are true. We may provide you with further information or documents as we proceed. We also ask that you inform us if there is additional information or material that you require.

Format of Report

While the Proceeding relates to conduct before an administrative tribunal (a Commission of Inquiry under the *Public Inquiry Act* (BC)), we would ask that you provide us a report consistent with that required in a judicial proceeding. Under the *Supreme Court Civil Rules*, your report must set out the following:

Identification

Please state your name, address and area of expertise.

Qualifications

Please provide a description of your professional qualifications, including your employment and educational experience in your area of expertise. Please attach a current curriculum vitae.

Instructions

Please state that the instructions we have provided to you in relation to the Proceeding are as set out in this letter and attach this letter (with enclosures) as an appendix to your report.

Nature of Opinion

Please state your opinion respecting each issue.

The nature of the opinion I have been asked to provide is as follows:

General

1. Please describe the concept of 100% known play as utilized in land-based casinos in the Gaming Jurisdictions.

2. Please describe the concept of 100% carded play as utilized in land-based casinos in the Gaming Jurisdictions.

3. Please describe the concept of 100% cashless play as utilized in land-based casinos in the Gaming Jurisdictions.

Practice in Gaming Jurisdiction

4. Please describe the casino operators that you are aware of in the Gaming Jurisdictions regarding how the following are used:

    (a) 100% known play; and

    (b) 100% known play with 100% carded play.

Regulatory Practice

5. In answering question four, please advise if you are aware whether:

    (a) regulators have indicated they will require 100% known play and/or 100% carded play in the Gaming Jurisdictions;

    (b) casino operators in Canadian jurisdictions have indicated if they will adapt changes toward 100% known play or 100% carded play in anticipation of regulatory changes from FINTRAC taking effect in June 2021 (setting a threshold of CAD 3,000 for identification and receipting)

Effects of 100% known, carded, and/or cashless play

6. Please summarize the benefits and detriments (if any) of 100% known play, 100% carded play and/or 100% cashless play in the Gaming Jurisdictions. To your knowledge, please describe the if casino operators implemented 100% known play, 100% carded play and/or 100% cashless play following regulations in the Gaming Jurisdictions.

In answering the question, please include practices in Gaming Jurisdictions, including those in North America where high limit play is available.

Reasons for Opinion

Please state the reasons for your opinion, including the following:

1. A description of the factual assumptions on which the opinion is based.

You have been provided with a "Statement of Assumed Facts", enclosed with this letter. We may supplement this with further facts or information, as this Proceeding develops. If at any time, however, you require further information or facts, please let us know and we will attempt to provide them. Also, if you learn about facts or information from your review of documents, please include those facts or information in your report.

It may be necessary for you to make assumptions in order to form your opinions. If you do, please clearly identify any assumptions that you make and list them in this section of your report.

2. A description of any research that you conducted that led you to form your opinion/opinions; and,

3. A list of every document, if any, that you relied on in forming your opinion.

If there are any other documents that you believe would be necessary or helpful to you in providing your opinion, please advise us and we will attempt to provide them. You are welcome to review any relevant documents which you consider necessary to form your opinions, but you must keep record of the documents you have reviewed. Please list all the documents that you reviewed in this part of your report.

Certification

Please certify in your report that:

1. You are aware of the following duty (set out in Rule 11-2(1) and reproduced in Appendix "B") (the "Duty"):

In giving an opinion to the court, an expert appointed under this Part by one or more parties or by the court has a duty to assist the court and is not to be an advocate for any party.

2. You have made your report in conformity with the Duty; and,

3. You will, if called on to give oral or written testimony, give that testimony in conformity with the Duty.

Signature

Please ensure that you personally sign your report.

Role as an Expert

As is apparent from the Duty discussed above, please bear in mind that your role is not that of an advocate, but rather to express the independently formed expert opinion that you hold. Further, please avoid giving an opinion that purports to state a legal conclusion.

Responsibility for Opinion

You must be fully familiar with all of the work done to form and express your opinion, and you must personally hold the opinion that has been tendered. This does not mean that parts of the work leading up to the formation and expression of your opinion cannot have been done, under supervision, by others. However, as the individual who may testify to your opinion in court, you must be the person "primarily responsible" for the opinion and therefore fully conversant with all aspects of its formation and expression. You must, as well, adopt the work of any others involved as your own and be able to answer questions about the methodology and conclusions of all persons who played any part in contributing to the development of your opinion.

Access to Documents, Information, Witnesses and Assumed Facts

In the course of providing your services, you may be given access to documents, information, and BCLC's employees and advisors, as required, in order for you to render your services.

All of your dealings with BCLC, including its employees and advisors related to the Statement of Work dated February 17, 2021, are privileged and strictly confidential. Further, to the extent that you are provided with access to documents and information, please keep them in strict confidence.

Maintenance of Your File

Please maintain in your expert opinion file an organized and complete collection of your papers, notes, calculations, correspondence, telephone logs, and similar materials that are prepared and received by you in the ordinary course of forming your opinion. Please follow your usual practice with respect to the retention of all such materials.

Yours truly,

Hunter Litigation Chambers

Per: 

K. Michael Stephens

Encl.

cc client

APPENDIX "A"
TO EXPERT RETAINER LETTER
DATED APRIL 28, 2021

STATEMENT OF ASSUMED FACTS

Background

1. There have been ongoing, active discussions at BCLC about potentially adopting a mandatory requirement for patrons to swipe their loyalty card (known as an Encore Rewards card), or some form of casino issued identification, upon entry and before playing as part of BCLC's AML effort.

2. This requirement would be a part of a suite of reforms that would work towards the longer-term objective of eliminating anonymous play and allowing BCLC to track every patron transaction that takes place in its casinos. BCLC is of the view that such reforms will help prevent money laundering in its casinos and enhance patron health.

3. The identification requirement would also assist BCLC to meet the new FINTRAC requirements coming into force on June 1, 2021 which among other things, require identification and a "receipt of funds" record for single transactions of CAD 3,000 or more.

4. With respect to customer identification efforts, on November 10, 2020, BCLC put out a request for information for a Customer Identity and Access Management (CIAM) solution. BCLC envisages a CIAM solution that will manage patron access and allow patrons, through a single patron account and identity, to engage with all of the products and services set out above. Such a software solution would allow BCLC to enhance the patron experience, as well as provide BCLC with valuable insight through analytics which could in turn be used to further BCLC's AML efforts.

5. Another measure also under discussion is the idea of "Account Based Gaming", which would not only require use of a card before play, but would link it to an individual's centralized gaming account into which a patron must deposit funds in order to play. Casino play would become completely cashless, and managed through some form of a digital wallet or patron card. Anonymous play at slots and tables would be completely eliminated.

6. These initiatives are still being considered and discussed internally at BCLC, and need to be subject to a full risk assessment before they are operationalized. BCLC also must engage Service Providers and the Gaming Policy and Enforcement Branch for their perspectives and input.

Defined Terms

7. "Time Period" in our letter of instruction means January 1, 2014 to December 31, 2020.

8. Please assume that the phrase "Gaming Jurisdictions" in our letter of assumptions (a) means Canada (excluding British Columbia), United States, European Union, Macau, Australia

or New Zealand and (b) applies only to land-based casinos. We understand that that the United Kingdom is included within consideration of the European Union for the Time Period.

APPENDIX "B"

Rule 11-2 — Duty of Expert Witnesses

Duty of expert witness

(1) In giving an opinion to the court, an expert appointed under this Part by one or more parties or by the court has a duty to assist the court and is not to be an advocate for any party.

Advice and certification

(2) If an expert is appointed under this Part by one or more parties or by the court, the expert must, in any report he or she prepares under this Part, certify that he or she

(a) is aware of the duty referred to in subrule (1),

(b) has made the report in conformity with that duty, and

(c) will, if called on to give oral or written testimony, give that testimony in conformity with that duty.

Exhibit 2

GAMBLING COMMISSION

The prevention of money laundering and combating the financing of terrorism

Guidance for remote and non-remote casinos
Fourth edition

March 2018

Contents

Figures

1 Introduction

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

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

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

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

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

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

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

- placement
- layering
- integration.

1.6 Placement is the first stage in the money laundering cycle. The laundering of criminal proceeds is often required because of the cash-intensive nature of the underlying crime (for example, drug dealing where payments take the form of cash, often in small denominations). The monies are placed into the financial system or retail market, or are smuggled to another country. The aim of the money launderer is to avoid detection by the authorities and to then transform the criminal proceeds into other assets.

1.7 Layering is the next stage and is an attempt to conceal or disguise the source and ownership of the criminal proceeds by creating complex layers of financial transactions which obscure the audit trail and provide anonymity. The purpose of layering is to disassociate the criminal proceeds from the criminal activity which generated them. Typically, layers are created by moving monies in and out of various accounts and using electronic fund transfers.

1.8 Integration is the final stage in the process. It involves integrating the criminal proceeds into the legitimate economic and financial system, and assimilating it with other assets in the system. Integration of the 'clean' money into the economy is accomplished by the money launderer making it appear to have been legally earned or obtained.

1.9 There is potential for the money launderer to use gambling at every stage of the process. The land-based gambling industry is particularly vulnerable during the placement stage as the use of cash is prevalent and the provenance of such cash is not always easy to determine. Although the remote gambling industry might appear less vulnerable as electronic transfers are required for placements, identity theft and identity fraud can enable the money launderer to move criminal proceeds with anonymity. Furthermore, the use of multiple internet transactions can facilitate the layering stage of money laundering.

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

Legal background

The FATF Recommendations and EU Directive

1.11 The Financial Action Task Force (FATF) is the inter-governmental body responsible for setting the international standards for anti-money laundering (AML) and countering terrorist financing (CTF). They issue recommendations which member countries should implement in order to combat money laundering and terrorist financing. These recommendations are implemented by over 190 countries.

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

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

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

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

The Proceeds of Crime Act

1.15 Criminal offences of money laundering were first introduced in the United Kingdom (the UK) in the Criminal Justice Act 1988 and the Drug Trafficking Offences Act 1986. POCA consolidated, updated and reformed the criminal law relating to money laundering to include any dealing in 'criminal property', which is defined widely as the proceeds of any type of crime, however small the amount.

1.16 POCA establishes a number of money laundering offences including:

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

1.17 The principal offences criminalise any involvement in the proceeds of any crime if the person knows or suspects that the property is criminal property.[1] These offences relate to the concealing, disguising, converting, transferring, acquisition, use and possession of criminal property, as well as an arrangement which facilitates the acquisition, retention, use or control of criminal property. For example, in the gambling industry, this may involve the taking of cash, cheque, or card payments, based on funds which are the proceeds of crime, in the form of a bet or wager, or holding money on account for a customer for the purposes of gambling.

1.18 Section 327 of POCA provides that a person commits an offence if he:

- conceals criminal property (for example, by depositing funds obtained through criminal activity into a gambling account)
- disguises criminal property (for example, by placing funds obtained through criminal activity into a gambling account and then withdrawing them at a later date)
- converts criminal property (for example, by placing bets in a gambling establishment and then cashing in the winnings)
- transfers criminal property (for example, by transferring property to another person or to a casino operator)
- removes criminal property from the UK (for example, by taking his winnings overseas).

Concealing or disguising property includes concealing or disguising its nature, source, location, disposition, movement or ownership, or any rights with respect to it. Whilst 'converting' criminal property is not defined in POCA, it is suggested that this be given its conventional legal meaning, that is that the 'converter' has dealt with the property in a manner inconsistent with the rights of the true owner of the property. For example, a criminal steals cash in a bank robbery and then uses that cash to open a gambling account and gamble.

1.19 Section 328 of POCA provides that a person commits an offence if he enters into or becomes concerned in an arrangement which he knows or suspects facilitates, by whatever means, the acquisition, retention, use or control of criminal property by or on behalf of another person. An example of this in the gambling industry would be for a casino operator knowingly to accept stakes that are the proceeds of criminal activity.

1.20 Section 329(1) of POCA provides that a person commits an offence if he:

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

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

Acquisition, use and possession under section 329(1) includes, for example, when a person carries, holds or looks after criminal property or acquires criminal property for 'inadequate consideration'. This means when a person buys or exchanges something which is significantly below market value (inadequate consideration). However, a person does not commit such an offence if he acquired or used or had possession of the property for adequate consideration.[2]

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

1.22 The offence of money laundering and the duty to report under POCA apply in relation to the proceeds of any criminal activity, wherever conducted, including abroad, that would constitute an offence if it took place in the UK. However, a person does not commit an offence of money laundering where it is known or believed, on reasonable grounds that the relevant criminal conduct occurred outside the United Kingdom and the relevant conduct was not criminal in the country where it took place and is not of a description prescribed by an order made by the Secretary of State.[3]

1.23 The money laundering offences assume that a criminal offence has occurred in order to generate the criminal property which is now being laundered. This is often known as a predicate offence. No conviction for the predicate offence is necessary for a person to be prosecuted for a money laundering offence.[4]

1.24 The penalty for conviction on indictment for an offence under sections 327, 328 or 329 of POCA is imprisonment for a term not exceeding 14 years, a fine, or both[5]. In addition, POCA contains provisions for the recovery of the proceeds of crime and forfeiture can be granted, regardless of whether a conviction for any offence has been obtained or is intended to be obtained. Under certain circumstances, criminal property can be recoverable even if it is disposed of to another person.[6]

The Terrorism Act

1.25 The Terrorism Act 2000 (the Terrorism Act) establishes several offences about engaging in or facilitating terrorism, as well as raising or possessing funds for terrorist purposes. It establishes a list of proscribed organisations that are believed to be involved in terrorism. In December 2007, tipping off offences and defences to the principal terrorist property offences were introduced[7].

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

---

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

The Money Laundering Regulations

1.27 The Regulations[8] represent the UK's response to the EU Directive and implement the law in the UK on this topic. They set requirements for the AML/CTF regime within the regulated sector (which includes casinos).

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

- have at least one piece of remote gambling equipment situated in Great Britain, or
- do not have remote gambling equipment situated in Great Britain, but the gambling facilities provided by remote casino are used in Great Britain.[9]

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

1.30 This guidance sets out how casino operators must and can comply with the law governing money laundering and terrorist financing. The law places responsibilities on the Commission as the supervisory authority for casinos. The Commission should produce guidance that helps casino operators to meet the requirements of the law, and is workable in the remote and non-remote casino environments and is approved by HM Treasury. This guidance, therefore, covers the full requirements of the UK law as it affects casinos.

The role of gambling operators

1.31 Operators have a responsibility to uphold the three licensing objectives set out in the Gambling Act 2005 (the Act). The first of those licensing objectives is to prevent gambling from being a source of crime or disorder, being associated with crime or disorder or being used to support crime.

1.32 As described in the preceding paragraphs, money laundering in the gambling sector takes two main forms:

- Exchanging money, assets, goods and property that were acquired criminally for money or assets that appear to be legitimate or 'clean' (so called classic money laundering). This is frequently achieved by transferring or passing the funds through some form of legitimate business transaction or structure.
- The use of criminal proceeds to fund gambling as a leisure activity (so called criminal or 'lifestyle' spend).

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

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

---

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

The role of the Gambling Commission

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

1.36 Under the Regulations[10], the Commission is designated as the supervisory authority for casinos. The Regulations[11] stipulate that a supervisory authority must:

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

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

- the risk assessments carried out by relevant persons to identify and assess the risks of money laundering and terrorist financing to which the business is subject
- the adequacy of the policies, procedures and controls adopted by the relevant persons and the way that those policies, procedures and controls have been implemented[12].

1.38 The Commission therefore adopts a risk-based approach to its role as supervisory authority. We focus our attention on circumstances where the processing of criminal funds or criminal spend indicates serious failures in an operator's arrangements for the management of risk and compliance with POCA, the Regulations and the Terrorism Act or a breach of a licence condition, or makes a reasonably significant contribution to the financial performance of the business, particularly concerning their continued suitability to hold a licence[13].

1.39 Where a casino operator fails to uphold the licensing objectives, for example by being ineffective in applying AML/CTF controls or ignoring their responsibilities under POCA, the Regulations and the Terrorism Act, or breaches an applicable licence condition, the Commission will consider reviewing the operating licence under section 116 of the Act. This could result in the suspension or revocation of the operator's licence under sections 118 and 119 of the Act. The Commission may also consider imposing a financial penalty where a licence condition has been breached, in accordance with section 121 of the Act.

---

[10] Regulation 7(1)(d).
[11] Regulation 46(1) and (2).
[12] Regulation 46(4).
[13] See the public statements.

1.40 Certain activities carried out by non-remote casinos regarding the methods of payment that they accept in respect of gambling services are categorised as money service business (MSB) activities. By acting as a cheque casher or currency exchange, or by accepting winners' cheques and foreign currency, casinos are subject to registration with, and supervision by, HM Revenue and Customs (HMRC). The exemptions that remove this requirement, where the MSB activities are occasional or very limited, do not apply to casinos because of the value of the transactions typically involved. However, in order to avoid dual regulation, and as provided by the Regulations[14], there is an agreement between HMRC and the Commission that the Commission performs the supervisory role for the MSB activities in question. This means that it is not necessary for non-remote casinos to register with HMRC in this regard. Casinos should however note that, in its capacities as a supervisory authority and a law enforcement authority, HMRC may use the UK AML regime to gather information for tax purposes[15].

Purpose of the guidance

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

1.42 The purpose of this guidance is to:

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

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

1.44 While the guidance focuses primarily on the relationship between casino operators and their customers, and the money laundering risks presented by transactions with customers, operators should also give due consideration to the money laundering risks posed by their business-to-business relationships, including any third parties they contract with[16].

[14] Regulation 7(2) and (3).
[15] Regulations 3 and 44 define HMRC as a law enforcement authority for the purposes of the Regulations. Regulation 52 allows supervisory authorities to disclose AML information to law enforcement authorities to fulfil the law enforcement authorities' functions, which, in the case of HMRC, includes collecting information for tax purposes. There are also obligations at regulations 21, 43-45, 49-50, 52, 63 and 64 in respect of law enforcement authorities, which broadly require relevant persons to respond to certain enquiries from law enforcement authorities and to provide information, and for law enforcement authorities and supervisors to cooperate and share information.
[16] Attention is drawn to paragraph 2.10 and code provision 1.1.2.

How should the guidance be used?

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

1.46 This guidance is not intended to be a substitute for legal advice and nothing in this document should be construed as such. Anyone requiring clarification on the legal issues contained in this document should seek their own independent legal advice. Neither is this document a substitute for casino operators' individual risk management plans. Casino operators should refer to the Regulations and associated legislation in making decisions in relation to the Regulations. The examples used throughout are for illustrative purposes only. The references to legislation and case law are accurate at the time of writing, but these may be subject to repeal or amendment.

Content of the guidance

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

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

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

1.50 The guidance contains the following sections:

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

Status of the guidance

1.51 POCA requires a court to take account of industry guidance, such as this, that has been approved by a Treasury minister when considering whether a person within the regulated sector has committed the offence of failing to report. Similarly, the Terrorism Act requires a court to take account of such approved industry guidance when considering whether a person has failed to report under that Act[17]. The Regulations require that a court must consider whether someone has followed this guidance if they are prosecuted for failing to comply with the Regulations.[18]

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

1.53 While the Commission is not a 'designated supervisory authority' under the Regulations[19], an ordinary code provision[20] within the licence conditions and codes of practice requires casino operators to act in accordance with this guidance.

1.54 The Commission and other agencies or authorities that have the appropriate authorisation under POCA in England and Wales[21] can, in certain circumstances, apply for orders and warrants in relation to money laundering, for the purpose of for example:

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

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

Licence conditions and codes of practice

1.56 Casino operators are required to comply with the applicable licence conditions and codes of practice, and should read this guidance in conjunction with the conditions and codes. Should casino operators breach the licence conditions or not follow the code provisions, the Commission may consider reviewing the operating licence in accordance with section 116 of the Act. This could result in the suspension or revocation of the operator's licence under sections 118 and 119 of the Act. The Commission may also consider imposing a financial penalty where we think that a licence condition has been breached, in accordance with section 121 of the Act.

[17] Section 21A(6) of the Terrorism Act.
[18] Sections 330 and 331 of POCA, section 21(6) of the Terrorism Act and Regulation 86(2).
[19] Regulation 76.
[20] Ordinary code provision 2.1.1.
[21] See The Proceeds of Crime Act 2002 (References to Financial Investigators) (England and Wales) Order 2015 (Statutory Instrument No. 2015/1853), as amended.

2 Risk-based approach

Introduction

2.1 The Regulations impose compulsory requirements and a breach can constitute a criminal offence.[22] However, within this legal framework of requirements, casinos have flexibility to devise policies, procedures and controls which best suit their assessment of the money laundering and terrorist financing risks faced by their business. The Regulations require the identification and assessment of money laundering and terrorist financing risks, and the establishment and maintenance of proportionate policies, procedures and controls to mitigate and manage effectively the risks identified.[23]

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

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

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

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

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

2.6 Casino operators can offset any burden of taking a risk-based approach with the benefits of having a realistic assessment of the threat of the operator being misused in connection with money laundering or terrorist financing. It focuses the effort where it is most needed and will have most impact. It is not a blanket one size fits all approach, and therefore operators have a degree of flexibility in their methods of compliance.

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

[22] Regulation 86.
[23] Regulations 18 and 19.

Where the casino operator forms part of a larger group of companies, there needs to be sufficient senior management oversight of the management of risk.

Identifying and assessing the risks

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

- information on the risks of money laundering and terrorist financing made available to them by the Commission
- risk factors, including factors relating to:
  - its customers
  - the countries or geographic areas in which it operates
  - its products or services
  - its transactions
  - its delivery channels[24].

2.9 Casino operators must:

- keep an up-to-date record in writing of all the steps taken to identify and assess the risks of money laundering and terrorist financing risks to which its business is subject
- provide the written record, the risk assessment it has prepared and the information on which it was based to the Commission on request[25].

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

- What risk is posed by the business profile and customers using the casino?
- What risk is posed to the casino operator by transactions with business associates and suppliers, including their beneficial ownership and source of funds?
- Is the business high volume consisting of many low spending customers?
- Is the business low volume with high spending customers, perhaps who use and operate within their cheque cashing facilities?
- Is the business a mixed portfolio? Are customers a mix of high spenders and lower spenders and/or a mix of regular and occasional customers?
- Are procedures in place to monitor customer transactions across outlets, products and platforms and to mitigate any money laundering potential?
- Is the business local with regular and generally well known customers?
- Are there a large proportion of overseas customers using foreign currency or overseas based bank cheque or debit cards?
- Are customers likely to be individuals who hold public positions (PEPs)?
- Are customers likely to be engaged in a business which involves significant amounts of cash?
- Are there likely to be situations where the source of funds cannot be easily established or explained by the customer?
- Are there likely to be situations where the customer's purchase or exchange of chips is irrational or not linked with gaming?
- Is the majority of business conducted in the context of business relationships?
- Is there a local clustering of gambling outlets which makes it easier for a person to launder criminal proceeds over multiple venues and products?
- Does the customer have multiple or continually changing sources of funds (for example, multiple bank accounts and cash, particularly where this is in different currencies or uncommon bank notes)?
- Does the customer have multiple or changing addresses?

[24] Regulation 18(1), (2) and (3).
[25] Regulation 18(4) and (6).

- Has the customer ever presented a fraudulent identity document or failed to provide an identity document repeatedly on request?
- Does the customer's behaviour follow a pattern, or is it constantly changing or changed suddenly recently?
- In relation to remote gaming, does the customer use shared internet protocol addresses, dormant accounts or virtual private network (VPN) connections (among other things, this could indicate that a group of people are using the same device or location to gamble for the purposes of committing fraud)?

As noted in paragraph 1.44, operators should also give due consideration to the money laundering risks posed by their business-to-business relationships, including any third parties they contract with. The assessment of these risks is based, among other things, on the risks posed to the operator by transactions and arrangements with business associates and third party suppliers such as payment providers and processors, including their beneficial ownership and source of funds. Effective management of third party relationships should assure operators that the relationship is a legitimate one, and that they can evidence why their confidence is justified.[26]

Risk assessments

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

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

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

2.13 The key to any risk assessment is that it adopts an approach that attempts to distinguish the extent of different risks to assist with prioritising mitigation efforts, rather than being a generic box-ticking exercise. The risk assessment process should consist of the following standard stages:

- identification
- analysis
- evaluation.

2.14 The identification process begins by developing an initial list of potential risks or risk factors when combating money laundering and terrorist financing. Risk factors are the specific threats or vulnerabilities that are the causes, sources or drivers of money laundering and terrorist financing risks. This list will be drawn from known or suspected threats or vulnerabilities.

[26] An example of good practice guidelines on conducting third party due diligence

The identification process should be as comprehensive as possible, although newly identified or previously unidentified risks may also be considered at any stage in the process.

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

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

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

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

Casinos should also consider the risks posed by particular products they offer.[27]

Country/geographic risk

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

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

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

Customer risk

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

[27] The risk categories used by the Commission in *Money laundering and terrorist financing risk within the British gambling industry* are customer, product and means of payment (as well as operator controls, and licensing and integrity controls).

- customers who are PEPs, family members of PEPs or known close associates of PEPs
- high spenders – the level of spending which will be considered to be high for an individual customer will vary among casino operators, and among casinos managed by the same operator
- disproportionate spenders – casino operators should obtain information about customers' financial resources so that they can determine whether customers' spending is proportionate to their income or wealth
- casual customers – this includes tourists, participants in junkets and local customers who are infrequent visitors
- regular customers with changing or unusual spending patterns
- improper use of third parties – criminals may use third parties or agents to avoid CDD undertaken at the threshold or to buy chips, or they may be used to gamble so as to break up large amounts of cash
- junkets – junkets can pose several higher risks, including criminal control of the junket operator or participants, the movement of funds across borders which obscures the source and ownership of the money gambled by participants and their identities, and structuring, refining and currency exchange risks
- multiple player accounts – some customers will open multiple player accounts under different names to hide their spending levels or to avoid breaching the CDD threshold
- unknown or anonymous customers – these customers may purchase large amounts of chips with cash at casino tables, and then redeem the chips for large denomination notes after minimal or no play.

Transaction risk (including means of payment)

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

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

- e-wallets – some e-wallets accept cash on deposit or cryptocurrencies, which pose a higher risk, and some customers may use e-wallets to disguise their gambling
- games involving multiple operators – for example, poker games often take place on platforms shared by a number of remote gambling operators, which can facilitate money laundering by customers, such as chip dumping.

Product risk

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

2.24 Products which may pose a money laundering risk for the casino operator therefore include:

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

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

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

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

- whether the casino operator's business model is focused on:
  - attracting a large number of customers who gamble relatively small amounts
  - attracting a small number of customers who gamble relatively large amounts
- speed and volume of business
- for non-remote casinos, the size of the premises
- the customer profile, for example whether:
  - the majority of customers are regular visitors or are members
  - the casino relies on passing trade, including tourists or those who are part of junkets (for non-remote casinos)
- for non-remote casinos, whether the casino has VIP rooms or other facilities for high rollers
- types of financial services offered to customers
- types of customer payments and payment methods

- types of gambling products offered
- the customers' gambling habits
- staffing levels, and staff experience and turnover
- the type and effectiveness of existing gambling supervision measures and mechanisms
- whether the casino operator:
    - owns or manages other non-remote and remote casinos
    - offers different types of gambling
    - has other internet gambling websites
- whether the casino is standalone or integrated with other leisure facilities
- whether the casino operator is based in one country or has a gambling presence in multiple countries.

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

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

2.30 Conversely, many customers carry a higher risk of money laundering. These may include known criminals, customers who are not regularly employed or who do not have a regular source of income from a known source which supports the level of activity being undertaken, or problem gamblers.

Examples

- A drug dealer, whose only legitimate source of income for ten years was state benefits, spent more than £1million in various gambling establishments over the course of two years, and lost some £200,000. All the transactions appeared to involve cash.
- A grandparent with no previous gambling history, on a state pension, began to make weekly bets of about £100. Investigations later revealed that the grandparent was placing the bets on behalf of a grandson, a known criminal, and that the money spent was the proceeds of his criminal activity.
- An individual was in receipt of state benefits with no other apparent form of income, but then gambled significant amounts through a licensed operator. Deposits of over £2million were made to an online gambling account over the course of about two years from a multiple of sources, such as debit card and credit card, and various e-money and e-wallet services. Investigations revealed that his gambling was funded by criminal activity.
- Over an extended period of time, an individual who claimed to be a gambling addict stole equipment worth a substantial amount of money from his employer and resold it for his own gain. He then used most of these criminal proceeds to gamble, depositing almost £6million into an online gambling account and losing almost £5million, involving about 40,000 individual gambling transactions. The individual remained in employment throughout this period.

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

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

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

2.33 In order to be able to detect customer activity that may be suspicious, it is necessary to monitor all transactions or activity.[28] The monitoring of customer activity should be carried out using the risk-based approach. Higher risk customers should be subjected to a frequency and depth of scrutiny greater than may be appropriate for lower risk customers. Casino operators should be aware that the level of risk attributed to customers may not correspond to their commercial value to the business.

2.34 Casino operators are best placed to identify and mitigate risks involved in their business activity. A crucial element of this is to have systems and controls to identify and link player activity, and for senior management to oversee risk management and determine whether their policies, procedures and controls are effective in design and application. Reliance on third parties to conduct risk assessment and management functions does not relieve the operator of its responsibility to assess and manage its own risks. Third party services should not be used in isolation or relied upon solely, and casino operators should be satisfied that the information supplied by the third party is sufficiently detailed, reliable and accurate.

2.35 There is a risk that customers will place and layer criminal proceeds through gambling transactions. We recommend that one way of mitigating this risk is to link the payout of winnings with the means by which a customer pays for gambling transactions. We acknowledge that this will not eliminate the risk, but returning winnings in the same form, for example in cash or back to the same bank account, limits the opportunity for a money launderer to layer the proceeds of criminal activity. Where it is not feasible to return funds to the source or in the same form, casino operators should have controls in place to manage the risk of money laundering occurring in these circumstances.

Risk management is dynamic

2.36 A money laundering/terrorist financing risk assessment is not a one-off exercise. Casino operators must therefore ensure that their policies, procedures and controls for managing money laundering and terrorist financing risks, including the detection of criminal spend, are kept under regular review. For example, industry innovation may expose operators to new risks and an appropriate assessment of the risk is recommended before implementing any new product, system, control, process or improvement.

[28] Regulation 8

2.37 Casino operators need to continually identify, assess and manage these risks, just like any other business risk. They should assess the level of risk in the context of how their business is structured and operated, and the controls in place to minimise the risks posed to their business by money launderers, including those engaged in criminal spend. The risk-based approach means that casino operators focus their resources on the areas which represent the greatest risk. The benefits of this approach include a more efficient and effective use of resources, minimising compliance costs and the flexibility to respond to new risks as money laundering methods change.

2.38 There is a specific requirement in the Regulations that, when new technology is adopted by casino operators, appropriate measures are taken in preparation for, and during, the adoption of such technology to assess and, if necessary, mitigate any money laundering or terrorist financing risks the new technology may cause.[29]

3 Customer relationships

3.1 Casino operators should be mindful that some risk indicators (for example, a pattern of increasing spend or spend inconsistent with apparent source of income) could be indicative of money laundering, but also equally of problem gambling, or both. There may also be patterns of play (for example, chasing losses) that appear to be indicative of problem gambling that could also be considered to indicate other risks (for example, spend that is inconsistent with the individual's apparent legitimate income could be the proceeds of crime). While patterns of play may be one indicator of risk, casino operators should satisfy themselves that they have asked, or are prepared to ask, the necessary questions of customers when deciding whether to establish a business relationship, maintain the relationship or terminate the relationship. In summary, it is perfectly plausible that an individual attempting to spend criminal proceeds or launder money could also be a problem gambler, but one does not necessarily follow the other. The responsibility is on the operator to be in a position to understand these dynamics and mitigate any risks to the licensing objectives.

3.2 Casino operators are subject to both certain provisions of POCA, the Regulations and the Act (and the relevant licence conditions and codes of practice). Operators have the responsibility to comply with the licensing objectives and, therefore, they should carry out appropriate enquiries and assessments to ensure they do so. While the conclusions drawn and actions taken may differ according to whether money laundering and/or social responsibility risks are identified, the effective identification and management of these risks rests upon the ability of casino operators to have a comprehensive knowledge of their customer relationships and for managers to be clear on their responsibilities.

3.3 It is also important that the casino operator is able to reconcile information relating to customers' gambling activities in different parts of the business so that they have a more complete picture of the risks posed by the activities of individual customers.

3.4 Commercial and business information should be considered for AML as well as social responsibility purposes when transacting with an individual. This should include arrangements for the monitoring of customers with whom a business relationship has been established. For example, information about customer spend can be used by the casino operator to proactively monitor high risk customers in relation to their money laundering risk.

3.5 Customer relationships need to be managed proficiently and records should be maintained as to what information was communicated to the customer, why it was communicated and what considerations were made.

[29] Regulation 19(4)(c)

If players expect that customer interaction is likely should they play with large amounts of money, or for lengthy periods, and such interaction is consistently applied, there would be less reason for players to question or become suspicious of the motives of these interactions. Casino operators may find it helpful to provide their customers with a leaflet which explains why they are being asked questions about their game play.

3.6 The Commission recognises that some casino operators may find their obligations under POCA and the Regulations challenging, particularly in relation to the management of customer relationships, but it is incumbent on operators to have policies, procedures and controls in place to ensure that they comply with all relevant provisions of POCA and the Regulations (and the Act and the relevant licence conditions and codes of practice), in particular in relation to CDD, the reporting of money laundering activity by customers and the obtaining of a defence (appropriate consent) where necessary.

3.7 Customer relationships for AML purposes consist of three aspects:

- the establishment of the business relationship with the customer, including verification of the customer's identity to a reasonable degree
- the monitoring of customer activity, including account deposits and withdrawals
- the termination of the business relationship with the customer.

3.8 At all stages of the relationship it is necessary to consider whether the customer is engaging in money laundering (including criminal spend); whether there is a need to report suspicious activity or seek a defence (appropriate consent); and any risks posed to the licensing objectives.

Establishment of business relationship

3.9 A business relationship is a business, professional or commercial relationship between a casino operator and a customer which arises out of the business of the casino operator and is expected by the operator, at the time when the contact is established, to have an element of duration.[30] Casino operators are advised to interpret this definition widely.

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

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

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

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

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

[30] Regulation 4(1).

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

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

Customer monitoring

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

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

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

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

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

Termination of business relationship

3.20 As already discussed, to avoid potentially committing one of the principal money laundering offences, casino operators need to consider ending the business relationship with a customer in the following circumstances:

- where it is known that the customer is attempting to use the operator to launder criminal proceeds or for criminal spend
- where the risk of breaches to POCA are considered by the operator to be too high
- where the customer's gambling activity leads to an increasing level of suspicion, or actual knowledge of, money laundering
- where the customer is proven to a reasonable degree of confidence to not be the identity they claim to be.

3.21 Additionally, where, in relation to any customer, the casino operator is unable to apply CDD measures, the business relationship with the customer *must* be terminated and the operator must submit a SAR to the NCA where they consider the circumstances to be suspicious.[31]

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

4 Senior management responsibility

Introduction

4.1 For the purposes of the Regulations and this guidance, 'senior management' means officers or employees of the casino operator with sufficient knowledge of the operator's money laundering and terrorist financing risk exposure, and of sufficient authority, to take decisions affecting its risk exposure.[32]

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

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

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

Obligations on all casino operators

4.5 An officer of a licensed casino operator which is subject to the Regulations (that is, a director, manager, secretary, chief executive, member of the management committee, or a person purporting to act in such a capacity) who consents to, or connives in, the commission of offences under the Regulations, or where the commission of any such offence is attributable to any neglect on their part, will be individually liable for the offence.[33]

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

[31] Regulation 31.
[32] Regulation 3(1).
[33] Regulation 92.

Policies, procedures and controls

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

- proportionate with regard to the size and nature of the operator's business
- approved by its senior management.[34]

4.8 In determining what is appropriate or proportionate with regard to the size and nature of their business, casino operators may take into account any guidance issued by the Commission or appropriate body, *and* approved by HM Treasury.[35] An appropriate body is a body which regulates or is representative of any trade, profession, business or employment carried on by a casino operator[36] (and includes trades bodies such as the National Casino Forum and the Remote Gambling Association).

4.9 Casino operators must maintain a record in writing of:

- their policies, procedures and controls
- any changes to those policies, procedures and controls
- the steps they have taken to communicate the policies, procedures and controls, or any changes to them, within the operator's business.[37]

4.10 The policies, procedures and controls must include:

- risk management practices
- internal controls
- CDD measures and ongoing monitoring, including enhanced measures for high risk customers
- reliance and record keeping
- the monitoring and management of compliance with, and the internal communication of, such policies, procedures and controls.[38]

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

- that provide for the identification and scrutiny of:
  - complex or unusually large transactions, or unusual patterns of transactions, that have no apparent economic or legal purpose
  - and other activity or situation that the casino operator regards as particularly likely, by its nature, to be related to money laundering or terrorist financing
- that specify the undertaking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of products or transactions that might favour anonymity
- which ensure that, when new technology is adopted by the casino operator, appropriate measures are taken in preparation for, and during, the adoption of such technology to assess and, if necessary, mitigate any money laundering or terrorist financing risks this new technology may cause
- under which anyone in the operator's business who knows or suspects, or has reasonable grounds for knowing or suspecting, money laundering or terrorist financing must report such knowledge or suspicion to the operator's nominated officer.[39]

---

[34] Regulation 19(1) and (2).
[35] Regulation 19(5).
[36] Regulation 3(1).
[37] Regulation 19(1)(c).
[38] Regulation 19(3).
[39] Regulation 19(4).

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

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

4.13 Casino operators must, where relevant, communicate the policies, procedures and controls they establish and maintain to their branches and subsidiary undertakings which are located outside the United Kingdom.[40]

Internal controls

4.14 Where appropriate, with regard to the size and nature of the business, a casino operator must appoint a member of its board of directors (or equivalent management body if there is no board) or of its senior management as the officer responsible for the operator's compliance with the Regulations.[41]

4.15 In determining what is appropriate or proportionate with regard to the size and nature of their business, casino operators must take into account their risk assessment and should take into account any guidance issued by the Commission or appropriate body, *and* approved by HM Treasury.[42] An appropriate body is a body which regulates or is representative of any trade, profession, business or employment carried on by a casino operator[43] (and includes trades bodies such as the National Casino Forum and the Remote Gambling Association).

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

4.17 The casino operator must, within 14 days of the appointment, inform the Commission of the identity of the individual appointed as the officer responsible for the operator's compliance with the Regulations, and any subsequent appointment to that position.[44]

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

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

- carrying out screening of relevant employees appointed by the operator, both before the appointment is made and during the course of the appointment, where:
  - screening means an assessment of the skills, knowledge and expertise of the individual to carry out their functions effectively, and the conduct and integrity of the individual
  - a relevant employee is an employee whose work is:
    - relevant to the operator's compliance with any requirement in the Regulations
    - otherwise capable of contributing to the identification or mitigation of the risks of money laundering and terrorist financing to which the operator is subject, or the prevention or detection of money laundering and terrorist financing in relation to the operator's business
- the establishment of an independent audit function with the responsibility to:
  - examine and evaluate the adequacy and effectiveness of the policies, procedures and controls adopted by the operator to comply with the Regulations
  - make recommendations in relation to those policies, procedures and controls
  - monitor the operator's compliance with those recommendations.[45]

4.19 In determining what is appropriate or proportionate with regard to the size and nature of their business, casino operators must take into account their risk assessment and should take into account any guidance issued by the Commission or appropriate body, *and* approved by HM Treasury.[46] An appropriate body is a body which regulates or is representative of any trade, profession, business or employment carried on by a casino operator[47] (and includes trades bodies such as the National Casino Forum and the Remote Gambling Association).

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

- whether it maintains, or has maintained during the previous five years, a business relationship with any person, and
- the nature of the relationship.[48]

Training

4.21 The Regulations require that all relevant employees of casinos must be trained on the prescribed AML and CTF topics[49]. Casino operators must ensure that their employees understand the Regulations, the Terrorism Act and POCA, and data protection, and apply the operator's policies, procedures and controls, including the requirements for CDD, record keeping and SARs.

4.22 One of the most important controls for 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, as well as in the accurate verification of customers' identities.

[45] Regulation 21.
[46] Regulation 21(10).
[47] Regulation 3(1).
[48] Regulation 21.
[49] Regulation 24.

The effective application of even the best designed control systems can be quickly compromised if the employees applying the systems are not adequately trained. The effectiveness of the training will therefore be important to the success of the casino operator's AML/CTF strategy.

4.23 Casino operators should devise and implement a clear and well-articulated policy and procedure for ensuring that relevant employees are aware of their legal obligations in respect of the prevention of money laundering and terrorist financing, and for providing them with regular training in the identification and reporting of anything that gives grounds for suspicion of money laundering or terrorist financing. Casino operators should also monitor the effectiveness of such training, to ensure that all employees are trained in an appropriate and timely manner, and that the training is fit for purpose.

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

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

- made aware of the law relating to money laundering and terrorist financing, and to the requirements of data protection, which are relevant to the implementation of the Regulations
- regularly given training in how to recognise and deal with transactions and other activities or situations which may be related to money laundering or terrorist financing.[50]

4.26 Casino operators must maintain a record in writing of the appropriate training measures they have taken and, in particular, of the training given to their relevant employees.[51]

4.27 'Relevant employees' are employees whose work is:

- relevant to the casino operator's compliance with any requirements in the Regulations, or
- able to contribute to:
  - the identification or mitigation of the risk of money laundering or terrorist financing to which the operator's business is subject, or
  - the prevention or detection of money laundering or terrorist financing in relation to the operator's business.[52]

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

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

- must take account of the nature of its business, its size, and the nature and extent of the money laundering and terrorist financing risks to which its business is subject
- should take account of the guidance issued by the Commission or by any body which represents the casino industry in Britain, such as the National Casino Forum or the Remote Gaming Association.[53]

[50] Regulation 24(1).
[51] Regulation 24(1)(b).
[52] Regulation 24(2).
[53] Regulation 24(3).

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

4.30 Casino operators should also ensure that relevant employees are aware of and understand:

- their responsibilities under the operator's policies and procedures for the prevention of money laundering and terrorist financing
- the money laundering and terrorist financing risks faced by an operator and each of its casino premises
- the operator's procedures for managing those risks
- the identity, role and responsibilities of the nominated officer, and what should be done in his absence
- the potential effect of a breach upon the operator and upon its employees
- how the casino will undertake CDD
- how the casino will track customers when CDD is not undertaken on entry to the casino
- how PEPs, family members of PEPs and known close associates of PEPs will be identified, and how to distinguish PEPs who present a relatively higher risk from those who present a relatively lower risk.

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

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

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

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

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

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

5 Nominated officer

5.1 Casino operators must appoint an individual in their firm as a nominated officer[54], who is responsible for:

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

5.2 This does not allow the nominated officer function to be outsourced to an individual independent of the firm. The requirement to appoint a nominated officer does not apply where the casino operator does not employ, or act in association with, any other person[55]. The casino operator must, within 14 days of the appointment, inform the Commission of the identity of the individual appointed as the nominated officer and any subsequent appointment to that position[56].

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

5.4 The nominated officer should be able to monitor the day-to-day operation of the operator's AML/CTF policies, and respond promptly to any reasonable request for information made by the Commission or law enforcement bodies. The nominated officer is expected to take ultimate managerial responsibility for AML issues, but this does not diminish senior management responsibility for AML.

5.5 The term 'nominated officer' is used and defined in the Regulations[57].

Standing of the nominated officer

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

5.7 The nominated officer must:

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

5.8 In determining the status of the nominated officer and identifying the appropriate position for this officer within the overall organisational structure, casino operators need to ensure their independence within the business and that they have access to all relevant information to enable them to discharge their duties.

[54] Regulation 21(3).
[55] Regulation 21(6).
[56] Regulation 21(4).
[57] Regulation 3(1).

Responsibilities will include objectively reviewing decisions and, on occasions, making recommendations that may conflict with, for instance, short term operational goals.

5.9 The Commission recognises that some casino operators may have a structure in which the nominated officer will hold other roles and responsibilities. The Commission is content, for example, that the nominated officer may take on other compliance roles and responsibilities. However, this is subject to the key principles set out here, including the ability to report directly to the board (or the head of the organisation) and the NCA, and the ability to make AML decisions independently of operational concerns.

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

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

5.12 Where a casino operator's nominated officer delegates to another employee, the nominated officer remains responsible for AML issues and is likely to remain liable for the commission of any criminal offences relating to POCA, the Terrorism Act or the Regulations. The Commission strongly recommends that in such circumstances:

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

Internal and external reports

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

5.14 Whilst disclosure to another of the fact that a person may be engaged in money laundering is generally an offence[58], such disclosures to a nominated officer, constable or customs officer are specifically protected, where they are made as soon as is practicable and the information came to their attention in the course of their trade, profession, business or employment.[59] We recommend that casino operators make employees aware that they have a legal defence to prosecution if they make an internal report to the nominated officer as soon as is reasonably practicable after the information or other matter comes to their attention. Whether or not this defence would be successful would be a matter for the court based on the exact circumstances of the case.

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

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

[58] Section 333A of POCA.
[59] Section 337 of POCA.

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

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

6 Customer due diligence

Introduction

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

6.2 Casino operators must apply CDD measures if they:

- establish a business relationship (see paragraphs 3.9 to 3.13 and 7.5 to 7.9)
- suspect money laundering or terrorist financing
- doubt the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification
- carry out an occasional transaction that amounts to a transfer of funds[60] which is more than €1,000[61].

6.3 Regardless of whether they have established a business relationship with the customer, suspect money laundering or terrorist financing, or doubt the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification, casino operators must *also* apply CDD measures in relation to any transaction that amounts to €2,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked.[62]

6.4 'Transaction' consists of:

- the wagering of a stake, including:
  - the purchase from, or exchange with, the casino of tokens for use in gambling at the casino
  - payment for the use of gaming machines
  - the deposit of funds required to take part in remote gambling, or
- the collection of winnings, including the withdrawal of funds deposited to take part in remote gambling or winnings arising from the staking of such funds.[63]

6.5 In determining whether a transaction amounts to €2,000 or more, casino operators do not need to take account of winnings from a previous transaction which had not been collected from the casino, gaming machine or remote gambling, but are being re-used in the transaction in question.[64] This means that casino operators do not need to include re-staked winnings (so called 'recycled winnings', 'turnover' or 'churn') when determining whether a customer has reached the €2,000 threshold.

---

[60] In this context, 'transfer of funds' means any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same, including: (a) a credit transfer as defined in point (1) of Article 2 of Regulation (EU) No 260/2012; (b) a direct debit as defined in point (2) of Article 2 of Regulation (EU) No 260/2012; (c) a money remittance as defined in point (13) of Article 4 of Directive 2007/64/EC, whether national or cross border; (d) a transfer carried out using a payment card, an electronic money instrument, or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics.
[61] Regulation 27(1).
[62] Regulation 27(5).
[63] Regulation 27(6).
[64] Regulation 27(7).

6.6 Casino operators must *also* apply CDD measures:

- at other appropriate times to existing customers on a risk-based approach
- when the operator becomes aware that the circumstances of an existing customer relevant to its risk assessment for that customer have changed.[65]

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

- any indication that the identity of the customer, or of the customer's beneficial owner, has changed
- any transactions which are not reasonably consistent with the operator's knowledge of the customer
- any change in the purpose or intended nature of the operator's relationship with the customer
- any other matter which could affect the operator's assessment of the money laundering or terrorist financing risk in relation to the customer.[66]

Customer due diligence measures

6.8 CDD measures consist of:

- identifying the customer, unless the identity of the customer is known to, and has been verified by, the casino operator
- verifying the customer's identity, unless the customer's identity has already been verified by the casino operator
- where there is a beneficial owner who is not the customer, identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner so that the casino operator is satisfied that it knows who the beneficial owner is
- assessing and, where appropriate, obtaining information on the purpose and intended nature of the business relationship.[67]

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

- verify that the person is authorised to act on the customer's behalf
- identify the person
- verify the person's identity on the basis of documents or information which, in either case, is obtained from a reliable source which is independent of both the person and the customer.[68]

6.10 For the purposes of CDD, 'verify' means verifying on the basis of documents or information which, in either case, have been obtained from a reliable source which is independent of the person whose identity is being verified. Documents issued or made available by an official body are to be regarded as being independent of a person even if they are provided or made available to the casino operator by, or on behalf of, that person.[69]

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

6.12 The Regulations define casino as 'the holder of a casino operating licence'.[70] The holder of a casino operating licence does not need to repeat CDD if 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.

---

[65] Regulation 27(8).
[66] Regulation 27(9).
[67] Regulation 28.
[68] Regulation 28(10).
[69] Regulation 28(18).
[70] Regulation 14(1)(b).

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

6.13 The ways in which a casino operator meets the requirements for CDD and the extent of the measures it takes must reflect the risk assessment it has carried out, and its assessment of the level of risk arising in any particular case. This may differ from case to case.[71]

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

- the purpose of a customer account, transaction or business relationship
- the amount deposited by a customer or the size of the transactions undertaken by the customer
- the regularity and duration of the business relationship.[72]

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

- the operator has taken CDD measures in relation to the customer
- the operator has submitted a suspicious activity report under POCA or the Terrorism Act, and
- continuing to apply CDD measures in relation to the customer would result in the operator committing tipping off offences under POCA or the Terrorism Act.[73]

6.16 Casino operators should satisfy themselves that the sources of information employed to carry out CDD checks are suitable to mitigate the full range of risks to which they might be exposed, and these would include money laundering and social responsibility risks. For example, local or open source information, such as press reports, may be particularly helpful in carrying out these checks. However, operators should ensure that they are not placing an overreliance on one source of information to conduct these checks.

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

- identified by the operator's risk assessment
- identified by the Commission and in information made available by the Commission.[74]

Timing of verification

6.18 Casino operators must comply with the requirement to verify the identity of the customer, any person claiming to act on behalf of the customer and, where applicable, any beneficial owner before the establishment of a business relationship or the carrying out of the transaction.[75]

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

- this is necessary so as not to interrupt the normal conduct of business
- there is little risk of money laundering and terrorist financing occurring, but
- only provided that the verification is completed as soon as practicable after contact is first established with the customer.[76]

---

[71] Regulation 28(12).
[72] Regulation 28(13).
[73] Regulation 28(15).
[74] Regulation 28(16).
[75] Regulation 30(2).
[76] Regulation 30(3).

Ongoing monitoring

6.20 The Regulations require casino operators to conduct ongoing monitoring of a business relationship. This must include the following:

- scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the casino's knowledge of the customer, the customer's business and risk profile
- undertaking reviews of existing records and keeping the documents or information obtained for the purpose of applying CDD measures up-to-date.[77]

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

Enhanced customer due diligence and enhanced ongoing monitoring

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

- in any case identified by the operator or in information provided by the Commission to the operator as one where there is a high risk of money laundering or terrorist financing[78]
- in any business relationship or transaction with a customer situated in a high-risk third country identified by the European Commission
- if the operator has determined that a customer or potential customer is a PEP, or a family member or known close associate of a PEP
- in any case where the operator discovers that a customer has provided false or stolen identification documentation or information and the operator proposes to continue to deal with the customer
- in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, and the transaction or transactions have no apparent economic or legal purpose
- in any other case which, by its nature, can present a higher risk of money laundering or terrorist financing.[79]

6.23 These enhanced measures:

- must include:
  - examining the background and purpose of the transaction, as far as reasonably possible
  - increasing the degree and nature of monitoring of the business relationship in which the transaction is made, to determine whether the transaction or the relationship appear to be suspicious[80]
- depending on the requirements of the case, may also include, among other things:
  - seeking additional independent, reliable sources to verify information provided or made available to the casino operator

[77] Regulation 28(11).
[78] A key source of information provided by the Commission in relation to where there is a high risk of money laundering or terrorist financing is *Money laundering and terrorist financing risk within the British gambling industry*. This risk assessment is updated at least annually and is available at www.gamblingcommission.gov.uk.
[79] Regulation 33(1).
[80] Regulation 33(4).

- taking additional measures to understand better the background, ownership and financial situation of the customer, and other parties to the transaction
- taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship
- increasing the monitoring of the business relationship, including greater scrutiny of the transactions[81].

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

- whether:
  - the business relationship is conducted in unusual circumstances
  - the customer is resident in a geographical area of high risk
  - the product or transaction might favour anonymity
  - the situation involves non-face-to-face business relationships or transactions (as in the case of remote casinos), without certain safeguards such as electronic signatures[82]
  - payments will be received from unknown or unassociated third parties of the customer
  - new products and new business practices are involved, including new delivery mechanisms, and the use of new or developing technologies (such as virtual currencies) for both existing and new products
- the business relationship or transaction involves countries:
  - identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter money laundering or terrorist financing
  - identified by credible sources as having significant levels of corruption or other criminal activity, such as money laundering, terrorism, and the production and supply of illicit drugs
  - subject to sanctions, embargoes or similar measures issued by, for example, the European Union or the United Nations
  - providing funding or support for terrorism
  - that have organisations operating within their territory which have been designated, by the government of the UK, as proscribed organisations under the Terrorist Act or, by other countries, international organisations or the European Union as terrorist organisations
  - identified by credible sources (such as evaluations, detailed assessment reports or follow-up reports published by FATF, the International Monetary Fund, the World Bank, the organisation for Economic Cooperation and Development or other international bodies or non-governmental organisations) as not implementing requirements to counter money laundering and terrorist financing that are consistent with the FATF recommendations.[83]

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

- the customer transacts with significant amounts of cash
- the customer provides false, forged or stolen identification documentation upon establishing a business relationship

---

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

- the customer transacts with multiple remote gambling operators, particularly where this occurs across multiple geographical areas
- the product, service or transaction involves peer-to-peer gaming
- the product is electronic roulette
- the product, service or transaction involves Ticket In/Ticket Out (TITO) or similar technology.[84]

6.26 In assessing whether there is a high risk of money laundering or terrorist financing, casino operators must bear in mind that the presence of one or more of the risk factors listed above may not always indicate that there is a high risk in a particular situation.[85]

Threshold approach

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

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

6.28 The threshold applies to the wagering of a stake or the collection of winnings, and is to be applied to single transactions or transactions that appear to be linked. Customers may execute a series of linked transactions that are individually below the €2,000 threshold but, when taken cumulatively, they meet or exceed the threshold. Transactions should be considered to be linked if, for example, they are carried out by the same customer through the same game or in one gaming session, or in the case of remote casinos, if they are part of the overall activity undertaken by a customer during a single period of being logged on to the operator's gambling facilities. These examples are not exhaustive and casino operators will need to consider whether there are other circumstances in which transactions are linked. Casino operators will also need to consider, among other things, whether a customer is deliberately spreading their wagering or collection of winnings over a number of transactions in order to circumvent the CDD requirements. They should also ensure that the triggering of the threshold by a customer is not evaded through the customer opening multiple accounts under fictitious names. The measures taken by the operator must be balanced against the requirement to conduct CDD upon establishing a business relationship with a customer (discussed in paragraphs 6.2 and 6.3), requirements for the timing of verification (discussed in paragraphs 6.18 and 6.19) and the need to conduct enhanced customer due diligence in high risk situations (discussed in paragraphs 6.22 to 6.26)[86]. This should be informed by the risk profile of the particular customer, including circumstances which alter the risk attributed to the customer (see paragraphs 6.6, 6.13 and 6.14).

---

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

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

6.30 It should be noted that, under the Regulations, 'gaming machine' has the same meaning as that in the Act[87]. In premises-based casinos, automated and semi-automated table games such as touch-bet roulette are not defined as gaming machines and therefore the take in these games should be counted towards the threshold approach for tokens.

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

6.32 Casinos adopting the threshold approach may wish to defer both identification and verification until the threshold is triggered. Alternatively, they may consider that it is more practical to conduct both identification and verification on entry, or conduct identification on entry and defer verification until the threshold is triggered. For example, a premises based casino may operate a membership scheme where customers are identified on admission to the casino but verification only occurs once the threshold is triggered. Similarly, remote casinos may require customers to identify themselves (and undertake age verification) on registering with the casino, but only require verification of identity if the threshold is triggered. This is sometimes called the hybrid approach.

6.33 There may be advantages in asking customers for their identification on entry, even if verification of this information is deferred until the threshold is reached, for example, identifying customers on entry means it will not be necessary to interrupt the customer's gambling once the threshold is reached and verification becomes necessary. In deciding which approach to take, operators must satisfy themselves and the Commission on a premises-by-premises basis that they have effective procedures, controls and systems in place to track and monitor customers across all the products and platforms that are offered.

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

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

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

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

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

Identification and verification on entry

6.38 The on entry approach requires casinos to identify and verify the identity of the customer before entry to any premises where gaming facilities are provided, or before access is given to remote gambling facilities (see paragraphs 6.18 and 6.19). Once the customer's identity is verified, they may commence gaming.

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

Identification and verification

6.40 Applying CDD measures involves several steps. The casino operator is required to identify customers and then verify their identities, either upon entry or when reaching the threshold. Identification of a customer means being told or coming to know of the customer's identifying details, such as their name and address. Verification, as outlined in paragraph 6.10, means proving a customer is who they claim to be, by obtaining and validating documents or information which supports this claim of identity. The operator *identifies* the customer by obtaining a range of information about the customer. The *verification* of the identity consists of the operator verifying some of this information against documents, data or information obtained from a reliable and independent source.

Identification

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

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

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

6.43 It may also be helpful to obtain information on customers' source of funds and level of legitimate income, for example their occupation. This information may assist casinos with their assessment about whether a customer's level of gambling is proportionate to their approximate income, or whether it is suspicious.

Verification

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

- obtaining or viewing original documents and ensuring that they are valid and genuine, by comparing them to published, authoritative guidance that outlines security features (which protect against forgeries)
- comparing the person presenting the document, or making the document available, to the document itself (for example, photograph comparison or comparison of information)
- conducting electronic verification through a scheme which properly establishes the customer's identity, not just that the customer exists
- obtaining information from another person in the regulated sector (for example, from banks), that can be used in conjunction with other documents and information to prove a customer's legitimacy over time, or positive or negative information.

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

6.45 It is generally considered good practice to require either:

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

and to compare the customer to at least one document from an authoritative source that verifies the customer's full name and address or full name and date of birth, and another supporting document that verifies their name and either date of birth or address, whichever was not included on the document from the authoritative source.

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

Electronic verification

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

6.48 Electronic data sources can provide a wide range of confirmatory material without necessarily requiring the customer to produce documents. Electronic sources can be a convenient method of verification.

They can be used either as the sole method of verification, or in combination with traditional document checks, on a risk basis. For an electronic check to provide satisfactory evidence of identity on its own it must use data from multiple sources, and across time, and incorporate qualitative checks that assess the strength of the information supplied. An electronic check that accesses data from a single source (for example, a single check against the electoral roll) is not enough on its own to verify identity.

6.49 Where such sources are used for a credit check, the customer's permission is required under the Data Protection Act 1998 (the Data Protection Act). Credit checks can provide inexpensive information on which to assess a customer's access to funds and to obtain a credit profile to match against spending patterns. For example, a criminal spending large amounts of criminal property would most likely not match his or her credit profile. A search for identity verification for AML/CTF purposes, however, leaves a different footprint on the customer's electronic record, and the customer's permission is not required, but they must be informed that this check is to take place. There are systems available that give typical financial and lifestyle profiles of people in a given postcode, such systems do not amount to credit check and do not require the use of personal information but can provide helpful indicators of someone's expected financial profile.

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

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

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

6.53 Negative information includes, but is not limited to, consideration of lists of known fraudulent individuals, lists of known fraudulent identity documents, lists of persons associated with known fraudulent identity documents, lists of persons utilising documents made or obtained with fraudulent identity documents, registers of deceased persons, registers of PEPs, lists of sanctioned persons, or information sources for current fraudulent trends or activity. Checking against such information may be appropriate where other factors suggest an increased risk of impersonation fraud.

Criteria for use of an electronic verification provider

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

- it is recognised, through registration with the Information Commissioner's Office, to store personal data
- it uses a range of positive information sources that can be called upon to link an applicant to both current and previous circumstances

- it accesses negative information sources, such as databases relating to identity fraud and deceased persons
- it accesses a wide range of alert data sources
- it has transparent processes that enable the operator to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject.

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

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

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

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

Documentary evidence

6.58 If verification is undertaken using documents, casino operators should usually rely upon documents issued by an authoritative source that can be assessed against official and published guidance on identity documents.

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

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

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

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

6.63 Alternatively, documents from an authoritative source without a photograph which incorporate the customer's full name may be used, supported by a second document, which is issued by an authoritative source, or issued by a public sector body or authority. This second document must also include the customer's full name and either his residential address or his date of birth.

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

- current signed passport
- birth certificate
- current photo card driving licence
- current EEA member state identity card
- current identity card issued by the Electoral Office for Northern Ireland
- residence permit issued by the Home Office
- firearms certificate or shotgun licence
- benefit book or original notification letter from the Department of Works and Pensions confirming the right to benefits
- council tax bill
- utility bill or statement that can, on a risk basis, be verified as true by the company that issued it, commonly by confirmation of a reference number, name and address, 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 that can, on a risk basis, be verified as true by the company that issued it, commonly by confirmation of a reference number, name and address - bank or credit cards alone will not be sufficient as these do not provide either residential address or date of birth.

Wherever the following type of evidence is used, adopting a risk-based approach, you may consider confirming these sources as valid by checking with the issuing authority:

- confirmation from an electoral register that a person of that name lives at that address
- recent original mortgage statement from a recognised lender
- solicitor's letter confirming recent house purchase or land registry confirmation of address
- local council or housing association rent card or tenancy agreement
- HMRC self-assessment statement or tax demand
- house or motor insurance certificate.

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

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

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

Politically exposed persons (PEPs)

Definition

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

- heads of state, heads of government, ministers and deputy or assistant ministers
- members of parliament or of similar legislative bodies
- members of the governing bodies of political parties
- members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances
- members of courts of auditors or of the boards of central banks
- ambassadors, chargés d'affaires and high-ranking officers in armed forces
- members of the administrative, management or supervisory bodies of state-owned enterprises
- directors, deputy directors and members of the board or equivalent function of an international organisation.[88]

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

- family members of the individuals listed above, including spouse, partner, children and their spouses or partners, and parents
- known close associates of the individuals listed above, including individuals with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relations, or who is a sole beneficial owner of a legal entity or arrangement set up for the benefit of the PEP.[89]

6.69 When deciding whether an individual is a known close associate of a PEP, casino operators need only consider information which is in their possession, or credible information which is publicly available.[90]

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

Risk-based approach to PEPs

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

6.72 Establishing whether individuals are PEPs is not always straightforward and can present difficulties. Where casino operators need to carry out specific checks, they may be able to rely on an internet search or consult relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations. Resources such as the Transparency International Corruption Perceptions Index, which ranks approximately 150 countries according to their perceived level of corruption, may be helpful in assessing the risk. This can be found at www.transparency.org/policy_research/surveys_indices/cpi. Another useful source of information is www.knowyourcountry.com. The International Monetary Fund, World Bank and some non-governmental organisations also publish relevant reports.

---

[88] Regulation 35(12) and (14). See paragraph 6.79 in relation to the treatment of PEPs.
[89] Regulation 35(12). See paragraph 6.79 in relation to the treatment of family members and known close associates of PEPs.
[90] Regulation 35(15).

If there is a need to conduct more thorough checks, or if there is a high likelihood of a casino operator having PEPs for customers, subscription to a specialist PEP database may be a valuable tool in assessing the risk.

6.73 New and existing customers may not initially meet the definition of a PEP, but that position may change over time. Equally, individuals who are initially identified as PEPs may cease to be PEPs. For example, the Regulations provide that casino operators must continue applying enhanced customer due diligence to PEPs for at least 12 months after they cease to hold a prominent public function[91]. The casino operator should, as far as practicable, be alert to public information relating to possible changes in the status of its customers with regard to political exposure. Casino operators should be alert to situations which suggest that the customer is a PEP. These situations include:

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

6.74 Although under the definition of a PEP an individual ceases to be so regarded after he has left office for 12 months, casino operators are encouraged to apply a risk-based approach in determining whether or when they should cease carrying out appropriately enhanced monitoring of transactions. In cases where the PEP presents a high risk of money laundering or terrorist financing, a longer period might be appropriate, in order to ensure that the higher risks associated with the individual's previous position have adequately abated.[92]

PEPs requirements

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

- have in place appropriate risk management systems and procedures to determine whether a customer (or the beneficial owner of a customer) is a PEP, or a family member or known close associate of a PEP
- have approval from its senior management for establishing or continuing a business relationship with such persons
- take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or transaction with such persons
- where a business relationship is entered into, conduct enhanced ongoing monitoring of the business relationship with such persons.[93]

6.76 Each casino operator's policies and procedures should cover when and how customers will be checked for PEP status and how and when senior management approval will be sought and provided, and deal with how the customer will be dealt with if there is any delay to approval being provided by senior management.

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

- the money laundering and terrorist risk assessment that the casino operator has conducted
- the level of risk of money laundering or terrorist financing inherent in the operator's business
- the extent to which that risk would be increased by a business relationship with a PEP, or a family member or known close associate of a PEP
- any relevant information made available by the Commission.[94]

---

[91] Regulation 35(9)(a).
[92] Regulation 35(9)(b).
[93] Regulation 33(5).
[94] Regulation 35(2).

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

- the level of risk associated with that customer
- the extent of the enhanced due diligence measures to be applied in relation to that customer, taking into account any guidance issued by the Commission or any other appropriate body (and approved by HM Treasury), and any relevant information made available by the Commission.[95]

6.79 There is a hierarchy of risk for individual PEPs, where some PEPs have higher relative risk and others have lower relative risk. The measures taken for particular PEPs should therefore be informed by the relative risk attributed to the PEP, including consideration of the jurisdiction from which they originate. The Financial Conduct Authority (the FCA) has published guidance in relation to the treatment of PEPs and, while casino operators are not subject to the rules made by the FCA[96], they are advised to consult this guidance when considering the level of risk posed by a particular PEP. The guidance provides advice on who should be treated as a PEP, who should be treated as a family member or known close associate of a PEP, and the level of risk posed by particular PEPs, family members and close associates. Among other things, it recommends that only those individuals in the UK who hold truly prominent positions should be treated as PEPs, and not to apply the definition to local government, more junior members of the senior civil service or anyone other than the most senior military officials[97]. However, this recommendation does not apply when dealing with PEPs from foreign jurisdictions. The FCA guidance also notes that a PEP entrusted with a prominent public function by the UK should be treated as lower risk, unless a regulated firm assesses that risk factors not linked to their position as a PEP mean that they pose a higher risk.

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

- have approval from its senior management for establishing or continuing the business relationship with that person
- take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or transactions with that person
- where the business relationship is entered into, conduct enhanced ongoing monitoring of the business relationship with that person.[98]

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

- for a period of at least 12 months after the date on which the individual ceased to be entrusted with a public function
- or for a longer period that the casino operator considers appropriate to address the risks of money laundering or terrorist financing in relation to that individual.[99]

6.82 When an individual who was a PEP is no longer entrusted with a prominent public function, casino operators are no longer required to apply enhanced customer due diligence measures to the family members or close associates of the PEP. The 12 month period referred to above does not apply in this case.[100]

---

[95] Regulation 35(3) and (4).
[96] Regulation 48(1).
[97] https://www.fca.org.uk/publication/finalised-guidance/fg17-06.pdf. See the Appendix to this guidance.
[98] Regulation 35(5).
[99] Regulation 35(9). This requirement does not apply to individuals who were no longer entrusted with a prominent public function before 26 June 2017 (Regulation 35(10)).
[100] Regulation 35(11).

Simplified customer due diligence

6.83 A casino operator is permitted to apply simplified customer due diligence measures in relation to a particular business relationship or transaction if it determines that the business relationship or transaction presents a low degree of money laundering and terrorist financing risk, taking into account its money laundering and terrorist financing risk assessment, any relevant information made available by the Commission and the risk factors in the following paragraph.[101] The casino operator's risk assessment should identify what products, services, transactions, customers or countries present a low degree of money laundering and terrorist financing risk. Remote casinos operators should note that business relationships and transactions with its customers cannot be considered to present a low degree of money laundering and terrorist financing risk, if no safeguards are in place (see paragraph 6.24).

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

- the country where the customer is resident is:
  - an EEA state
  - a third country which has effective systems to counter money laundering and terrorist financing
  - a third country identified by credible sources as having a low level of corruption or other criminal activity, such as terrorism, money laundering , and the production and supply of illicit drugs
  - a third country which, on the basis of credible sources, such as evaluations, detailed assessment reports or published follow-up reports published by FATF, the International Monetary Fund, the World Bank, the Organisation for Economic Co-operation and Development or other international bodies or non-governmental organisations, has requirements to counter money laundering and terrorist financing that are consistent with the Recommendations published by FATF and effectively implements those Recommendations.[102]

6.85 In making an assessment of a low degree of risk, casino operators must bear in mind that the presence of one or more risk factors may not always indicate that there is a low risk of money laundering and terrorist financing in a particular situation.[103]

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

- continue to comply with the customer due diligence requirements, but it can adjust the extent, timing or type of the measures it undertakes to reflect the determination it has made under paragraph 6.83 in regard to the low degree of money laundering or terrorist financing risk associated with a particular business relationship or transaction, and
- carry out sufficient monitoring of any business relationships or transactions subject to simplified measures to enable it to detect any unusual or suspicious transactions.[104]

[101] Regulation 37(1).
[102] Regulation 37(3).
[103] Regulation 37(4).
[104] Regulation 37(2).

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

- it doubts the veracity or accuracy of any documents or information previously obtained for the purposes of identification or verification
- its money laundering and terrorist financing risk assessment changes and it no longer considers that there is a low degree of risk of money laundering and terrorist financing
- it suspects money laundering or terrorist financing, or
- any of the high risk situations or conditions in paragraph 6.22 apply.[105]

Reliance

6.88 A casino operator may rely on certain third parties to apply the required CDD measures, however, the operator remains liable for any failure to apply such measures.[106]

6.89 The third parties which may be relied on are:

- other persons who are subject to the requirements of the Regulations (financial institutions, credit institutions, auditors, insolvency practitioners, external accountants, tax advisers, independent legal professionals, trust or company service providers, estate agents, high value dealers, and other casinos)
- persons who carry on business in another EEA state (other than the UK) who is subject to requirements in national legislation implementing the Directive as an obliged entity, and is supervised for compliance with the requirements in the Directive
- persons who carry on business in a third country who are subject to requirements in relation to CDD and record keeping which are equivalent to those in the Directive, and are supervised for compliance with those requirements.[107]

6.90 A casino operator may not rely on a third party established in a country which has been identified by the EC as a high risk third country.[108]

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

- must immediately obtain from the third party all the information needed to satisfy the requirements for the identification and verification of the customer, any beneficial owner and any person acting on behalf of the customer
- must have an arrangement with the third party that:
  - enables the operator to obtain from the third party immediately on request copies of any identification and verification data and other relevant documentation on the identity of the customer, beneficial owner or any person acting on behalf of the customer
  - requires the third party to retain copies of such data and documents for a period of five years beginning on the date that the business relationship with the customer ended.[109]

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

- the operator is relying on information provided by a third party which is a member of the same group as the operator (for example, in the case of group companies with overseas casinos)
- that group applies CDD measures, rules on record keeping and programmes against money laundering and terrorist financing in accordance with the Regulations, the Directive or rules having equivalent effect

---

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

- the effective implementation of these requirements is supervised at group level by an authority of an EEA state with responsibility for implementation of the Directive or by an equivalent authority of a third country.[110]

6.93 A casino operator is permitted to apply CDD measures by means of an agent or an outsourcing service provider, provided that the arrangements between the operator and the agent or service provider make clear that the operator remains liable for any failure to apply the CDD measures.[111]

6.94 In this context, an outsourcing service provider is a person who performs a process, service or activity on behalf of the casino operator and is not an employee of the operator.[112]

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

Requirements to cease transactions or terminate relationship

6.96 Where a casino operator is unable to apply the required CDD measures in relation to a particular customer, the operator:

- must not carry out a transaction with or for the customer through a bank account
- must not establish a business relationship or carry out a transaction with the customer other than through a bank account
- must terminate any existing business relationship with the customer
- must consider whether they are required to make a report, or a further report, to the NCA. [113]

6.97 Where the casino operator is required not to carry out a transaction with or for a customer through a bank account, this does not prevent money deposited in a customer's gambling account being repaid to the customer, provided that, where the operator is required to make a report to the NCA, the operator has a defence (appropriate consent) under POCA, or consent under the Terrorism Act, to the transaction.[114]

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

Requirements for remote casinos

6.99 Where remote casino operators are unable to complete or apply the required CDD measures[115] in relation to a particular customer at the point the CDD threshold for transactions[116] is reached, and are accordingly required to cease transactions or terminate the business relationship with the customer[117], they should adopt the following procedure:

- at the point where the threshold is reached, remote casino operators should put all funds owed to the customer into an account (or equivalent) from which no withdrawals can be made
- further deposits can be made to that account as long as they too are locked into it until CDD is completed
- bets can be made from the account, again providing any winnings are locked until CDD is completed

---

[110] Regulation 39(6).
[111] Regulation 39(7).
[112] Regulation 39(8).
[113] Regulation 31.
[114] Regulation 31(2).
[115] These measures are discussed in paragraphs 6.8 to 6.17.
[116] See paragraphs 6.3 to 6.5.
[117] In accordance with regulation 31(1).

- once CDD is completed, the account can be unlocked and business continue as normal
- if CDD cannot be completed, then the operator must proceed in line with regulation 31(1)(c) and terminate the existing business relationship with the customer
- if funds are to be repaid, then the amount repaid should consist of all funds owed to the customer at the point that the threshold was reached, plus all deposits made at that point and thereafter
- funds should be refunded back to the originating account, and:
    - there should be appropriate risk mitigation
    - where it is suspected that the funds are the proceeds of crime, remote casino operators should submit SARs or seek a defence (appropriate consent) before refunding any of the funds
- if the refund is to be completed back to another account (whether partially or completely):
    - risk assessment must be done that should take into account information such as:
        - multiple destinations – is the customer requesting that the money be sent to several bank accounts?
        - high risk destination – is the customer requesting that the money be returned to a country where there is a significant money laundering or terrorist financing concern?
        - above €2,000 – is the amount above the threshold for CDD?
    - there should be appropriate risk mitigation
    - where it is known or suspected that the funds are the proceeds of crime, remote casino operators should submit SARs or seek a defence (appropriate consent) before refunding any of the funds
- there should be ongoing monitoring of the account and, if necessary, reporting of findings via relevant fraud monitoring services in the public and private sector.

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

List of persons subject to financial sanctions

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

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

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

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

6.105 Further information regarding the prohibitions can be found in the OFSI publication.

6.106 OFSI has the power to grant licences exempting certain transactions from the financial restrictions. Requests to disapply the financial restrictions in relation to a designated person are considered by OFSI on a case-by-case basis to ensure that there is no risk of funds being diverted to otherwise restricted purposes. To apply for a licence, OFSI can be contacted using the contact details provided below. Further regime-specific guidance concerning licensing and compliance can be found on gov.uk.

6.107 Casino operators need to have the necessary policies, procedures and controls in place to monitor financial transactions so that payments are not made to designated persons, thereby preventing breaches of the financial restrictions legislation. For manual checking, operators can register with the OFSI update service (directly or via a third party). If checking is automated, operators will need to ensure that the relevant software includes checks against the latest Consolidated List.

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

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

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

6.110 Written reports can be made to OFSI via email.

6.111 Casino operators should consider the likelihood of sanctioned persons using the casino's facilities, taking into account matters such as where the person is resident, and the local demographics of the casino and the its customer base. Operators should bear in mind that sanctioned persons are not exclusively resident abroad, but may also live and operate in the UK and use either a high end casino or a small provincial casino.

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

7 Record keeping

General legal and regulatory requirements

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

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

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

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

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

- no relationship, or
- a 'business relationship', depending on the circumstances.

Business relationships

7.5 A business relationship is a business, professional or commercial relationship between a casino operator and a customer which arises out of the business of the casino operator and is expected by the operator, at the time when the contact is established, to have an element of duration.[118] Casino operators are advised to interpret this definition widely.

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

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

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

7.8 Ongoing monitoring of business relationships is a requirement for casino operators and includes scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the casino's knowledge of the customer, the customer's business and risk profile.[119]

---

[118] Regulation 4(1).
[119] Regulation 28(11).

7.9 As noted in paragraph 6.21, casinos are expected to approach this requirement on a risk-sensitive basis. Dependent on how frequently a casino forms 'business relationships' it may be good practice to apply ongoing monitoring more widely. Regular players should be the subject of closer scrutiny and their level of play should be assessed with reference to the information already known about them, and where necessary, additional information must be collected and retained about the source of their funds.

Other casino customers

7.10 Some casino customers may not fall into the business relationship definition. For example, customers spending low amounts at gaming during single, infrequent and irregular visits to a casino and who are not subject to tracking. There may be no expectation at any stage that there will be any duration to the relationship with the customer. Strictly speaking such business falls outside of the record-keeping requirements (provided the transactions are below the €2,000 threshold for CDD), however, the Commission nonetheless considers it good practice to retain such records.

Customer information

7.11 In relation to the evidence of a customer's identity, casino operators must keep a copy of any documents or information obtained to satisfy the CDD measures required under the Regulations.[120]

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

7.13 There is a separate requirement in the Regulations to ensure that documents, data or information held by casinos are kept up to date.[121] 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, procedures and controls.

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

Supporting records (non-remote casinos)

7.15 The requirement to keep supporting records is linked to 'business relationships' which is defined in the Regulations[122] and the extent and nature of records created. In many casinos, customers (regardless of whether or not they have formed a business relationship) purchase chips with cash at gaming tables where, in low risk situations, no records are created and therefore are not available to be kept.

---

[120] Regulation 40(2).
[121] Regulation 28(11).
[122] Regulations 3 and 4.

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

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

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

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

Supporting records (remote casinos)

7.20 Remote casinos will, by the nature of their business, generate detailed records of all transactions with each customer but for the purposes of the record keeping requirements it is sufficient to retain the deposit and withdrawal figures for each named customer.

Supporting records (gaming machines)

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

7.22 The essentials of any system of monitoring are that:

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

7.23 Monitoring can be either:

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

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

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

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

Retention period

7.26 Records of identification and verification of customers must be kept for a period of five years after the business relationship with the customer has ended, for example where the customer closes his gambling account with the operator or ceases to visit or use the casino.[123]

7.27 Supporting records must be retained for a period of five years from the date the business relationship ended.[124]

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

- the casino operator is required to retain records containing personal data by or under any law or the purposes of any court proceedings
- the subject of the data has agreed to the retention of the data, or
- the casino operator has reasonable grounds for believing that records containing the personal data need to be retained for the purposes of legal proceedings.[125]

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

Form in which records are to be kept

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

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

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

7.32 Where the record keeping obligations under the Regulations are not observed, an operator or person is open to prosecution and sanctions, including imprisonment for up to two years and/or a fine, or regulatory censure.[126]

---

[123] Regulation 40(3).
[124] Regulation 40(3).
[125] Regulation 40(5).
[126] Regulation 83(1).

Data protection

7.33 Any personal data obtained by casino operators for the purposes of the Regulations may only be processed for the purposes of preventing money laundering and terrorist financing.[127]

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

- use of the data is permitted by or under any law other than the Regulations, or
- the casino operator has obtained the agreement of the subject of the data to the proposed use of the data.[128]

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

- the registrable particulars of the operator
- a statement that any personal data received from the customer will be processed only for the purposes of preventing money laundering or terrorist financing, or as permitted by the circumstances described in paragraph 7.34 above.[129]

8 Suspicious activities and reporting

Introduction

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

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

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

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

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

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

[127] Regulation 41(1).
[128] Regulation 41(3).
[129] Regulation 41(4).

What is meant by knowledge and suspicion?

8.4 In the context of POCA, knowledge means *actual* knowledge. Having knowledge means actually knowing something to be true. In a criminal court, it must be proved that the individual in fact knew that a person was engaged in money laundering. Knowledge can be inferred from the surrounding circumstances, so, for example, a failure to ask obvious questions may be relied upon by a jury to infer knowledge[130]. The knowledge must, however, have come to the casino operator (or to the employee) in the course of casino business or (in the case of a nominated officer) as a consequence of a disclosure under section 330 of POCA. Information that comes to the casino operator or employee in other circumstances does not come within the scope of the regulated sector obligation to make a report. This does not preclude a report being made should employees choose to do so. Employees may also be obliged to make a report by other parts of the Act. Further information can be found in Part 7 of POCA.

8.5 In the case of *Da Silva* [2006] EWCA Crim 1654, the Court of Appeal stated the following in relation to suspicion:

> "*It seems to us that the essential element in the word "suspect" and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice.*"

There is thus no requirement for the suspicion to be clear or firmly grounded on specific facts, but there must be a degree of satisfaction, not necessarily amounting to belief but at least extending beyond mere speculation, that an event has occurred or not.

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

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

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

8.9 In order for either an internal or external report to be made it is not necessary to know or to establish the exact nature of any underlying criminal offence, or that the particular funds or property were definitely those arising from a crime. Furthermore, it is not necessary to await conviction of a customer for money laundering or other criminal offences in order to have suspicion that money laundering has taken place.

---

[130] Refer to *Baden v Societe Generale pour Favouriser le Developpement du Commerce et de l'Industrie en France* [1983] BCLC 325.

What is meant by reasonable grounds to know or suspect?

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

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

What constitutes suspicious activity?

8.12 There are numerous things that can make someone either know or suspect that they are dealing with the proceeds of crime. Some examples of how suspicions may be raised are listed below, although this is not an exhaustive list and there may well be other circumstances which raise suspicion.

Examples

- A man convicted of dealing in drugs is released from prison and immediately starts gambling large amounts of money. He is known to be out of work and other customers inform employees that he is supplying drugs again. This will give rise to the suspicion that he is spending the proceeds of his criminal activity.
- Stakes wagered by a customer become unusually high or out of the ordinary and the customer is believed to be spending beyond his or her known means. This requires some knowledge of the customer but, nevertheless, there may be circumstances that appear unusual and raise the suspicion that he is using money obtained unlawfully. It may be that the customer lives in low cost accommodation with no known source of income but nonetheless is spending money well above his or her apparent means. There is no set amount which dictates when a SAR should be made and much will depend on what is known, or suspected, about the customer.
- A customer exhibits unusual gambling patterns with an almost guaranteed return or very little financial risk (sometimes across multiple operators). It is accepted that some customers prefer to gamble in this way but, in some instances, the actions may raise suspicion because they are different from the customer's normal gambling practices.
- Money is deposited by a customer or held over a period and withdrawn by the customer without being used for gambling. For instance, suspicions should be raised by any large amounts deposited in gaming machines or gambling accounts that are then cashed or withdrawn after very little game play or gambling.
- A customer regularly gambles large amounts of money and appears to find a level of losses acceptable. In this instance, the customer may be spending the proceeds of crime and sees the losses as an acceptable consequence of the process of laundering those proceeds.

- A customer's spend increases over a period of time, thereby masking high spend and potential money laundering.
- A customer spends little, but often, and his annual aggregate spend is high and out of kilter with his expected spend. This could indicate potential money laundering.
- A customer displays gambling patterns where spend is high but the risk is low, for example gambling on red and black in roulette. The customer could be laundering money in a way that guarantees minimal loss.
- A customer gambles with significant amounts of money in a currency without a reasonable explanation for the source of that currency, such as Scottish and Northern Irish bank notes presented by a customer in an English casino.
- Instances of high spend by customers that lead to significant commercial risk for the operator may also indicate suspicious activity.

8.13 It is important to note that, once knowledge or suspicion of criminal spend is linked to a customer in one area of the business (for example, table games), it is good practice to monitor the customer's activity in other areas of the business (for example, gaming machine play).

Internal reporting

8.14 Employees of a casino operator have a legal defence if they report to the nominated officer where they have grounds for knowledge or suspicion of money laundering or terrorist financing. All casino operators therefore need to ensure that all relevant employees know they should report suspicions to their nominated officer. Internal reports to a nominated officer, and reports made by a nominated officer to the NCA, must be made as soon as is practicable.

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

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

Evaluation and determination by the nominated officer

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

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

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

External reporting

8.20 To avoid committing a failure to report offence, the nominated officer must make a disclosure to the NCA where he decides that a report gives rise to grounds for knowledge or suspicion. The national reception point for the disclosure of suspicions, and for seeking a defence (consent) to proceed with the transaction or activity, is the UK Financial Intelligence Unit (UKFIU) within the NCA.

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

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

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

Submission of suspicious activity reports[131]

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

- **SAR Online**, which is a secure web-based reporting system for small or medium sized reporting entities with access to the internet, which allows SARs to be submitted electronically through www.ukciu.gov.uk/saronline.aspx. It is the NCA's preferred method of reporting. Reporters must register themselves as a source (reporting entity) on the system once, and then submit SARs by completing linked electronic screens that reflect the fields included in the paper based reports. Requests for a defence (consent) can be submitted using SAR Online, and as long as the box for consent is checked at the start of the process, the system alerts the Consent Team automatically, ensuring swift identification and management of requests for a defence (appropriate consent). It is not necessary to send the request by fax as well as submission online.

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

SAR Online is the NCA's preferred method for small and medium sized reporting entities to submit SARs. The benefit to the reporter is 24/7 reporting, an automatic acknowledgment of receipt with the ELMER reference number, and investigators are able to access the information more rapidly.

- **Paper based reporting**, using the standard NCA Suspicious Activity Report Form. The NCA prefers submissions to be typed to enable it to be scanned and prevent errors in data entry. The form and guidance on using the form can be found on the NCA website. Completed forms should be posted to UKFIU, PO Box 8000, London, SE11 5EN. If using the form to request a defence (appropriate consent), it should be faxed immediately to 0207 238 8286, but it is not necessary to post and fax a request. The paper based reporting system will not elicit an acknowledgment of receipt or an ELMER reference number for your records, and the SAR will take some time to reach investigators.

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

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

8.26 Casino operators should ensure that they check all the facts they have about the customer and include all relevant information when submitting a SAR, which may include the following:

- Do the staff know the customer's identity?
- Is a physical description of the customer available?
- Has the customer provided any records that will assist in identifying him, for example credit or debit card details?
- Has the customer ever self-excluded?
- What are the customer's product preferences and does he hold other gambling accounts (for example, prefers casino gaming, but also uses online gambling facilities)?

8.27 In order that an informed overview of the situation may be maintained, all contact between the casino operator and law enforcement agencies should be controlled through, or reported back to, the nominated officer or a deputy acting in the absence of the nominated officer. The NCA may apply to the magistrates' court (or, in Scotland, the sheriff) for an order (a further information order), following the submission of a SAR, requiring the nominated officer to provide more information in respect of the SAR[132]. Law enforcement agencies may also apply for a disclosure order requiring any person considered to have information relevant to an investigation to answer questions, provide information or to produce documents[133].

8.28 POCA also makes provision for the voluntary sharing of information between persons in the regulated sector when deciding whether to submit a SAR, and joint SARs by persons in the regulated sector, subject to certain limitations. The exchange of information in these circumstances is protected from breaching any confidentiality obligations or other restrictions.[134]

---

[132] Section 339ZH of POCA.
[133] Section 357 of POCA.
[134] Sections 339ZB to 339ZG of POCA.

Requesting a defence

8.29 If casino operators handle any proceeds of crime they may commit one of the principal money laundering offences in POCA or the Terrorism Act. However, if the nominated officer submits a SAR to the NCA this can provide a defence. There is a statutory mechanism which allows the NCA either to grant or refuse the 'prohibited act' going ahead, or to prevent the suspected money laundering going ahead[135]. This statutory mechanism is called 'appropriate consent' and is referred to by the NCA as *Requesting a defence from the NCA under POCA and TACT*.

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

- concealing, disguising, converting, transferring or removing criminal property[136]
- facilitating the acquisition, retention, use or control of criminal property by, or on behalf of, another person[137]
- acquisition, use or possession of criminal property[138].

These are referred to as 'prohibited acts'.

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

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

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

8.33 A nominated officer, police constable, NCA employee or customs officer can give a person (which may include, for example, a casino employee) *actual* 'appropriate consent' to a suspect transaction proceeding.[139] However, it should be noted that the NCA is the only body able to issue formal notification of a defence (consent) by means of an official NCA letter, which the nominated officer can then retain for his records.

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

- consent is not refused within seven working days (beginning with the day after the notice is given)
- if consent is refused and following such refusal, the 'moratorium period' (31 calendar days starting with the day on which the person receives notice that consent to the doing of the act is refused) has expired (but see paragraph 8.35).[140]

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

---

[135] Section 335 of POCA.
[136] Section 327 of POCA.
[137] Section 328 of POCA.
[138] Section 329 of POCA.
[139] Section 335(1) of POCA.
[140] Section 335(2) of POCA.

8.35 Casino operators should be aware that the NCA and other authorities, such as the FCA and Serious Fraud Office, can apply to the Crown Court (or, in Scotland, the sheriff) for an order to extend the moratorium period for a further 31 days. An order can be given on up to six occasions which allows the moratorium period to be extended for a maximum period of 186 days in total. To grant an order for an extension, in each case the Court must be satisfied that the NCA or other authority's investigation is being carried out "diligently and expeditiously", additional time is needed to complete the investigation and an extension would be reasonable in the circumstances.[141]

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

- the NCA employee has provided a defence (consented to the transaction)
- a defence (consent) is not refused within seven working days (beginning with the day after the notice is given)
- if a defence (consent) is refused and following such refusal, the 'moratorium period' (31 calendar days starting with the day on which the person receives notice that consent to the doing of the act is refused) has expired (but see paragraph 8.35).[142]

8.37 Reporting suspicious activity before or reporting after the event are not equal options which a casino operator can choose between, and retrospective reporting is unlikely to be seen in the same light as reporting prior to the event. A report made after money laundering has already taken place will only be a legal defence if there was a 'reasonable excuse' for failing to make the report before the money laundering took place.[143] Where a customer request is received prior to a transaction or activity taking place, or arrangements being put in place (for example, where a customer requests the opening of a gambling account), and there is knowledge or suspicion, or reasonable grounds for suspicion, that the transaction, arrangements, or the funds/property involved, may relate to money laundering, a SAR must be submitted to the NCA and a defence (consent) sought to proceed with that transaction or activity. In such circumstances, it is an offence for a nominated officer to agree to a transaction or activity going ahead within the seven working day notice period from the working day following the date of disclosure, unless the NCA provides a defence (gives consent).[144]

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

8.39 In the casino environment, business is often conducted out of normal office hours. In addition, gambling transactions may sometimes be more 'immediate' than, for example, depositing funds into a bank account where the funds may be withdrawn at a later date. In these circumstances it may sometimes not be feasible or practical to obtain a defence (appropriate consent) prior to or during a transaction. Knowledge or suspicion of money laundering or terrorist financing may be triggered after a customer has completed all the stages of a gambling transaction; that is, they have bought in, they have played and they have cashed out. Under those circumstances, it may be reasonable to report after the transaction. However, the defence of 'reasonable excuse' when reporting after the transaction is untested by case law and should be considered on a case-by-case basis.[145] Where the relationship with the customer is expected to have an element of duration and involve numerous transactions, it is advisable to seek a defence (consent) prior to transacting with the customer.

---

[141] Section 336A of POCA.
[142] Section 336 of POCA.
[143] Section 327(2)(b) of POCA.
[144] Section 336(3) and (4) of POCA.
[145] Section 327(2)(b) of POCA.

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

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

8.42 Casino operators should also note that in the Commission's view the reporting defence is not intended to be used repeatedly in relation to the same customer. In the case of repeated SAR submissions on the same customer, it is the Commission's view that this is not a route by which operators can guarantee a reporting defence retrospectively. If patterns of gambling lead to an increasing level of suspicion of money laundering, or to actual knowledge of money laundering, operators must seriously consider whether they wish to allow the customer to continue using their gambling facilities. Casino operators are, of course, free to terminate their business relationships if they wish and, provided this is handled appropriately, there will be no risk of 'tipping off' or prejudicing an investigation. However, operators should think about liaising with the law enforcement investigating officer to consider whether it is likely that termination of the business relationship would alert the customer or prejudice an investigation in any other way.

8.43 How customers suspected of money laundering or terrorist financing will be dealt with is an important area of risk management for all casino operators. They should deal with the issue in their policies, procedures and controls. As all operators are at risk of committing the principal offences, it is advisable to consider these issues carefully before they arise in practice.

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

Applying for a defence

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

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

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

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

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

8.49 *Home Office Circular 029/2008* contains guidance on the operation of the consent regime in POCA. It was issued to ensure consistency of practice on the part of law enforcement in considering requests for consent under Part 7 of POCA. This was in response to concerns from the financial services industry and other sectors and professions that decisions should be taken in an effective and proportionate way, with due engagement with all participants. The circular was formulated in agreement with key partner agencies and sets out the high-level principles by which the law enforcement agencies should make decisions on consent, and how these principles should be applied.

8.50 Although POCA provides that consent can be granted by a constable (which includes authorised NCA officers) or a customs officer, there is a recognised need to ensure that the practices of all law enforcement agencies are consistent in this area. Therefore, as a result of the circular, the NCA operates as the national centre for all authorised disclosures and also for the issue of decisions concerning the granting or refusal of a defence (consent). To avoid confusion those making requests for a defence (consent) should route requests through the NCA. The decision making process will consist of a collaborative effort between the NCA and the other law enforcement agencies, with the latter providing a recommendation to the NCA. While the final decision will be taken by the NCA, in most cases it is likely to be based largely on the recommendation provided by the interested law enforcement agency.

8.51 All requests for a defence (consent) are dealt with by the NCA on a case-by-case basis. It may take the maximum of seven working days to deal with a defence (consent) request, however, in most cases the NCA is able to respond to requests for a defence (consent) within three days.[146] Nominated officers should take this into account when deciding whether it is practical and reasonable to request a defence (consent) prior to the transaction or activity rather than making a report after the transaction or activity.

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

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

[146] NCA Annual Report

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

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

8.56 The NCA cannot give advice to nominated officers and casino operators in relation to the specific circumstances where SARs should be submitted or the terms for requesting a defence (appropriate consent). Comprehensive guidance on requesting a defence is available on the NCA's website. We draw your attention, in particular, to the following NCA publication: *Requesting a defence from the NCA under POCA and TACT*[147].

Suspicious activity reporting requirements for remote casinos

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

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

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

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

Suspicious activity reporting

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

[147] Available from www.nationalcrimeagency.gov.uk

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

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

8.64 These reporting requirements are summarised in the table below:

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

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

Applying for a defence

8.65 Where remote casino operators wish to make use of the defences provided by sections 327(2)(a), 328(2)(a) and 329(2)(a) of POCA where they believe that, by proceeding with a transaction with a British customer, they will be committing a prohibited act, they should apply for a defence (appropriate consent), in accordance with section 335 of POCA, from the NCA.[148]

Failing to report

8.66 POCA and the Terrorism Act create offences of failing to report suspicious activity[149]. Where a person fails to comply with the obligations to make disclosures to a nominated officer and/or the NCA as soon as practicable after the information giving rise to the knowledge or suspicion comes to the employee they are open to criminal prosecution. The criminal sanction, under POCA or the Terrorism Act, is a prison term of up to five years, and/or a fine.

[148] See paragraphs 8.45 to 8.56.
[149] Sections 330 and 331 of POCA, and section 19 of the Terrorism Act.

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

- knows the identity of the money launderer or the whereabouts of the laundered property
- believes the information on which the suspicion was based may assist in identifying the money launderer or the whereabouts of the laundered property.[150]

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

After a report has been made

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

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

Tipping off, or prejudicing an investigation

8.71 Under section 333A of POCA a person in the regulated sector commits an offence if:

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

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

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

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

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

[150] Sections 330(3A) and 331(3A) of POCA

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

- does not know or suspect that the documents are relevant to the investigation
- does not intend to conceal any facts disclosed by the documents from any appropriate officer or (in Scotland) proper person carrying out the investigation.[151]

8.74 POCA therefore, in this regard, contains separate offences of tipping off and prejudicing an investigation. These offences are similar and overlapping, but there are also significant differences between them. It is important for those working in the regulated sector to be aware of the conditions for each offence. Each offence relates to situations where the information on which the disclosure was based came to the person making the disclosure in the course of a business in the regulated sector. The Terrorism Act contains similar offences[152]. There are a number of disclosures which are permitted and that do not give rise to these offences (permitted disclosures) – see paragraphs 8.65 to 8.67.

8.75 Once an internal or external report of suspicious activity has been made, it is a criminal offence for anyone to release information that is likely to prejudice an investigation that might be conducted following that disclosure. An offence is not committed if the person does not know or suspect that the disclosure is likely to prejudice an investigation, or if the disclosure is permitted under POCA or the Terrorism Act[153]. Reasonable enquiries of a customer, conducted in a tactful manner, regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity is prudent practice, forms an integral part of CDD measures and should not give rise to tipping off.

8.76 Where a confiscation investigation, a civil recovery investigation, a detained cash investigation or a money laundering investigation is being, or is about to be, conducted, it is a criminal offence for anyone to disclose this fact if that disclosure is likely to prejudice the investigation. It is also a criminal offence to falsify, conceal, destroy or otherwise dispose of documents which are relevant to the investigation (or to cause or permit these offences). It is, however, a defence if the person does not know or suspect that disclosure is likely to prejudice the investigation, or if the disclosure is permitted under POCA or the Terrorism Act (see paragraphs 8.77 to 8.79).

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

- 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.[154]

8.78 An employee, officer or partner of a casino operator does not commit an offence under POCA or the Terrorism Act if the disclosure is to an employee, officer or partner of the casino operator.[155]

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

- any investigation that might be conducted following a disclosure
- an investigation into allegations that an offence under Part 7 of POCA or Part III of the Terrorism Act has been committed, is being contemplated or is being carried out.[156]

---

[151] Section 342(6) of POCA.
[152] Sections 21D and 39 of the Terrorism Act.
[153] Section 342(3) of POCA and section 20 of the Terrorism Act.
[154] Section 333D of POCA and section 21G of the Terrorism Act.
[155] Section 333B of POCA and section 21E of the Terrorism Act.
[156] Section 333D of POCA and section 21G of the Terrorism Act.

8.80 The fact that a transaction is notified to the NCA before the event, and the NCA does not refuse a request for a defence (consent) within seven working days following the day after disclosure is made, or a restraint order is not obtained within the moratorium period, does not alter the position so far as 'tipping off' is concerned.

8.81 This means that a casino operator:

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

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

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

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

8.85 The offence of money laundering, and the duty to report under POCA, apply in relation to the proceeds of any criminal activity, wherever conducted, including abroad, that would constitute an offence if it took place in the UK. A person does not commit an offence where it is known or believed on reasonable grounds that the conduct occurred outside the UK; and the conduct was not criminal in the country where it took place. However, if the criminal activity would constitute an offence in the UK if committed here and would be punishable by imprisonment for a maximum term in excess of twelve months then the defence does not apply except if the offence is an offence under section 23 or 25 of the Financial Services and Markets Act 2000.

8.86 There is also a specific offence of failure to disclose terrorist financing which was added to the Terrorism Act through the Anti-terrorism Crime and Security Act 2001. This offence is limited to the regulated sector, which includes casinos. The offence can be committed if a person forms knowledge or suspicion of terrorist financing or reasonable grounds for suspecting terrorist financing, during the course of working for a casino, but does not make a report. Guidance issued by the Commission and approved by HM Treasury must be taken into consideration by any court considering whether this offence has been committed[157].

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

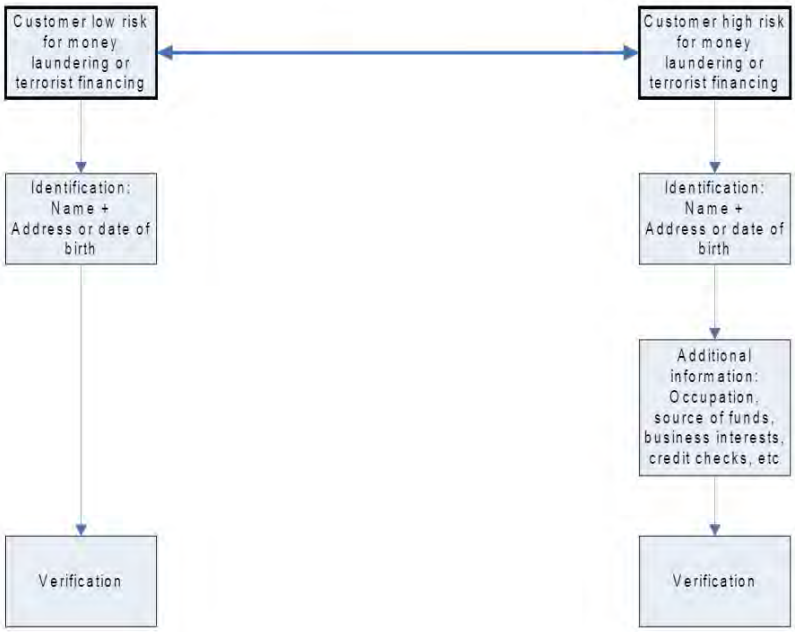
Interaction with customers

8.87 Normal customer enquiries will not, in the Commission's view, amount to tipping off or prejudicing an investigation under POCA, unless you know or suspect that a SAR has already been submitted and that an investigation is current or impending and make the enquiries of the customer in a way that it discloses those facts. Indeed, such customer enquiries are likely to be necessary not only in relation to money laundering but also in connection with social responsibility duties (for example, problem gambling). In regard to this offence, counter or frontline staff may not be aware that the nominated officer has submitted a SAR to the NCA. Reasonable and tactful enquiries regarding the background to a transaction or activity that is inconsistent with the customer's normal pattern of activity is good practice, forms an integral part of CDD measures (and may be driven by social responsibility concerns) and should not give rise to tipping off or the prejudicing of an investigation.

8.88 If patterns of gambling lead to an increasing level of suspicion of money laundering, or even to actual knowledge of money laundering, casino operators should seriously consider whether they wish to allow the customer to continue using their gaming facilities. If a casino operator wishes to terminate a customer relationship, and provided this is handled sensitively, there will be low risk of tipping off or prejudicing an investigation. However, if the decision has been made to terminate the relationship and there is a remaining suspicion of money laundering with funds to repatriate, consideration should be given to asking for a defence (appropriate consent).

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

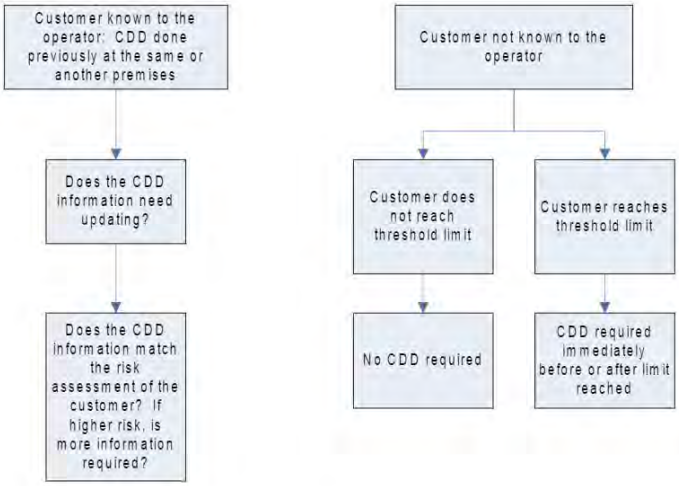
Figure 1: Risk-based approach



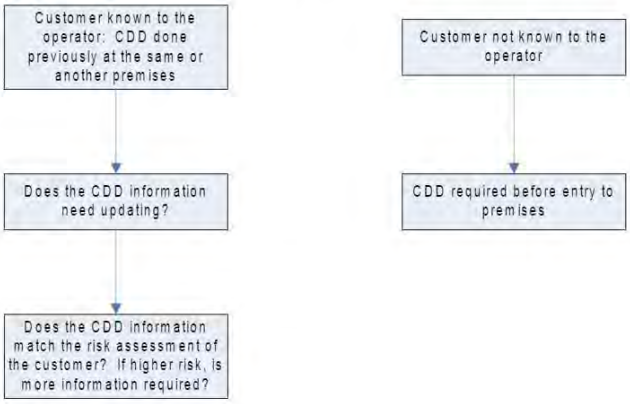
Note:
Casino operators should undertake risk assessments of each premises and each remote site and:
(a) look at the average drop/win per customer, and
(b) risk assess each customer.

Figure 2: Customer due diligence

Threshold model



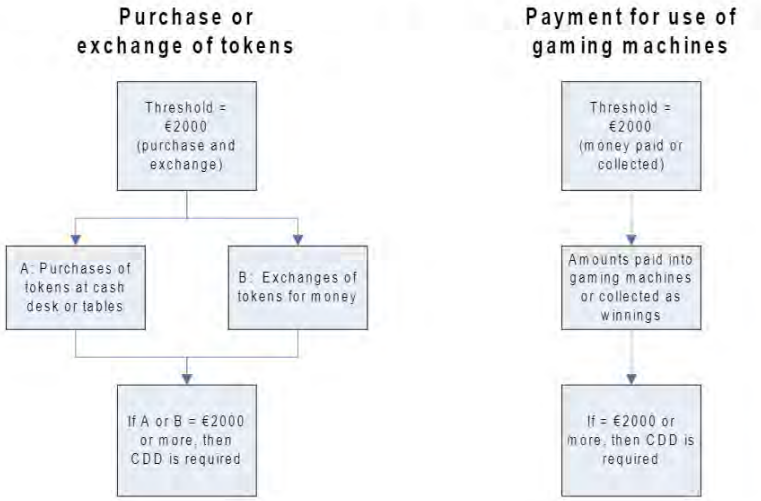
On entry model



Notes:

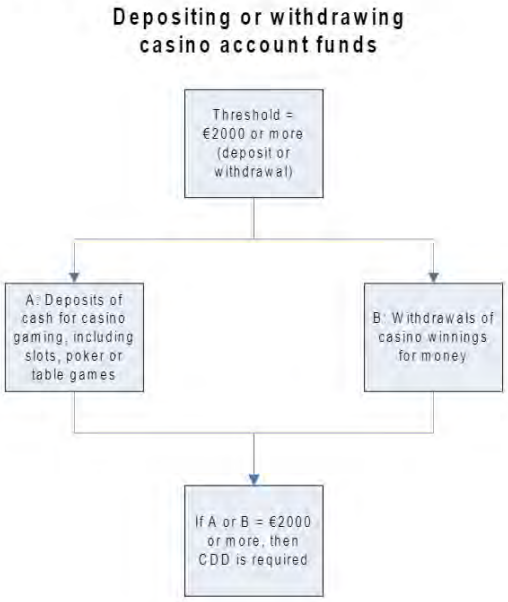
1. Operator to be reasonably satisfied that the customer is who they claim to be.
2. The requirement applies to an operator, not to each premises.
3. Identification: Name, plus residential address or date of birth.
4. Verification: Documents or electronically.
5. Records of CDD to be kept for five years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

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



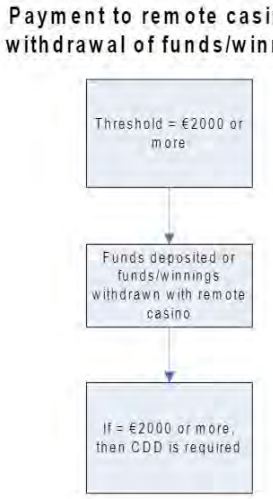
Notes:
1. A customer could spend €1800 on tokens and a further €1800 in a gaming machine and not reach the threshold.
2. Risk-based approach – operator analysis of spending behaviours at each premises and an objective assessment made of the likelihood of customers reaching either threshold. Measures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

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



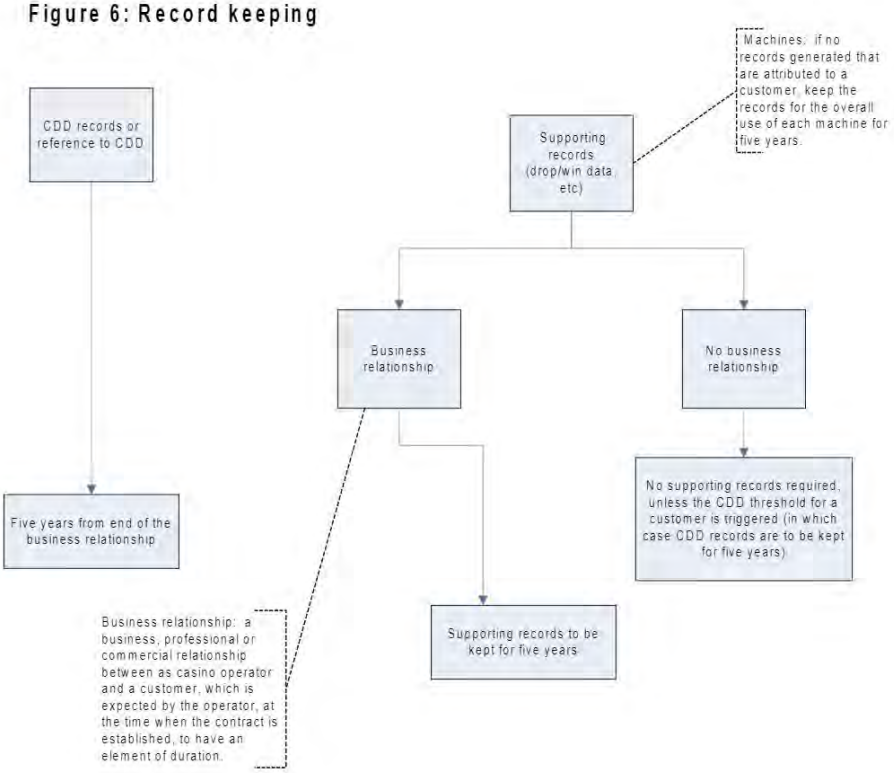
Note:
Risk-based approach – operator analysis of spending behaviours at each premises and an objective assessment made of the likelihood of customers reaching the threshold. Measures then put in place need to capture all customers likely to hit the threshold.

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



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

Figure 6: Record keeping



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

Figure 7: Reasonable grounds to suspect (objective test)

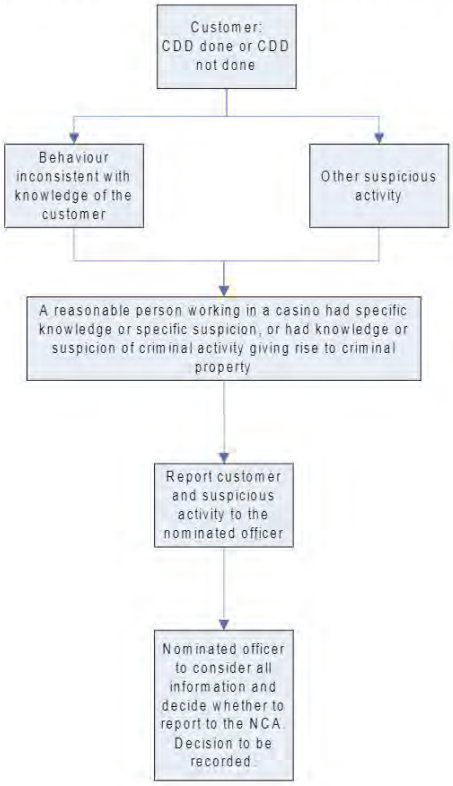


Figure 8: Knowledge or suspicion of money laundering or terrorist financing (subjective test)

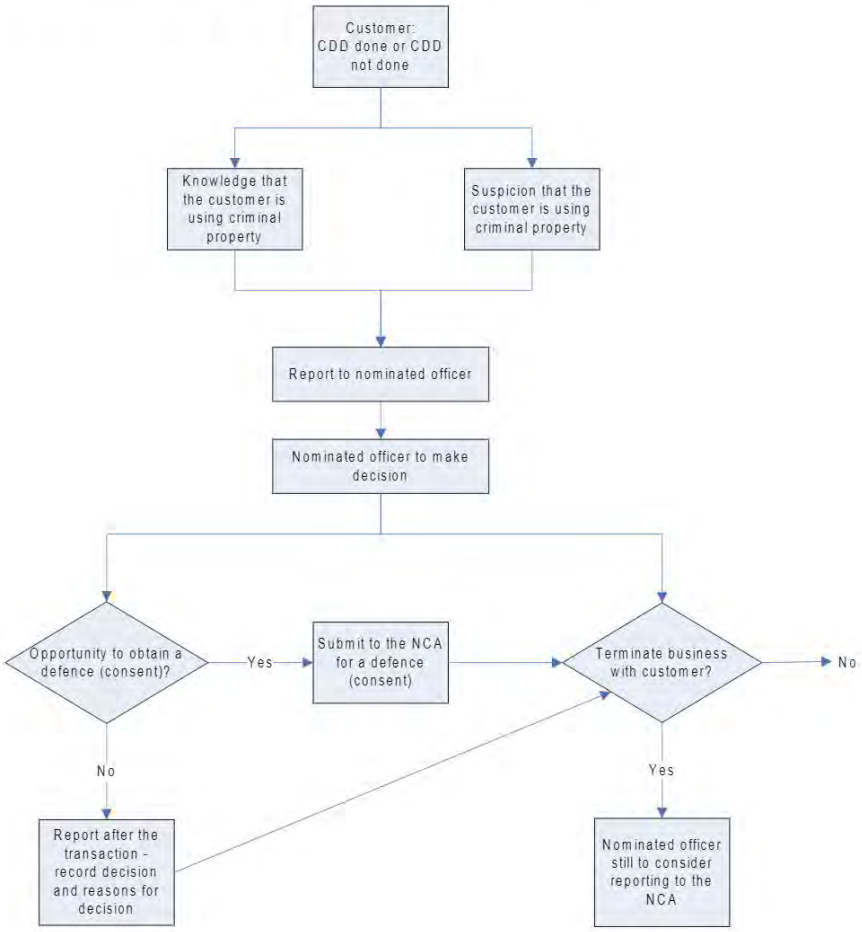


Figure 9: Defence under POCA or Terrorism Act

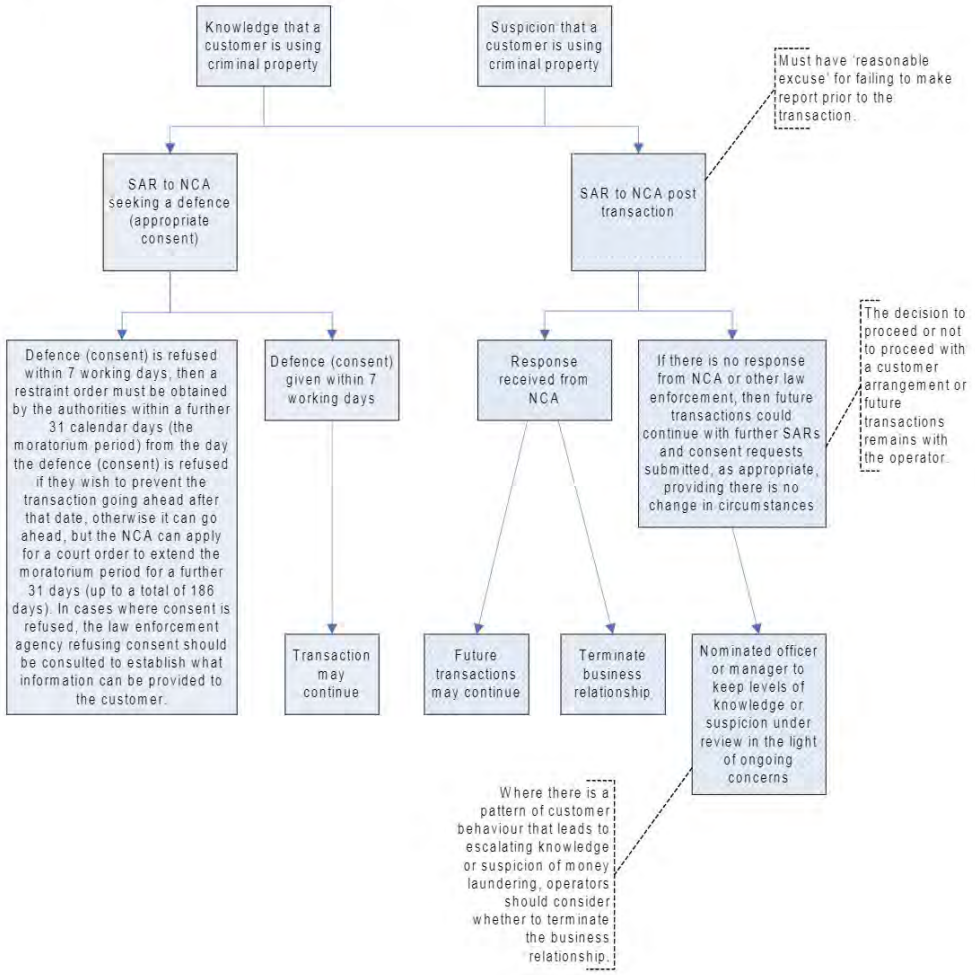
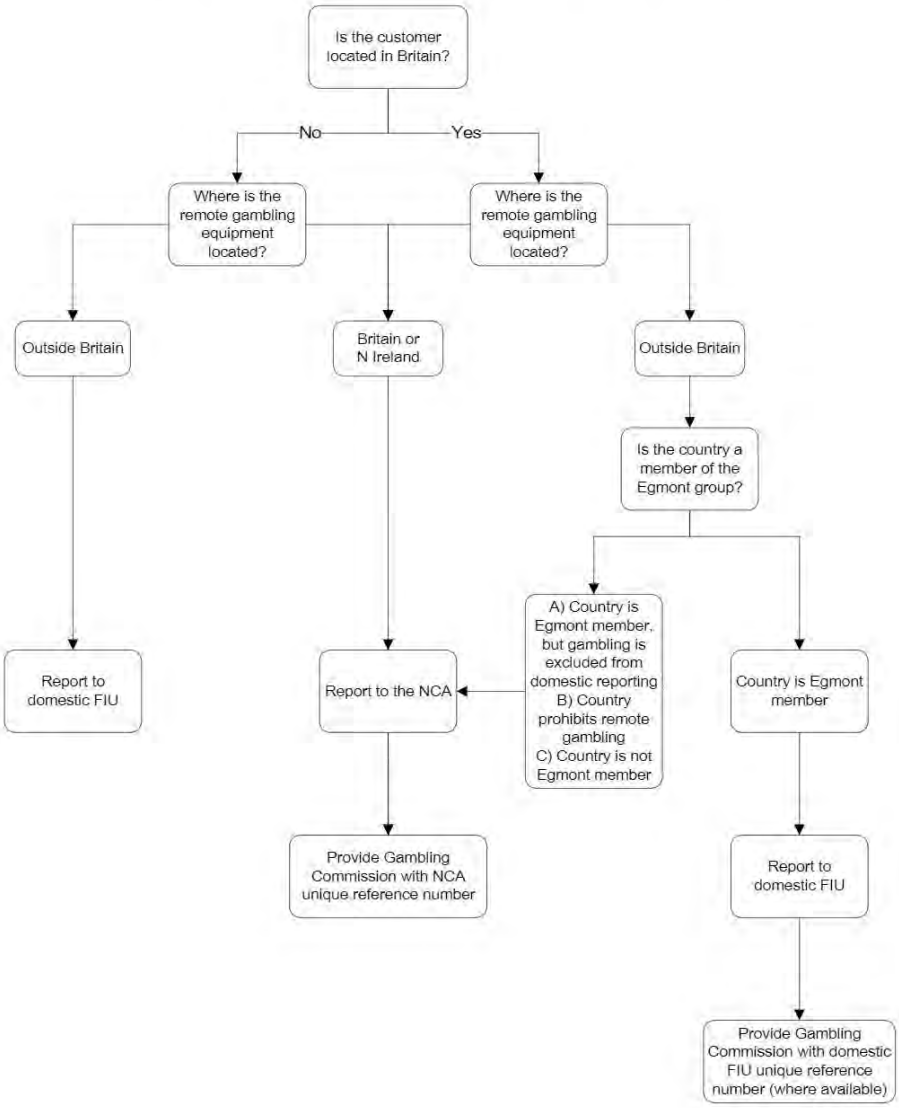


Figure 10: Suspicious activity reporting requirements for remote casinos



Annex A – Glossary of terms

AML	Anti-money laundering.
Beneficial ownership	Beneficial ownership is enjoyed by anyone who has the benefits of ownership of property, but does not apparently own the asset itself. The term is defined in the Regulations.
Business relationship	A business, professional or commercial relationship between a casino operator and a customer, which is expected to have an element of duration.
Business-to-business	A term used to describe commerce transactions between businesses, or the exchange of products, services or information between businesses. In other words, it is business which is conducted between firms, rather than between firms and consumers (or customers).
Casino operators	Firms holding a casino operating licence issued by the Commission.
Criminal spend	In the context of gambling, the use of the proceeds of crime to fund gambling as a leisure activity (also known as lifestyle spend).
CTF	Countering terrorist financing.
Customer tracking	The process of capturing drop and win data for a customer.
Drop/win figures	Data recorded by casinos that covers the total value of chips purchased as well as the total loss or win for a customer over a 24-hour period.
Money laundering	The process by which criminal or 'dirty' money is legitimised or made 'clean', including any action taken to conceal, arrange, use or possess the proceeds of any criminal conduct. Defined in section 340 of POCA.
Non-remote casinos	Casinos licensed to operate commercial casino premises.
Operators	Firms holding an operating licence issued by the Commission.
PFL	Personal functional licence.
POCA	The Proceeds of Crime Act 2002, which is intended to reduce money laundering and the profitability of organised crime through the use of tools such as asset recovery.
PML	Personal management licence.
Proceeds of crime	Property from which a person benefits directly or indirectly, by being party to criminal activity, for example, stolen money, money from drug dealing or property stolen in a burglary or robbery.
Remote casinos	Casinos licensed to offer casino games by means of remote communication.

SAR	A suspicious activity report - the means by which suspicious activity relating to possible money laundering or the financing of terrorism is reported to the NCA under POCA or the Terrorism Act.
Source of funds	Where the funds, money or cash to finance the transaction come from.
Supervisory authorities	Supervisory authorities, which are listed in regulation 7 of the Regulations. The Commission is the supervisory authority for casinos.
The Act	The Gambling Act 2005.
The Commission	The Gambling Commission.
The NCA	The National Crime Agency, which became operational in October 2013. It is a crime-fighting agency with national and international reach that works in partnership with other law enforcement organisations to cut serious and organised crime. The NCA is the organisation to which suspicious activity is reported.
The Regulations	The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.
The Terrorism Act	The Terrorism Act 2000.
Third country	A country which is outside the European Union.
UKFIU	The United Kingdom Financial Intelligence Unit, which is the unit within the NCA that operates the disclosure regime for money laundering.

Finalised guidance

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

July 2017

1 Executive Summary

Legislative Background

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

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

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

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

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

Summary of the Guidance

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

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

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

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

2 Final guidance

Introduction

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

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

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

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

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

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

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

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

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

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

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

What are firms' obligations under the Regulations?

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

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

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

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

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

---

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

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

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

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

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

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

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

---

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

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

Who should be treated as a PEP?

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

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

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

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

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

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

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

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

Who should be considered a family member?

---

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

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

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

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

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

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

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

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

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

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

Do all PEPs pose the same risk?

---

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

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

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

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

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

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

Lower risk indicators – product

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

Lower risk indicators – geographical

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

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

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

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

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

Lower risk indicators – personal and professional

A PEP may pose a lower risk if they:

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

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

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

Higher risk indicator – product

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

Higher risk indicators – geographical

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

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

Higher risk indicators – personal and professional

The following characteristics might suggest a PEP is higher risk:

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

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

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

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

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

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

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

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

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

[37] See Regulation 35

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

What measures may firms take in lower risk situations?

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

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

What measures may firms take in higher risk situations?

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

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

Long-term insurance contracts

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

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

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

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

Beneficial owners of legal entities who are PEPs

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

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

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

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

Exhibit 3

DIRECTIVE 2005/60/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 26 October 2005

on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 47(2), first and third sentences, and Article 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Economic and Social Committee [1],

Having regard to the opinion of the European Central Bank [2],

Acting in accordance with the procedure laid down in Article 251 of the Treaty [3],

Whereas:

(1) Massive flows of dirty money can damage the stability and reputation of the financial sector and threaten the single market, and terrorism shakes the very foundations of our society. In addition to the criminal law approach, a preventive effort via the financial system can produce results.

(2) The soundness, integrity and stability of credit and financial institutions and confidence in the financial system as a whole could be seriously jeopardised by the efforts of criminals and their associates either to disguise the origin of criminal proceeds or to channel lawful or unlawful money for terrorist purposes. In order to avoid Member States' adopting measures to protect their financial systems which could be inconsistent with the functioning of the internal market and with the prescriptions of the rule of law and Community public policy, Community action in this area is necessary.

(3) In order to facilitate their criminal activities, money launderers and terrorist financers could try to take advantage of the freedom of capital movements and the freedom to supply financial services which the integrated financial area entails, if certain coordinating measures are not adopted at Community level.

(4) In order to respond to these concerns in the field of money laundering, Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering [4] was adopted. It required Member States to prohibit money laundering and to oblige the financial sector, comprising credit institutions and a wide range of other financial institutions, to identify their customers, keep appropriate records, establish internal procedures to train staff and guard against money laundering and to report any indications of money laundering to the competent authorities.

(5) Money laundering and terrorist financing are frequently carried out in an international context. Measures adopted solely at national or even Community level, without taking account of international coordination and cooperation, would have very limited effects. The measures adopted by the Community in this field should therefore be consistent with other action undertaken in other international fora. The Community action should continue to take particular account of the Recommendations of the Financial Action Task Force (hereinafter referred to as the FATF), which constitutes the foremost international body active in the fight against money laundering and terrorist financing. Since the FATF Recommendations were substantially revised and expanded in 2003, this Directive should be in line with that new international standard.

(6) The General Agreement on Trade in Services (GATS) allows Members to adopt measures necessary to protect public morals and prevent fraud and adopt measures for prudential reasons, including for ensuring the stability and integrity of the financial system.

(7) Although initially limited to drugs offences, there has been a trend in recent years towards a much wider definition of money laundering based on a broader range of predicate offences. A wider range of predicate offences facilitates the reporting of suspicious transactions and international cooperation in this area. Therefore, the definition of serious crime should be brought into line with the definition of serious crime in Council Framework Decision 2001/500/JHA of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime [5].

---

[1] Opinion delivered on 11 May 2005 (not yet published in the Official Journal).

[2] OJ C 40, 17.2.2005, p. 9.

[3] Opinion of the European Parliament of 26 May 2005 (not yet published in the Official Journal) and Council Decision of 19 September 2005.

[4] OJ L 166, 28.6.1991, p. 77. Directive as amended by Directive 2001/97/EC of the European Parliament and of the Council (OJ L 344, 28.12.2001, p. 76).

[5] OJ L 182, 5.7.2001, p. 1.

(8) Furthermore, the misuse of the financial system to channel criminal or even clean money to terrorist purposes poses a clear risk to the integrity, proper functioning, reputation and stability of the financial system. Accordingly, the preventive measures of this Directive should cover not only the manipulation of money derived from crime but also the collection of money or property for terrorist purposes.

(9) Directive 91/308/EEC, though imposing a customer identification obligation, contained relatively little detail on the relevant procedures. In view of the crucial importance of this aspect of the prevention of money laundering and terrorist financing, it is appropriate, in accordance with the new international standards, to introduce more specific and detailed provisions relating to the identification of the customer and of any beneficial owner and the verification of their identity. To that end a precise definition of 'beneficial owner' is essential. Where the individual beneficiaries of a legal entity or arrangement such as a foundation or trust are yet to be determined, and it is therefore impossible to identify an individual as the beneficial owner, it would suffice to identify the class of persons intended to be the beneficiaries of the foundation or trust. This requirement should not include the identification of the individuals within that class of persons.

(10) The institutions and persons covered by this Directive should, in conformity with this Directive, identify and verify the identity of the beneficial owner. To fulfil this requirement, it should be left to those institutions and persons whether they make use of public records of beneficial owners, ask their clients for relevant data or obtain the information otherwise, taking into account the fact that the extent of such customer due diligence measures relates to the risk of money laundering and terrorist financing, which depends on the type of customer, business relationship, product or transaction.

(11) Credit agreements in which the credit account serves exclusively to settle the loan and the repayment of the loan is effected from an account which was opened in the name of the customer with a credit institution covered by this Directive pursuant to Article 8(1)(a) to (c) should generally be considered as an example of types of less risky transactions.

(12) To the extent that the providers of the property of a legal entity or arrangement have significant control over the use of the property they should be identified as a beneficial owner.

(13) Trust relationships are widely used in commercial products as an internationally recognised feature of the comprehensively supervised wholesale financial markets. An obligation to identify the beneficial owner does not arise from the fact alone that there is a trust relationship in this particular case.

(14) This Directive should also apply to those activities of the institutions and persons covered hereunder which are performed on the Internet.

(15) As the tightening of controls in the financial sector has prompted money launderers and terrorist financers to seek alternative methods for concealing the origin of the proceeds of crime and as such channels can be used for terrorist financing, the anti-money laundering and anti-terrorist financing obligations should cover life insurance intermediaries and trust and company service providers.

(16) Entities already falling under the legal responsibility of an insurance undertaking, and therefore falling within the scope of this Directive, should not be included within the category of insurance intermediary.

(17) Acting as a company director or secretary does not of itself make someone a trust and company service provider. For that reason, the definition covers only those persons that act as a company director or secretary for a third party and by way of business.

(18) The use of large cash payments has repeatedly proven to be very vulnerable to money laundering and terrorist financing. Therefore, in those Member States that allow cash payments above the established threshold, all natural or legal persons trading in goods by way of business should be covered by this Directive when accepting such cash payments. Dealers in high-value goods, such as precious stones or metals, or works of art, and auctioneers are in any event covered by this Directive to the extent that payments to them are made in cash in an amount of EUR 15 000 or more. To ensure effective monitoring of compliance with this Directive by that potentially wide group of institutions and persons, Member States may focus their monitoring activities in particular on those natural and legal persons trading in goods that are exposed to a relatively high risk of money laundering or terrorist financing, in accordance with the principle of risk-based supervision. In view of the different situations in the various Member States, Member States may decide to adopt stricter provisions, in order to properly address the risk involved with large cash payments.

(19) Directive 91/308/EEC brought notaries and other independent legal professionals within the scope of the Community anti-money laundering regime; this coverage should be maintained unchanged in this Directive; these legal professionals, as defined by the Member States, are subject to the provisions of this Directive when participating in financial or corporate transactions, including providing tax advice, where there is the greatest risk of the services of those legal professionals being misused for the purpose of laundering the proceeds of criminal activity or for the purpose of terrorist financing.

(20) Where independent members of professions providing legal advice which are legally recognised and controlled, such as lawyers, are ascertaining the legal position of a client or representing a client in legal proceedings, it would not be appropriate under this Directive to put those legal professionals in respect of these activities under an obligation to report suspicions of money laundering or terrorist financing. There must be exemptions from any obligation to report information obtained either before, during or after judicial proceedings, or in the course of ascertaining the legal position for a client. Thus, legal advice shall remain subject to the obligation of professional secrecy unless the legal counsellor is taking part in money laundering or terrorist financing, the legal advice is provided for money laundering or terrorist financing purposes or the lawyer knows that the client is seeking legal advice for money laundering or terrorist financing purposes.

(21) Directly comparable services need to be treated in the same manner when provided by any of the professionals covered by this Directive. In order to ensure the respect of the rights laid down in the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Treaty on European Union, in the case of auditors, external accountants and tax advisors, who, in some Member States, may defend or represent a client in the context of judicial proceedings or ascertain a client's legal position, the information they obtain in the performance of those tasks should not be subject to the reporting obligations in accordance with this Directive.

(22) It should be recognised that the risk of money laundering and terrorist financing is not the same in every case. In line with a risk-based approach, the principle should be introduced into Community legislation that simplified customer due diligence is allowed in appropriate cases.

(23) The derogation concerning the identification of beneficial owners of pooled accounts held by notaries or other independent legal professionals should be without prejudice to the obligations that those notaries or other independent legal professionals have pursuant to this Directive. Those obligations include the need for such notaries or other independent legal professionals themselves to identify the beneficial owners of the pooled accounts held by them.

(24) Equally, Community legislation should recognise that certain situations present a greater risk of money laundering or terrorist financing. Although the identity and business profile of all customers should be established, there are cases where particularly rigorous customer identification and verification procedures are required.

(25) This is particularly true of business relationships with individuals holding, or having held, important public positions, particularly those from countries where corruption is widespread. Such relationships may expose the financial sector in particular to significant reputational and/or legal risks. The international effort to combat corruption also justifies the need to pay special attention to such cases and to apply the complete normal customer due diligence measures in respect of domestic politically exposed persons or enhanced customer due diligence measures in respect of politically exposed persons residing in another Member State or in a third country.

(26) Obtaining approval from senior management for establishing business relationships should not imply obtaining approval from the board of directors but from the immediate higher level of the hierarchy of the person seeking such approval.

(27) In order to avoid repeated customer identification procedures, leading to delays and inefficiency in business, it is appropriate, subject to suitable safeguards, to allow customers to be introduced whose identification has been carried out elsewhere. Where an institution or person covered by this Directive relies on a third party, the ultimate responsibility for the customer due diligence procedure remains with the institution or person to whom the customer is introduced. The third party, or introducer, also retains his own responsibility for all the requirements in this Directive, including the requirement to report suspicious transactions and maintain records, to the extent that he has a relationship with the customer that is covered by this Directive.

(28) In the case of agency or outsourcing relationships on a contractual basis between institutions or persons covered by this Directive and external natural or legal persons not covered hereby, any anti-money laundering and anti-terrorist financing obligations for those agents or outsourcing service providers as part of the institutions or persons covered by this Directive, may only arise from contract and not from this Directive. The responsibility for complying with this Directive should remain with the institution or person covered hereby.

(29) Suspicious transactions should be reported to the financial intelligence unit (FIU), which serves as a national centre for receiving, analysing and disseminating to the competent authorities suspicious transaction reports and other information regarding potential money laundering or terrorist financing. This should not compel Member States to change their existing reporting systems where the reporting is done through a public prosecutor or other law enforcement authorities, as long as the information is forwarded promptly and unfiltered to FIUs, allowing them to conduct their business properly, including international cooperation with other FIUs.

(30) By way of derogation from the general prohibition on executing suspicious transactions, the institutions and persons covered by this Directive may execute suspicious transactions before informing the competent authorities, where refraining from the execution thereof is impossible or likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation. This, however, should be without prejudice to the international obligations accepted by the Member States to freeze without delay funds or other assets of terrorists, terrorist organisations or those who finance terrorism, in accordance with the relevant United Nations Security Council resolutions.

(31) Where a Member State decides to make use of the exemptions provided for in Article 23(2), it may allow or require the self-regulatory body representing the persons referred to therein not to transmit to the FIU any information obtained from those persons in the circumstances referred to in that Article.

(32) There has been a number of cases of employees who report their suspicions of money laundering being subjected to threats or hostile action. Although this Directive cannot interfere with Member States' judicial procedures, this is a crucial issue for the effectiveness of the anti-money laundering and anti-terrorist financing system. Member States should be aware of this problem and should do whatever they can to protect employees from such threats or hostile action.

(33) Disclosure of information as referred to in Article 28 should be in accordance with the rules on transfer of personal data to third countries as laid down in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1]. Moreover, Article 28 cannot interfere with national data protection and professional secrecy legislation.

(34) Persons who merely convert paper documents into electronic data and are acting under a contract with a credit institution or a financial institution do not fall within the scope of this Directive, nor does any natural or legal person that provides credit or financial institutions solely with a message or other support systems for transmitting funds or with clearing and settlement systems.

(35) Money laundering and terrorist financing are international problems and the effort to combat them should be global. Where Community credit and financial institutions have branches and subsidiaries located in third countries where the legislation in this area is deficient, they should, in order to avoid the application of very different standards within an institution or group of institutions, apply the Community standard or notify the competent authorities of the home Member State if this application is impossible.

(36) It is important that credit and financial institutions should be able to respond rapidly to requests for information on whether they maintain business relationships with named persons. For the purpose of identifying such business relationships in order to be able to provide that information quickly, credit and financial institutions should have effective systems in place which are commensurate with the size and nature of their business. In particular it would be appropriate for credit institutions and larger financial institutions to have electronic systems at their disposal. This provision is of particular importance in the context of procedures leading to measures such as the freezing or seizing of assets (including terrorist assets), pursuant to applicable national or Community legislation with a view to combating terrorism.

[1] OJ L 281, 23.11.1995, p. 31. Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

(37) This Directive establishes detailed rules for customer due diligence, including enhanced customer due diligence for high-risk customers or business relationships, such as appropriate procedures to determine whether a person is a politically exposed person, and certain additional, more detailed requirements, such as the existence of compliance management procedures and policies. All these requirements are to be met by each of the institutions and persons covered by this Directive, while Member States are expected to tailor the detailed implementation of those provisions to the particularities of the various professions and to the differences in scale and size of the institutions and persons covered by this Directive.

(38) In order to ensure that the institutions and others subject to Community legislation in this field remain committed, feedback should, where practicable, be made available to them on the usefulness and follow-up of the reports they present. To make this possible, and to be able to review the effectiveness of their systems to combat money laundering and terrorist financing Member States should keep and improve the relevant statistics.

(39) When registering or licensing a currency exchange office, a trust and company service provider or a casino nationally, competent authorities should ensure that the persons who effectively direct or will direct the business of such entities and the beneficial owners of such entities are fit and proper persons. The criteria for determining whether or not a person is fit and proper should be established in conformity with national law. As a minimum, such criteria should reflect the need to protect such entities from being misused by their managers or beneficial owners for criminal purposes.

(40) Taking into account the international character of money laundering and terrorist financing, coordination and cooperation between FIUs as referred to in Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information [1], including the establishment of an EU FIU-net, should be encouraged to the greatest possible extent. To that end, the Commission should lend such assistance as may be needed to facilitate such coordination, including financial assistance.

(41) The importance of combating money laundering and terrorist financing should lead Member States to lay down effective, proportionate and dissuasive penalties in national law for failure to respect the national provisions adopted pursuant to this Directive. Provision should be made for penalties in respect of natural and legal persons. Since legal persons are often involved in complex money laundering or terrorist financing operations, sanctions should also be adjusted in line with the activity carried on by legal persons.

(42) Natural persons exercising any of the activities referred to in Article 2(1)(3)(a) and (b) within the structure of a legal person, but on an independent basis, should be independently responsible for compliance with the provisions of this Directive, with the exception of Article 35.

(43) Clarification of the technical aspects of the rules laid down in this Directive may be necessary to ensure an effective and sufficiently consistent implementation of this Directive, taking into account the different financial instruments, professions and risks in the different Member States and the technical developments in the fight against money laundering and terrorist financing. The Commission should accordingly be empowered to adopt implementing measures, such as certain criteria for identifying low and high risk situations in which simplified due diligence could suffice or enhanced due diligence would be appropriate, provided that they do not modify the essential elements of this Directive and provided that the Commission acts in accordance with the principles set out herein, after consulting the Committee on the Prevention of Money Laundering and Terrorist Financing.

(44) The measures necessary for the implementation of this Directive should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission [2]. To that end a new Committee on the Prevention of Money Laundering and Terrorist Financing, replacing the Money Laundering Contact Committee set up by Directive 91/308/EEC, should be established.

(45) In view of the very substantial amendments that would need to be made to Directive 91/308/EEC, it should be repealed for reasons of clarity.

(46) Since the objective of this Directive, namely the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of the action, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

[1] OJ L 271, 24.10.2000, p. 4.

[2] OJ L 184, 17.7.1999, p. 23.

(47) In exercising its implementing powers in accordance with this Directive, the Commission should respect the following principles: the need for high levels of transparency and consultation with institutions and persons covered by this Directive and with the European Parliament and the Council; the need to ensure that competent authorities will be able to ensure compliance with the rules consistently; the balance of costs and benefits to institutions and persons covered by this Directive on a long-term basis in any implementing measures; the need to respect the necessary flexibility in the application of the implementing measures in accordance with a risk-sensitive approach; the need to ensure coherence with other Community legislation in this area; the need to protect the Community, its Member States and their citizens from the consequences of money laundering and terrorist financing.

(48) This Directive respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. Nothing in this Directive should be interpreted or implemented in a manner that is inconsistent with the European Convention on Human Rights,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

SUBJECT MATTER, SCOPE AND DEFINITIONS

Article 1

1. Member States shall ensure that money laundering and terrorist financing are prohibited.

2. For the purposes of this Directive, the following conduct, when committed intentionally, shall be regarded as money laundering:

(a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;

(b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or from an act of participation in such activity;

(c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;

(d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points.

3. Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

4. For the purposes of this Directive, 'terrorist financing' means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism ([1]).

5. Knowledge, intent or purpose required as an element of the activities mentioned in paragraphs 2 and 4 may be inferred from objective factual circumstances.

Article 2

1. This Directive shall apply to:

(1) credit institutions;

(2) financial institutions;

(3) the following legal or natural persons acting in the exercise of their professional activities:

(a) auditors, external accountants and tax advisors;

(b) notaries and other independent legal professionals, when they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or execution of transactions for their client concerning the:

(i) buying and selling of real property or business entities;

(ii) managing of client money, securities or other assets;

([1]) OJ L 164, 22.6.2002, p. 3.

(iii) opening or management of bank, savings or securities accounts;

(iv) organisation of contributions necessary for the creation, operation or management of companies;

(v) creation, operation or management of trusts, companies or similar structures;

(c) trust or company service providers not already covered under points (a) or (b);

(d) real estate agents;

(e) other natural or legal persons trading in goods, only to the extent that payments are made in cash in an amount of EUR 15 000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked;

(f) casinos.

2. Member States may decide that legal and natural persons who engage in a financial activity on an occasional or very limited basis and where there is little risk of money laundering or terrorist financing occurring do not fall within the scope of Article 3(1) or (2).

Article 3

For the purposes of this Directive the following definitions shall apply:

(1) 'credit institution' means a credit institution, as defined in the first subparagraph of Article 1(1) of Directive 2000/12/EC of the European Parliament and of the Council of 20 March 2000 relating to the taking up and pursuit of the business of credit institutions [1], including branches within the meaning of Article 1(3) of that Directive located in the Community of credit institutions having their head offices inside or outside the Community;

(2) 'financial institution' means:

(a) an undertaking other than a credit institution which carries out one or more of the operations included in points 2 to 12 and 14 of Annex I to Directive 2000/12/EC, including the activities of currency exchange offices (bureaux de change) and of money transmission or remittance offices;

(b) an insurance company duly authorised in accordance with Directive 2002/83/EC of the European Parliament and of the Council of 5 November 2002 concerning life assurance [2], insofar as it carries out activities covered by that Directive;

(c) an investment firm as defined in point 1 of Article 4(1) of Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments [3];

(d) a collective investment undertaking marketing its units or shares;

(e) an insurance intermediary as defined in Article 2(5) of Directive 2002/92/EC of the European Parliament and of the Council of 9 December 2002 on insurance mediation [4], with the exception of intermediaries as mentioned in Article 2(7) of that Directive, when they act in respect of life insurance and other investment related services;

(f) branches, when located in the Community, of financial institutions as referred to in points (a) to (e), whose head offices are inside or outside the Community;

(3) 'property' means assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets;

(4) 'criminal activity' means any kind of criminal involvement in the commission of a serious crime;

(5) 'serious crimes' means, at least:

(a) acts as defined in Articles 1 to 4 of Framework Decision 2002/475/JHA;

(b) any of the offences defined in Article 3(1)(a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances;

(c) the activities of criminal organisations as defined in Article 1 of Council Joint Action 98/733/JHA of 21 December 1998 on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union [5];

(d) fraud, at least serious, as defined in Article 1(1) and Article 2 of the Convention on the Protection of the European Communities' Financial Interests [6];

(e) corruption;

(f) all offences which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards those States which have a minimum threshold for offences in their legal system, all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months;

[1] OJ L 126, 26.5.2000, p. 1. Directive as last amended by Directive 2005/1/EC (OJ L 79, 24.3.2005, p. 9).
[2] OJ L 345, 19.12.2002, p. 1. Directive as last amended by Directive 2005/1/EC.
[3] OJ L 145, 30.4.2004, p. 1.
[4] OJ L 9, 15.1.2003, p. 3.
[5] OJ L 351, 29.12.1998, p. 1.
[6] OJ C 316, 27.11.1995, p. 49.

(6) 'beneficial owner' means the natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted. The beneficial owner shall at least include:

(a) in the case of corporate entities:

(i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards; a percentage of 25 % plus one share shall be deemed sufficient to meet this criterion;

(ii) the natural person(s) who otherwise exercises control over the management of a legal entity:

(b) in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:

(i) where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 25 % or more of the property of a legal arrangement or entity;

(ii) where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;

(iii) the natural person(s) who exercises control over 25 % or more of the property of a legal arrangement or entity;

(7) 'trust and company service providers' means any natural or legal person which by way of business provides any of the following services to third parties:

(a) forming companies or other legal persons;

(b) acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

(c) providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement;

(d) acting as or arranging for another person to act as a trustee of an express trust or a similar legal arrangement;

(e) acting as or arranging for another person to act as a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements in conformity with Community legislation or subject to equivalent international standards;

(8) 'politically exposed persons' means natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons;

(9) 'business relationship' means a business, professional or commercial relationship which is connected with the professional activities of the institutions and persons covered by this Directive and which is expected, at the time when the contact is established, to have an element of duration;

(10) 'shell bank' means a credit institution, or an institution engaged in equivalent activities, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.

Article 4

1. Member States shall ensure that the provisions of this Directive are extended in whole or in part to professions and to categories of undertakings, other than the institutions and persons referred to in Article 2(1), which engage in activities which are particularly likely to be used for money laundering or terrorist financing purposes.

2. Where a Member State decides to extend the provisions of this Directive to professions and to categories of undertakings other than those referred to in Article 2(1), it shall inform the Commission thereof.

Article 5

The Member States may adopt or retain in force stricter provisions in the field covered by this Directive to prevent money laundering and terrorist financing.

CHAPTER II

CUSTOMER DUE DILIGENCE

SECTION 1

General provisions

Article 6

Member States shall prohibit their credit and financial institutions from keeping anonymous accounts or anonymous passbooks. By way of derogation from Article 9(6), Member States shall in all cases require that the owners and beneficiaries of existing anonymous accounts or anonymous passbooks be made the subject of customer due diligence measures as soon as possible and in any event before such accounts or passbooks are used in any way.

Article 7

The institutions and persons covered by this Directive shall apply customer due diligence measures in the following cases:

(a) when establishing a business relationship;

(b) when carrying out occasional transactions amounting to EUR 15 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(c) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;

(d) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

Article 8

1. Customer due diligence measures shall comprise:

(a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

(b) identifying, where applicable, the beneficial owner and taking risk-based and adequate measures to verify his identity so that the institution or person covered by this Directive is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the customer;

(c) obtaining information on the purpose and intended nature of the business relationship;

(d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's or person's knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date.

2. The institutions and persons covered by this Directive shall apply each of the customer due diligence requirements set out in paragraph 1, but may determine the extent of such measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction. The institutions and persons covered by this Directive shall be able to demonstrate to the competent authorities mentioned in Article 37, including self-regulatory bodies, that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.

Article 9

1. Member States shall require that the verification of the identity of the customer and the beneficial owner takes place before the establishment of a business relationship or the carrying-out of the transaction.

2. By way of derogation from paragraph 1, Member States may allow the verification of the identity of the customer and the beneficial owner to be completed during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing occurring. In such situations these procedures shall be completed as soon as practicable after the initial contact.

3. By way of derogation from paragraphs 1 and 2, Member States may, in relation to life insurance business, allow the verification of the identity of the beneficiary under the policy to take place after the business relationship has been established. In that case, verification shall take place at or before the time of payout or at or before the time the beneficiary intends to exercise rights vested under the policy.

4. By way of derogation from paragraphs 1 and 2, Member States may allow the opening of a bank account provided that there are adequate safeguards in place to ensure that transactions are not carried out by the customer or on its behalf until full compliance with the aforementioned provisions is obtained.

5. Member States shall require that, where the institution or person concerned is unable to comply with points (a), (b) and (c) of Article 8(1), it may not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, or shall terminate the business relationship, and shall consider making a report to the financial intelligence unit (FIU) in accordance with Article 22 in relation to the customer.

Member States shall not be obliged to apply the previous subparagraph in situations when notaries, independent legal professionals, auditors, external accountants and tax advisors are in the course of ascertaining the legal position for their client or performing their task of defending or representing that client in, or concerning judicial proceedings, including advice on instituting or avoiding proceedings.

6. Member States shall require that institutions and persons covered by this Directive apply the customer due diligence procedures not only to all new customers but also at appropriate times to existing customers on a risk-sensitive basis.

Article 10

1. Member States shall require that all casino customers be identified and their identity verified if they purchase or exchange gambling chips with a value of EUR 2 000 or more.

2. Casinos subject to State supervision shall be deemed in any event to have satisfied the customer due diligence requirements if they register, identify and verify the identity of their customers immediately on or before entry, regardless of the amount of gambling chips purchased.

SECTION 2

Simplified customer due diligence

Article 11

1. By way of derogation from Articles 7(a), (b) and (d), 8 and 9(1), the institutions and persons covered by this Directive shall not be subject to the requirements provided for in those Articles where the customer is a credit or financial institution covered by this Directive, or a credit or financial institution situated in a third country which imposes requirements equivalent to those laid down in this Directive and supervised for compliance with those requirements.

2. By way of derogation from Articles 7(a), (b) and (d), 8 and 9(1) Member States may allow the institutions and persons covered by this Directive not to apply customer due diligence in respect of:

(a) listed companies whose securities are admitted to trading on a regulated market within the meaning of Directive 2004/39/EC in one or more Member States and listed companies from third countries which are subject to disclosure requirements consistent with Community legislation;

(b) beneficial owners of pooled accounts held by notaries and other independent legal professionals from the Member States, or from third countries provided that they are subject to requirements to combat money laundering or terrorist financing consistent with international standards and are supervised for compliance with those requirements and provided that the information on the identity of the beneficial owner is available, on request, to the institutions that act as depository institutions for the pooled accounts;

(c) domestic public authorities,

or in respect of any other customer representing a low risk of money laundering or terrorist financing which meets the technical criteria established in accordance with Article 40(1)(b).

3. In the cases mentioned in paragraphs 1 and 2, institutions and persons covered by this Directive shall in any case gather sufficient information to establish if the customer qualifies for an exemption as mentioned in these paragraphs.

4. The Member States shall inform each other and the Commission of cases where they consider that a third country meets the conditions laid down in paragraphs 1 or 2 or in other situations which meet the technical criteria established in accordance with Article 40(1)(b).

5. By way of derogation from Articles 7(a), (b) and (d), 8 and 9(1), Member States may allow the institutions and persons covered by this Directive not to apply customer due diligence in respect of:

(a) life insurance policies where the annual premium is no more than EUR 1 000 or the single premium is no more than EUR 2 500;

(b) insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral;

(c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;

(d) electronic money, as defined in Article 1(3)(b) of Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions ([1]), where, if the device cannot be recharged, the maximum amount stored in the device is no more than EUR 150, or where, if the device can be recharged, a limit of EUR 2 500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1 000 or more is redeemed in that same calendar year by the bearer as referred to in Article 3 of Directive 2000/46/EC,

or in respect of any other product or transaction representing a low risk of money laundering or terrorist financing which meets the technical criteria established in accordance with Article 40(1)(b).

Article 12

Where the Commission adopts a decision pursuant to Article 40(4), the Member States shall prohibit the institutions and persons covered by this Directive from applying simplified due diligence to credit and financial institutions or listed companies from the third country concerned or other entities following from situations which meet the technical criteria established in accordance with Article 40(1)(b).

SECTION 3

Enhanced customer due diligence

Article 13

1. Member States shall require the institutions and persons covered by this Directive to apply, on a risk-sensitive basis, enhanced customer due diligence measures, in addition to the measures referred to in Articles 7, 8 and 9(6), in situations which by their nature can present a higher risk of money laundering or terrorist financing, and at least in the situations set out in paragraphs 2, 3, 4 and in other situations representing a high risk of money laundering or terrorist financing which meet the technical criteria established in accordance with Article 40(1)(c).

2. Where the customer has not been physically present for identification purposes, Member States shall require those institutions and persons to take specific and adequate measures to compensate for the higher risk, for example by applying one or more of the following measures:

(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 requiring confirmatory certification by a credit or financial institution covered by this Directive;

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

3. In respect of cross-frontier correspondent banking relationships with respondent institutions from third countries, Member States shall require their credit institutions to:

(a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision;

(b) assess the respondent institution's anti-money laundering and anti-terrorist financing controls;

(c) obtain approval from senior management before establishing new correspondent banking relationships;

(d) document the respective responsibilities of each institution;

(e) with respect to payable-through accounts, be satisfied that the respondent credit institution has verified the identity of and performed ongoing due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer due diligence data to the correspondent institution, upon request.

4. In respect of transactions or business relationships with politically exposed persons residing in another Member State or in a third country, Member States shall require those institutions and persons covered by this Directive to:

(a) have appropriate risk-based procedures to determine whether the customer is a politically exposed person;

(b) have senior management approval for establishing business relationships with such customers;

(c) take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction;

(d) conduct enhanced ongoing monitoring of the business relationship.

([1]) OJ L 275, 27.10.2000, p. 39.

5. Member States shall prohibit credit institutions from entering into or continuing a correspondent banking relationship with a shell bank and shall require that credit institutions take appropriate measures to ensure that they do not engage in or continue correspondent banking relationships with a bank that is known to permit its accounts to be used by a shell bank.

6. Member States shall ensure that the institutions and persons covered by this Directive pay special attention to any money laundering or terrorist financing threat that may arise from products or transactions that might favour anonymity, and take measures, if needed, to prevent their use for money laundering or terrorist financing purposes.

SECTION 4

Performance by third parties

Article 14

Member States may permit the institutions and persons covered by this Directive to rely on third parties to meet the requirements laid down in Article 8(1)(a) to (c). However, the ultimate responsibility for meeting those requirements shall remain with the institution or person covered by this Directive which relies on the third party.

Article 15

1. Where a Member State permits credit and financial institutions referred to in Article 2(1)(1) or (2) situated in its territory to be relied on as a third party domestically, that Member State shall in any case permit institutions and persons referred to in Article 2(1) situated in its territory to recognise and accept, in accordance with the provisions laid down in Article 14, the outcome of the customer due diligence requirements laid down in Article 8(1)(a) to (c), carried out in accordance with this Directive by an institution referred to in Article 2(1)(1) or (2) in another Member State, with the exception of currency exchange offices and money transmission or remittance offices, and meeting the requirements laid down in Articles 16 and 18, even if the documents or data on which these requirements have been based are different to those required in the Member State to which the customer is being referred.

2. Where a Member State permits currency exchange offices and money transmission or remittance offices referred to in Article 3(2)(a) situated in its territory to be relied on as a third party domestically, that Member State shall in any case permit them to recognise and accept, in accordance with Article 14, the outcome of the customer due diligence requirements laid down in Article 8(1)(a) to (c), carried out in accordance with this Directive by the same category of institution in another Member State and meeting the requirements laid down in Articles 16 and 18, even if the documents or data on which these requirements have been based are different to those required in the Member State to which the customer is being referred.

3. Where a Member State permits persons referred to in Article 2(1)(3)(a) to (c) situated in its territory to be relied on as a third party domestically, that Member State shall in any case permit them to recognise and accept, in accordance with Article 14, the outcome of the customer due diligence requirements laid down in Article 8(1)(a) to (c), carried out in accordance with this Directive by a person referred to in Article 2(1)(3)(a) to (c) in another Member State and meeting the requirements laid down in Articles 16 and 18, even if the documents or data on which these requirements have been based are different to those required in the Member State to which the customer is being referred.

Article 16

1. For the purposes of this Section, 'third parties' shall mean institutions and persons who are listed in Article 2, or equivalent institutions and persons situated in a third country, who meet the following requirements:

(a) they are subject to mandatory professional registration, recognised by law;

(b) they apply customer due diligence requirements and record keeping requirements as laid down or equivalent to those laid down in this Directive and their compliance with the requirements of this Directive is supervised in accordance with Section 2 of Chapter V, or they are situated in a third country which imposes equivalent requirements to those laid down in this Directive.

2. Member States shall inform each other and the Commission of cases where they consider that a third country meets the conditions laid down in paragraph 1(b).

Article 17

Where the Commission adopts a decision pursuant to Article 40(4), Member States shall prohibit the institutions and persons covered by this Directive from relying on third parties from the third country concerned to meet the requirements laid down in Article 8(1)(a) to (c).

Article 18

1. Third parties shall make information requested in accordance with the requirements laid down in Article 8(1)(a) to (c) immediately available to the institution or person covered by this Directive to which the customer is being referred.

2. Relevant copies of identification and verification data and other relevant documentation on the identity of the customer or the beneficial owner shall immediately be forwarded, on request, by the third party to the institution or person covered by this Directive to which the customer is being referred.

Article 19

This Section shall not apply to outsourcing or agency relationships where, on the basis of a contractual arrangement, the outsourcing service provider or agent is to be regarded as part of the institution or person covered by this Directive.

CHAPTER III

REPORTING OBLIGATIONS

SECTION 1

General provisions

Article 20

Member States shall require that the institutions and persons covered by this Directive pay special attention to any activity which they regard as particularly likely, by its nature, to be related to money laundering or terrorist financing and in particular complex or unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose.

Article 21

1. Each Member State shall establish a FIU in order effectively to combat money laundering and terrorist financing.

2. That FIU shall be established as a central national unit. It shall be responsible for receiving (and to the extent permitted, requesting), analysing and disseminating to the competent authorities, disclosures of information which concern potential money laundering, potential terrorist financing or are required by national legislation or regulation. It shall be provided with adequate resources in order to fulfil its tasks.

3. Member States shall ensure that the FIU has access, directly or indirectly, on a timely basis, to the financial, administrative and law enforcement information that it requires to properly fulfil its tasks.

Article 22

1. Member States shall require the institutions and persons covered by this Directive, and where applicable their directors and employees, to cooperate fully:

(a) by promptly informing the FIU, on their own initiative, where the institution or person covered by this Directive knows, suspects or has reasonable grounds to suspect that money laundering or terrorist financing is being or has been committed or attempted;

(b) by promptly furnishing the FIU, at its request, with all necessary information, in accordance with the procedures established by the applicable legislation.

2. The information referred to in paragraph 1 shall be forwarded to the FIU of the Member State in whose territory the institution or person forwarding the information is situated. The person or persons designated in accordance with the procedures provided for in Article 34 shall normally forward the information.

Article 23

1. By way of derogation from Article 22(1), Member States may, in the case of the persons referred to in Article 2(1)(3)(a) and (b), designate an appropriate self-regulatory body of the profession concerned as the authority to be informed in the first instance in place of the FIU. Without prejudice to paragraph 2, the designated self-regulatory body shall in such cases forward the information to the FIU promptly and unfiltered.

2. Member States shall not be obliged to apply the obligations laid down in Article 22(1) to notaries, independent legal professionals, auditors, external accountants and tax advisors with regard to information they receive from or obtain on one of their clients, in the course of ascertaining the legal position for their client or performing their task of defending or representing that client in, or concerning judicial proceedings, including advice on instituting or avoiding proceedings, whether such information is received or obtained before, during or after such proceedings.

Article 24

1. Member States shall require the institutions and persons covered by this Directive to refrain from carrying out transactions which they know or suspect to be related to money laundering or terrorist financing until they have completed the necessary action in accordance with Article 22(1)(a). In conformity with the legislation of the Member States, instructions may be given not to carry out the transaction.

2. Where such a transaction is suspected of giving rise to money laundering or terrorist financing and where to refrain in such manner is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation, the institutions and persons concerned shall inform the FIU immediately afterwards.

Article 25

1. Member States shall ensure that if, in the course of inspections carried out in the institutions and persons covered by this Directive by the competent authorities referred to in Article 37, or in any other way, those authorities discover facts that could be related to money laundering or terrorist financing, they shall promptly inform the FIU.

2. Member States shall ensure that supervisory bodies empowered by law or regulation to oversee the stock, foreign exchange and financial derivatives markets inform the FIU if they discover facts that could be related to money laundering or terrorist financing.

Article 26

The disclosure in good faith as foreseen in Articles 22(1) and 23 by an institution or person covered by this Directive or by an employee or director of such an institution or person of the information referred to in Articles 22 and 23 shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the institution or person or its directors or employees in liability of any kind.

Article 27

Member States shall take all appropriate measures in order to protect employees of the institutions or persons covered by this Directive who report suspicions of money laundering or terrorist financing either internally or to the FIU from being exposed to threats or hostile action.

SECTION 2

Prohibition of disclosure

Article 28

1. The institutions and persons covered by this Directive and their directors and employees shall not disclose to the customer concerned or to other third persons the fact that information has been transmitted in accordance with Articles 22 and 23 or that a money laundering or terrorist financing investigation is being or may be carried out.

2. The prohibition laid down in paragraph 1 shall not include disclosure to the competent authorities referred to in Article 37, including the self-regulatory bodies, or disclosure for law enforcement purposes.

3. The prohibition laid down in paragraph 1 shall not prevent disclosure between institutions from Member States, or from third countries provided that they meet the conditions laid down in Article 11(1), belonging to the same group as defined by Article 2(12) of Directive 2002/87/EC of the European Parliament and of the Council of 16 December 2002 on the supplementary supervision of credit institutions, insurance undertakings and investment firms in a financial conglomerate ([1]).

4. The prohibition laid down in paragraph 1 shall not prevent disclosure between persons referred to in Article 2(1)(3)(a) and (b) from Member States, or from third countries which impose requirements equivalent to those laid down in this Directive, who perform their professional activities, whether as employees or not, within the same legal person or a network. For the purposes of this Article, a 'network' means the larger structure to which the person belongs and which shares common ownership, management or compliance control.

5. For institutions or persons referred to in Article 2(1)(1), (2) and (3)(a) and (b) in cases related to the same customer and the same transaction involving two or more institutions or persons, the prohibition laid down in paragraph 1 shall not prevent disclosure between the relevant institutions or persons provided that they are situated in a Member State, or in a third country which imposes requirements equivalent to those laid down in this Directive, and that they are from the same professional category and are subject to equivalent obligations as regards professional secrecy and personal data protection. The information exchanged shall be used exclusively for the purposes of the prevention of money laundering and terrorist financing.

6. Where the persons referred to in Article 2(1)(3)(a) and (b) seek to dissuade a client from engaging in illegal activity, this shall not constitute a disclosure within the meaning of the paragraph 1.

7. The Member States shall inform each other and the Commission of cases where they consider that a third country meets the conditions laid down in paragraphs 3, 4 or 5.

Article 29

Where the Commission adopts a decision pursuant to Article 40(4), the Member States shall prohibit the disclosure between institutions and persons covered by this Directive and institutions and persons from the third country concerned.

([1]) OJ L 35, 11.2.2003, p. 1.

CHAPTER IV

RECORD KEEPING AND STATISTICAL DATA

Article 30

Member States shall require the institutions and persons covered by this Directive to keep the following documents and information for use in any investigation into, or analysis of, possible money laundering or terrorist financing by the FIU or by other competent authorities in accordance with national law:

(a) in the case of the customer due diligence, a copy or the references of the evidence required, for a period of at least five years after the business relationship with their customer has ended;

(b) in the case of business relationships and transactions, the supporting evidence and records, consisting of the original documents or copies admissible in court proceedings under the applicable national legislation for a period of at least five years following the carrying-out of the transactions or the end of the business relationship.

Article 31

1. Member States shall require the credit and financial institutions covered by this Directive to apply, where applicable, in their branches and majority-owned subsidiaries located in third countries measures at least equivalent to those laid down in this Directive with regard to customer due diligence and record keeping.

Where the legislation of the third country does not permit application of such equivalent measures, the Member States shall require the credit and financial institutions concerned to inform the competent authorities of the relevant home Member State accordingly.

2. Member States and the Commission shall inform each other of cases where the legislation of the third country does not permit application of the measures required under the first subparagraph of paragraph 1 and coordinated action could be taken to pursue a solution.

3. Member States shall require that, where the legislation of the third country does not permit application of the measures required under the first subparagraph of paragraph 1, credit or financial institutions take additional measures to effectively handle the risk of money laundering or terrorist financing.

Article 32

Member States shall require that their credit and financial institutions have systems in place that enable them to respond fully and rapidly to enquiries from the FIU, or from other authorities, in accordance with their national law, as to whether they maintain or have maintained during the previous five years a business relationship with specified natural or legal persons and on the nature of that relationship.

Article 33

1. Member States shall ensure that they are able to review the effectiveness of their systems to combat money laundering or terrorist financing by maintaining comprehensive statistics on matters relevant to the effectiveness of such systems.

2. Such statistics shall as a minimum cover the number of suspicious transaction reports made to the FIU, the follow-up given to these reports and indicate on an annual basis the number of cases investigated, the number of persons prosecuted, the number of persons convicted for money laundering or terrorist financing offences and how much property has been frozen, seized or confiscated.

3. Member States shall ensure that a consolidated review of these statistical reports is published.

CHAPTER V

ENFORCEMENT MEASURES

SECTION 1

Internal procedures, training and feedback

Article 34

1. Member States shall require that the institutions and persons covered by this Directive establish adequate and appropriate policies and procedures of customer due diligence, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication in order to forestall and prevent operations related to money laundering or terrorist financing.

2. Member States shall require that credit and financial institutions covered by this Directive communicate relevant policies and procedures where applicable to branches and majority-owned subsidiaries in third countries.

Article 35

1. Member States shall require that the institutions and persons covered by this Directive take appropriate measures so that their relevant employees are aware of the provisions in force on the basis of this Directive.

These measures shall include participation of their relevant employees in special ongoing training programmes to help them recognise operations which may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases.

Where a natural person falling within any of the categories listed in Article 2(1)(3) performs his professional activities as an employee of a legal person, the obligations in this Section shall apply to that legal person rather than to the natural person.

2. Member States shall ensure that the institutions and persons covered by this Directive have access to up-to-date information on the practices of money launderers and terrorist financers and on indications leading to the recognition of suspicious transactions.

3. Member States shall ensure that, wherever practicable, timely feedback on the effectiveness of and follow-up to reports of suspected money laundering or terrorist financing is provided.

SECTION 2

Supervision

Article 36

1. Member States shall provide that currency exchange offices and trust and company service providers shall be licensed or registered and casinos be licensed in order to operate their business legally. Without prejudice to future Community legislation, Member States shall provide that money transmission or remittance offices shall be licensed or registered in order to operate their business legally.

2. Member States shall require competent authorities to refuse licensing or registration of the entities referred to in paragraph 1 if they are not satisfied that the persons who effectively direct or will direct the business of such entities or the beneficial owners of such entities are fit and proper persons.

Article 37

1. Member States shall require the competent authorities at least to effectively monitor and to take the necessary measures with a view to ensuring compliance with the requirements of this Directive by all the institutions and persons covered by this Directive.

2. Member States shall ensure that the competent authorities have adequate powers, including the power to compel the production of any information that is relevant to monitoring compliance and perform checks, and have adequate resources to perform their functions.

3. In the case of credit and financial institutions and casinos, competent authorities shall have enhanced supervisory powers, notably the possibility to conduct on-site inspections.

4. In the case of the natural and legal persons referred to in Article 2(1)(3)(a) to (e), Member States may allow the functions referred to in paragraph 1 to be performed on a risk-sensitive basis.

5. In the case of the persons referred to in Article 2(1)(3)(a) and (b), Member States may allow the functions referred to in paragraph 1 to be performed by self-regulatory bodies, provided that they comply with paragraph 2.

SECTION 3

Cooperation

Article 38

The Commission shall lend such assistance as may be needed to facilitate coordination, including the exchange of information between FIUs within the Community.

SECTION 4

Penalties

Article 39

1. Member States shall ensure that natural and legal persons covered by this Directive can be held liable for infringements of the national provisions adopted pursuant to this Directive. The penalties must be effective, proportionate and dissuasive.

2. Without prejudice to the right of Member States to impose criminal penalties, Member States shall ensure, in conformity with their national law, that the appropriate administrative measures can be taken or administrative sanctions can be imposed against credit and financial institutions for infringements of the national provisions adopted pursuant to this Directive. Member States shall ensure that these measures or sanctions are effective, proportionate and dissuasive.

3. In the case of legal persons, Member States shall ensure that at least they can be held liable for infringements referred to in paragraph 1 which are committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:

(a) a power of representation of the legal person;

(b) an authority to take decisions on behalf of the legal person, or

(c) an authority to exercise control within the legal person.

4. In addition to the cases already provided for in paragraph 3, Member States shall ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 3 has made possible the commission of the infringements referred to in paragraph 1 for the benefit of a legal person by a person under its authority.

CHAPTER VI

IMPLEMENTING MEASURES

Article 40

1. In order to take account of technical developments in the fight against money laundering or terrorist financing and to ensure uniform implementation of this Directive, the Commission may, in accordance with the procedure referred to in Article 41(2), adopt the following implementing measures:

(a) clarification of the technical aspects of the definitions in Article 3(2)(a) and (d), (6), (7), (8), (9) and (10);

(b) establishment of technical criteria for assessing whether situations represent a low risk of money laundering or terrorist financing as referred to in Article 11(2) and (5);

(c) establishment of technical criteria for assessing whether situations represent a high risk of money laundering or terrorist financing as referred to in Article 13;

(d) establishment of technical criteria for assessing whether, in accordance with Article 2(2), it is justified not to apply this Directive to certain legal or natural persons carrying out a financial activity on an occasional or very limited basis.

2. In any event, the Commission shall adopt the first implementing measures to give effect to paragraphs 1(b) and 1(d) by 15 June 2006.

3. The Commission shall, in accordance with the procedure referred to in Article 41(2), adapt the amounts referred to in Articles 2(1)(3)(e), 7(b), 10(1) and 11(5)(a) and (d) taking into account Community legislation, economic developments and changes in international standards.

4. Where the Commission finds that a third country does not meet the conditions laid down in Article 11(1) or (2), Article 28(3), (4) or (5), or in the measures established in accordance with paragraph 1(b) of this Article or in Article 16(1)(b), or that the legislation of that third country does not permit application of the measures required under the first subparagraph of Article 31(1), it shall adopt a decision so stating in accordance with the procedure referred to in Article 41(2).

Article 41

1. The Commission shall be assisted by a Committee on the Prevention of Money Laundering and Terrorist Financing, hereinafter 'the Committee'.

2. Where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof and provided that the implementing measures adopted in accordance with this procedure do not modify the essential provisions of this Directive.

The period laid down in Article 5(6) of Decision 1999/468/EC shall be set at three months.

3. The Committee shall adopt its Rules of Procedure.

4. Without prejudice to the implementing measures already adopted, the implementation of the provisions of this Directive concerning the adoption of technical rules and decisions in accordance with the procedure referred to in paragraph 2 shall be suspended four years after the entry into force of this Directive. On a proposal from the Commission, the European Parliament and the Council may renew the provisions concerned in accordance with the procedure laid down in Article 251 of the Treaty and, to that end, shall review them prior to the expiry of the four-year period.

CHAPTER VII

FINAL PROVISIONS

Article 42

By 15 December 2009, and at least at three-yearly intervals thereafter, the Commission shall draw up a report on the implementation of this Directive and submit it to the European Parliament and the Council. For the first such report, the Commission shall include a specific examination of the treatment of lawyers and other independent legal professionals.

Article 43

By 15 December 2010, the Commission shall present a report to the European Parliament and to the Council on the threshold percentages in Article 3(6), paying particular attention to the possible expediency and consequences of a reduction of the percentage in points (a)(i), (b)(i) and (b)(iii) of Article 3(6) from 25 % to 20 %. On the basis of the report the Commission may submit a proposal for amendments to this Directive.

Article 44

Directive 91/308/EEC is hereby repealed.

References made to the repealed Directive shall be construed as being made to this Directive and should be read in accordance with the correlation table set out in the Annex.

Article 45

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 15 December 2007. They shall forthwith communicate to the Commission the text of those provisions together with a table showing how the provisions of this Directive correspond to the national provisions adopted.

When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 46

This Directive shall enter into force on the 20th day after its publication in the *Official Journal of the European Union*.

Article 47

This Directive is addressed to the Member States.

Done at Strasbourg, 26 October 2005.

For the European Parliament	*For the Council*
The President	*The President*
J. BORRELL FONTELLES	D. ALEXANDER

ANNEX

CORRELATION TABLE

This Directive	Directive 91/308/EEC
Article 1(1)	Article 2
Article 1(2)	Article 1(C)
Article 1(2)(a)	Article 1(C) first point
Article 1(2)(b)	Article 1(C) second point
Article 1(2)(c)	Article 1(C) third point
Article 1(2)(d)	Article 1(C) fourth point
Article 1(3)	Article 1(C), third paragraph
Article 1(4)	
Article 1(5)	Article 1(C), second paragraph
Article 2(1)(1)	Article 2a(1)
Article 2(1)(2)	Article 2a(2)
Article 2(1)(3)(a), (b) and (d) to (f)	Article 2a(3) to (7)
Article 2(1)(3)(c)	
Article 2(2)	
Article 3(1)	Article 1(A)
Article 3(2)(a)	Article 1(B)(1)
Article 3(2)(b)	Article 1(B)(2)
Article 3(2)(c)	Article 1(B)(3)
Article 3(2)(d)	Article 1(B)(4)
Article 3(2)(e)	
Article 3(2)(f)	Article 1(B), second paragraph
Article 3(3)	Article 1(D)
Article 3(4)	Article 1(E), first paragraph
Article 3(5)	Article 1(E), second paragraph
Article 3(5)(a)	
Article 3(5)(b)	Article 1(E), first indent

This Directive	Directive 91/308/EEC
Article 3(5)(c)	Article 1(E), second indent
Article 3(5)(d)	Article 1(E), third indent
Article 3(5)(e)	Article 1(E), fourth indent
Article 3(5)(f)	Article 1(E), fifth indent, and third paragraph
Article 3(6)	
Article 3(7)	
Article 3(8)	
Article 3(9)	
Article 3(10)	
Article 4	Article 12
Article 5	Article 15
Article 6	
Article 7(a)	Article 3(1)
Article 7(b)	Article 3(2)
Article 7(c)	Article 3(8)
Article 7(d)	Article 3(7)
Article 8(1)(a)	Article 3(1)
Article 8(1)(b) to (d)	
Article 8(2)	
Article 9(1)	Article 3(1)
Article 9(2) to (6)	
Article 10	Article 3(5) and (6)
Article 11(1)	Article 3(9)
Article 11(2)	
Article 11(3) and (4)	
Article 11(5)(a)	Article 3(3)
Article 11(5)(b)	Article 3(4)
Article 11(5)(c)	Article 3(4)
Article 11(5)(d)	

This Directive	Directive 91/308/EEC
Article 12	
Article 13(1) and (2)	Article 3(10) and (11)
Article 13(3) to (5)	
Article 13(6)	Article 5
Article 14	
Article 15	
Article 16	
Article 17	
Article 18	
Article 19	
Article 20	Article 5
Article 21	
Article 22	Article 6(1) and (2)
Article 23	Article 6(3)
Article 24	Article 7
Article 25	Article 10
Article 26	Article 9
Article 27	
Article 28(1)	Article 8(1)
Article 28(2) to (7)	
Article 29	
Article 30(a)	Article 4, first indent
Article 30(b)	Article 4, second indent
Article 31	
Article 32	
Article 33	
Article 34(1)	Article 11(1) (a)
Article 34(2)	
Article 35(1), first paragraph	Article 11(1)(b), first sentence
Article 35(1), second paragraph	Article 11(1)(b) second sentence
Article 35(1), third paragraph	Article 11(1), second paragraph

This Directive	Directive 91/308/EEC
Article 35(2)	
Article 35(3)	
Article 36	
Article 37	
Article 38	
Article 39(1)	Article 14
Article 39(2) to (4)	
Article 40	
Article 41	
Article 42	Article 17
Article 43	
Article 44	
Article 45	Article 16
Article 46	Article 16

Exhibit 4

DIRECTIVES

DIRECTIVE (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 20 May 2015

on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank ([1]),

Having regard to the opinion of the European Economic and Social Committee ([2]),

Acting in accordance with the ordinary legislative procedure ([3]),

Whereas:

(1) Flows of illicit money can damage the integrity, stability and reputation of the financial sector, and threaten the internal market of the Union as well as international development. Money laundering, terrorism financing and organised crime remain significant problems which should be addressed at Union level. In addition to further developing the criminal law approach at Union level, targeted and proportionate prevention of the use of the financial system for the purposes of money laundering and terrorist financing is indispensable and can produce complementary results.

(2) The soundness, integrity and stability of credit institutions and financial institutions, and confidence in the financial system as a whole could be seriously jeopardised by the efforts of criminals and their associates to disguise the origin of criminal proceeds or to channel lawful or illicit money for terrorist purposes. In order to facilitate their criminal activities, money launderers and financers of terrorism could try to take advantage of the freedom of capital movements and the freedom to supply financial services which the Union's integrated financial area entails. Therefore, certain coordinating measures are necessary at Union level. At the same time, the objectives of protecting society from crime and protecting the stability and integrity of the Union's financial system should be balanced against the need to create a regulatory environment that allows companies to grow their businesses without incurring disproportionate compliance costs.

(3) This Directive is the fourth directive to address the threat of money laundering. Council Directive 91/308/EEC ([4]) defined money laundering in terms of drugs offences and imposed obligations solely on the financial sector.

([1]) OJ C 166, 12.6.2013, p. 2.
([2]) OJ C 271, 19.9.2013, p. 31.
([3]) Position of the European Parliament of 11 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 20 April 2015 (not yet published in the Official Journal). Position of the European Parliament of 20 May 2015 (not yet published in the Official Journal).
([4]) Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering (OJ L 166, 28.6.1991, p. 77).

Directive 2001/97/EC of the European Parliament and of the Council [1] extended the scope of Directive 91/308/EEC both in terms of the crimes covered and in terms of the range of professions and activities covered. In June 2003, the Financial Action Task Force (FATF) revised its Recommendations to cover terrorist financing, and provided more detailed requirements in relation to customer identification and verification, the situations where a higher risk of money laundering or terrorist financing may justify enhanced measures and also the situations where a reduced risk may justify less rigorous controls. Those changes were reflected in Directive 2005/60/EC of the European Parliament and of the Council [2] and in Commission Directive 2006/70/EC [3].

(4) Money laundering and terrorist financing are frequently carried out in an international context. Measures adopted solely at national or even at Union level, without taking into account international coordination and cooperation, would have very limited effect. The measures adopted by the Union in that field should therefore be compatible with, and at least as stringent as, other actions undertaken in international fora. Union action should continue to take particular account of the FATF Recommendations and instruments of other international bodies active in the fight against money laundering and terrorist financing. With a view to reinforcing the efficacy of the fight against money laundering and terrorist financing, the relevant Union legal acts should, where appropriate, be aligned with the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation adopted by the FATF in February 2012 (the 'revised FATF Recommendations').

(5) Furthermore, the misuse of the financial system to channel illicit or even lawful money into terrorist purposes poses a clear risk to the integrity, proper functioning, reputation and stability of the financial system. Accordingly, the preventive measures laid down in this Directive should address the manipulation of money derived from serious crime and the collection of money or property for terrorist purposes.

(6) The use of large cash payments is highly vulnerable to money laundering and terrorist financing. In order to increase vigilance and mitigate the risks posed by such cash payments, persons trading in goods should be covered by this Directive to the extent that they make or receive cash payments of EUR 10 000 or more. Member States should be able to adopt lower thresholds, additional general limitations to the use of cash and further stricter provisions.

(7) The use of electronic money products is increasingly considered to be a substitute for bank accounts, which, in addition to the measures laid down in Directive 2009/110/EC of the European Parliament and of the Council [4], justifies subjecting those products to anti-money laundering and countering the financing of terrorism (AML/CFT) obligations. However, in certain proven low-risk circumstances and under strict risk-mitigating conditions, Member States should be allowed to exempt electronic money products from certain customer due diligence measures, such as the identification and verification of the customer and of the beneficial owner, but not from the monitoring of transactions or of business relationships. The risk-mitigating conditions should include a requirement that exempt electronic money products be used exclusively for purchasing goods or services, and that the amount stored electronically be low enough to preclude circumvention of the AML/CFT rules. Such an exemption should be without prejudice to the discretion given to Member States to allow obliged entities to apply simplified customer due diligence measures to other electronic money products posing lower risks, in accordance with Article 15.

(8) As concerns the obliged entities which are subject to this Directive, estate agents could be understood to include letting agents, where applicable.

---

[1] Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering (OJ L 344, 28.12.2001, p. 76).

[2] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (OJ L 309, 25.11.2005, p. 15).

[3] Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of politically exposed person and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis (OJ L 214, 4.8.2006, p. 29).

[4] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p. 7).

(9) Legal professionals, as defined by the Member States, should be subject to this Directive when participating in financial or corporate transactions, including when providing tax advice, where there is the greatest risk of the services of those legal professionals being misused for the purpose of laundering the proceeds of criminal activity or for the purpose of terrorist financing. There should, however, be exemptions from any obligation to report information obtained before, during or after judicial proceedings, or in the course of ascertaining the legal position of a client. Therefore, legal advice should remain subject to the obligation of professional secrecy, except where the legal professional is taking part in money laundering or terrorist financing, the legal advice is provided for the purposes of money laundering or terrorist financing, or the legal professional knows that the client is seeking legal advice for the purposes of money laundering or terrorist financing.

(10) Directly comparable services should be treated in the same manner when provided by any of the professionals covered by this Directive. In order to ensure respect for the rights guaranteed by the Charter of Fundamental Rights of the European Union (the 'Charter'), in the case of auditors, external accountants and tax advisors, who, in some Member States, are entitled to defend or represent a client in the context of judicial proceedings or to ascertain a client's legal position, the information they obtain in the performance of those tasks should not be subject to the reporting obligations laid down in this Directive.

(11) It is important expressly to highlight that 'tax crimes' relating to direct and indirect taxes are included in the broad definition of 'criminal activity' in this Directive, in line with the revised FATF Recommendations. Given that different tax offences may be designated in each Member State as constituting 'criminal activity' punishable by means of the sanctions as referred to in point (4)(f) of Article 3 of this Directive, national law definitions of tax crimes may diverge. While no harmonisation of the definitions of tax crimes in Member States' national law is sought, Member States should allow, to the greatest extent possible under their national law, the exchange of information or the provision of assistance between EU Financial Intelligence Units (FIUs).

(12) There is a need to identify any natural person who exercises ownership or control over a legal entity. In order to ensure effective transparency, Member States should ensure that the widest possible range of legal entities incorporated or created by any other mechanism in their territory is covered. While finding a specified percentage shareholding or ownership interest does not automatically result in finding the beneficial owner, it should be one evidential factor among others to be taken into account. Member States should be able, however, to decide that a lower percentage may be an indication of ownership or control.

(13) Identification and verification of beneficial owners should, where relevant, extend to legal entities that own other legal entities, and obliged entities should look for the natural person(s) who ultimately exercises control through ownership or through other means of the legal entity that is the customer. Control through other means may, inter alia, include the criteria of control used for the purpose of preparing consolidated financial statements, such as through a shareholders' agreement, the exercise of dominant influence or the power to appoint senior management. There may be cases where no natural person is identifiable who ultimately owns or exerts control over a legal entity. In such exceptional cases, obliged entities, having exhausted all other means of identification, and provided there are no grounds for suspicion, may consider the senior managing official(s) to be the beneficial owner(s).

(14) The need for accurate and up-to-date information on the beneficial owner is a key factor in tracing criminals who might otherwise hide their identity behind a corporate structure. Member States should therefore ensure that entities incorporated within their territory in accordance with national law obtain and hold adequate, accurate and current information on their beneficial ownership, in addition to basic information such as the company name and address and proof of incorporation and legal ownership. With a view to enhancing transparency in order to combat the misuse of legal entities, Member States should ensure that beneficial ownership information is stored in a central register located outside the company, in full compliance with Union law. Member States can, for that purpose, use a central database which collects beneficial ownership information, or the business register, or another central register. Member States may decide that obliged entities are responsible for filling in the register. Member States should make sure that in all cases that information is made available to competent authorities and FIUs and is provided to obliged entities when the latter take customer due diligence measures. Member States should also ensure that other persons who are able to demonstrate a legitimate interest with respect to money laundering, terrorist financing, and the associated predicate offences, such as corruption, tax

crimes and fraud, are granted access to beneficial ownership information, in accordance with data protection rules. The persons who are able to demonstrate a legitimate interest should have access to information on the nature and extent of the beneficial interest held consisting of its approximate weight.

(15) For that purpose, Member States should be able, under national law, to allow for access that is wider than the access provided for under this Directive.

(16) Timely access to information on beneficial ownership should be ensured in ways which avoid any risk of tipping off the company concerned.

(17) In order to ensure a level playing field among the different types of legal forms, trustees should also be required to obtain, hold and provide beneficial ownership information to obliged entities taking customer due diligence measures and to communicate that information to a central register or a central database and they should disclose their status to obliged entities. Legal entities such as foundations and legal arrangements similar to trusts should be subject to equivalent requirements.

(18) This Directive should also apply to activities of obliged entities which are performed on the internet.

(19) New technologies provide time-effective and cost-effective solutions to businesses and to customers and should therefore be taken into account when evaluating risk. The competent authorities and obliged entities should be proactive in combating new and innovative ways of money laundering.

(20) The representatives of the Union in the governing bodies of the European Bank for Reconstruction and Development are encouraged to implement this Directive and to publish on its website AML/CFT policies, containing detailed procedures that would give effect to this Directive.

(21) The use of gambling sector services to launder the proceeds of criminal activity is of concern. In order to mitigate the risks relating to gambling services, this Directive should provide for an obligation for providers of gambling services posing higher risks to apply customer due diligence measures for single transactions amounting to EUR 2 000 or more. Member States should ensure that obliged entities apply the same threshold to the collection of winnings, wagering a stake, including by the purchase and exchange of gambling chips, or both. Providers of gambling services with physical premises, such as casinos and gaming houses, should ensure that customer due diligence, if it is taken at the point of entry to the premises, can be linked to the transactions conducted by the customer on those premises. However, in proven low-risk circumstances, Member States should be allowed to exempt certain gambling services from some or all of the requirements laid down in this Directive. The use of an exemption by a Member State should be considered only in strictly limited and justified circumstances, and where the risks of money laundering or terrorist financing are low. Such exemptions should be subject to a specific risk assessment which also considers the degree of vulnerability of the applicable transactions. They should be notified to the Commission. In the risk assessment, Member States should indicate how they have taken into account any relevant findings in the reports issued by the Commission in the framework of the supranational risk assessment.

(22) The risk of money laundering and terrorist financing is not the same in every case. Accordingly, a holistic, risk-based approach should be used. The risk-based approach is not an unduly permissive option for Member States and obliged entities. It involves the use of evidence-based decision-making in order to target the risks of money laundering and terrorist financing facing the Union and those operating within it more effectively.

(23) Underpinning the risk-based approach is the need for Member States and the Union to identify, understand and mitigate the risks of money laundering and terrorist financing that they face. The importance of a supranational approach to risk identification has been recognised at international level, and the European Supervisory Authority (European Banking Authority) (EBA), established by Regulation (EU) No 1093/2010 of the European Parliament and of the Council ([1]), the European Supervisory Authority (European Insurance and Occupational Pensions Authority) (EIOPA), established by Regulation (EU) No 1094/2010 of the European Parliament and of the Council ([2]), and the European Supervisory Authority (European Securities and Markets Authority) (ESMA),

([1]) Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

([2]) Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48).

established by Regulation (EU) No 1095/2010 of the European Parliament and of the Council ([1]), should be tasked with issuing an opinion, through their Joint Committee, on the risks affecting the Union financial sector.

(24) The Commission is well placed to review specific cross-border threats that could affect the internal market and that cannot be identified and effectively combatted by individual Member States. It should therefore be entrusted with the responsibility for coordinating the assessment of risks relating to cross-border activities. Involvement of the relevant experts, such as the Expert Group on Money Laundering and Terrorist Financing and the representatives from the FIUs, as well as, where appropriate, from other Union-level bodies, is essential for the effectiveness of that process. National risk assessments and experience are also an important source of information for the process. Such assessment of the cross-border risks by the Commission should not involve the processing of personal data. In any event, data should be fully anonymised. National and Union data protection supervisory authorities should be involved only if the assessment of the risk of money laundering and terrorist financing has an impact on the privacy and data protection of individuals.

(25) The results of risk assessments should, where appropriate, be made available to obliged entities in a timely manner to enable them to identify, understand, manage and mitigate their own risks.

(26) In addition, to identify, understand, manage and mitigate risks at Union level to an even greater degree, Member States should make available the results of their risk assessments to each other, to the Commission and to EBA, EIOPA and ESMA (the 'ESAs').

(27) When applying this Directive, it is appropriate to take account of the characteristics and needs of smaller obliged entities which fall under its scope, and to ensure treatment which is appropriate to their specific needs, and the nature of the business.

(28) In order to protect the proper functioning of the Union financial system and of the internal market from money laundering and terrorist financing, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union (TFEU) should be delegated to the Commission in order to identify third-country jurisdictions which have strategic deficiencies in their national AML/CFT regimes ('high-risk third countries'). The changing nature of money laundering and terrorist financing threats, facilitated by a constant evolution of technology and of the means at the disposal of criminals, requires that quick and continuous adaptations of the legal framework as regards high-risk third countries be made in order to address efficiently existing risks and prevent new ones from arising. The Commission should take into account information from international organisations and standard setters in the field of AML/CFT, such as FATF public statements, mutual evaluation or detailed assessment reports or published follow-up reports, and adapt its assessments to the changes therein, where appropriate.

(29) Member States should at least provide for enhanced customer due diligence measures to be applied by the obliged entities when dealing with natural persons or legal entities established in high-risk third countries identified by the Commission. Reliance on third parties established in such high-risk third countries should also be prohibited. Countries not included in the list should not be automatically considered to have effective AML/CFT systems and natural persons or legal entities established in such countries should be assessed on a risk-sensitive basis.

(30) Risk itself is variable in nature, and the variables, on their own or in combination, may increase or decrease the potential risk posed, thus having an impact on the appropriate level of preventative measures, such as customer due diligence measures. Therefore, there are circumstances in which enhanced due diligence should be applied and others in which simplified due diligence may be appropriate.

(31) It should be recognised that certain situations present a greater risk of money laundering or terrorist financing. Although the identity and business profile of all customers should be established, there are cases in which particularly rigorous customer identification and verification procedures are required.

([1]) Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84).

(32) This is particularly true of relationships with individuals who hold or who have held important public functions, within the Union or internationally, and particularly individuals from countries where corruption is widespread. Such relationships may expose the financial sector in particular to significant reputational and legal risks. The international effort to combat corruption also justifies the need to pay particular attention to such persons and to apply appropriate enhanced customer due diligence measures with respect to persons who are or who have been entrusted with prominent public functions domestically or abroad and with respect to senior figures in international organisations.

(33) The requirements relating to politically exposed persons are of a preventive and not criminal nature, and should not be interpreted as stigmatising politically exposed persons as being involved in criminal activity. Refusing a business relationship with a person simply on the basis of the determination that he or she is a politically exposed person is contrary to the letter and spirit of this Directive and of the revised FATF Recommendations.

(34) Obtaining approval from senior management for establishing business relationships does not need to imply, in all cases, obtaining approval from the board of directors. It should be possible for such approval to be granted by someone with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and of sufficient seniority to take decisions affecting its risk exposure.

(35) In order to avoid repeated customer identification procedures, leading to delays and inefficiency in business, it is appropriate, subject to suitable safeguards, to allow customers whose identification has been carried out elsewhere to be introduced to the obliged entities. Where an obliged entity relies on a third party, the ultimate responsibility for customer due diligence should remain with the obliged entity to which the customer is introduced. The third party, or the person that has introduced the customer, should also retain its own responsibility for compliance with this Directive, including the requirement to report suspicious transactions and maintain records, to the extent that it has a relationship with the customer that is covered by this Directive.

(36) In the case of agency or outsourcing relationships on a contractual basis between obliged entities and external persons not covered by this Directive, any AML/CFT obligations upon those agents or outsourcing service providers as part of the obliged entities could arise only from the contract between the parties and not from this Directive. Therefore the responsibility for complying with this Directive should remain primarily with the obliged entity.

(37) All Member States have, or should, set up operationally independent and autonomous FIUs to collect and analyse the information which they receive with the aim of establishing links between suspicious transactions and underlying criminal activity in order to prevent and combat money laundering and terrorist financing. An operationally independent and autonomous FIU should mean that the FIU has the authority and capacity to carry out its functions freely, including the autonomous decision to analyse, request and disseminate specific information. Suspicious transactions and other information relevant to money laundering, associated predicate offences and terrorist financing should be reported to the FIU, which should serve as a central national unit for receiving, analysing and disseminating to the competent authorities the results of its analyses. All suspicious transactions, including attempted transactions, should be reported, regardless of the amount of the transaction. Reported information could also include threshold-based information.

(38) By way of derogation from the general prohibition against carrying out suspicious transactions, obliged entities should be able to carry out suspicious transactions before informing the competent authorities where refraining from such carrying out is impossible or likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation. This, however, should be without prejudice to the international obligations accepted by the Member States to freeze without delay funds or other assets of terrorists, terrorist organisations or those who finance terrorism, in accordance with the relevant United Nations Security Council resolutions.

(39) For certain obliged entities, Member States should have the possibility to designate an appropriate self-regulatory body as the authority to be informed in the first instance instead of the FIU. In accordance with the case-law of the European Court of Human Rights, a system of first instance reporting to a self-regulatory body constitutes an important safeguard for upholding the protection of fundamental rights as concerns the reporting obligations applicable to lawyers. Member States should provide for the means and manner by which to achieve the protection of professional secrecy, confidentiality and privacy.

(40) Where a Member State decides to designate such a self-regulatory body, it may allow or require that body not to transmit to the FIU any information obtained from persons represented by that body where such information has

been received from, or obtained on, one of their clients, in the course of ascertaining the legal position of their client, or in performing their task of defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings, whether such information is received or obtained before, during or after such proceedings.

(41) There have been a number of cases where employees who have reported their suspicions of money laundering have been subjected to threats or hostile action. Although this Directive cannot interfere with Member States' judicial procedures, it is crucial that this issue be addressed to ensure effectiveness of the AML/CFT system. Member States should be aware of this problem and should do whatever they can to protect individuals, including employees and representatives of the obliged entity, from such threats or hostile action, and to provide, in accordance with national law, appropriate protection to such persons, particularly with regard to their right to the protection of their personal data and their rights to effective judicial protection and representation.

(42) Directive 95/46/EC of the European Parliament and of the Council ([1]), as transposed into national law, applies to the processing of personal data for the purposes of this Directive. Regulation (EC) No 45/2001 of the European Parliament and of the Council ([2]) applies to the processing of personal data by the Union institutions and bodies for the purposes of this Directive. The fight against money laundering and terrorist financing is recognised as an important public interest ground by all Member States. This Directive is without prejudice to the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, including Council Framework Decision 2008/977/JHA ([3]), as implemented in national law.

(43) It is essential that the alignment of this Directive with the revised FATF Recommendations is carried out in full compliance with Union law, in particular as regards Union data protection law and the protection of fundamental rights as enshrined in the Charter. Certain aspects of the implementation of this Directive involve the collection, analysis, storage and sharing of data. Such processing of personal data should be permitted, while fully respecting fundamental rights, only for the purposes laid down in this Directive, and for the activities required under this Directive such as carrying out customer due diligence, ongoing monitoring, investigation and reporting of unusual and suspicious transactions, identification of the beneficial owner of a legal person or legal arrangement, identification of a politically exposed person, sharing of information by competent authorities and sharing of information by credit institutions and financial institutions and other obliged entities. The collection and subsequent processing of personal data by obliged entities should be limited to what is necessary for the purpose of complying with the requirements of this Directive and personal data should not be further processed in a way that is incompatible with that purpose. In particular, further processing of personal data for commercial purposes should be strictly prohibited.

(44) The revised FATF Recommendations demonstrate that, in order to be able to cooperate fully and comply swiftly with information requests from competent authorities for the purposes of the prevention, detection or investigation of money laundering and terrorist financing, obliged entities should maintain, for at least five years, the necessary information obtained through customer due diligence measures and the records on transactions. In order to avoid different approaches and in order to fulfil the requirements relating to the protection of personal data and legal certainty, that retention period should be fixed at five years after the end of a business relationship or of an occasional transaction. However, if necessary for the purposes of prevention, detection or investigation of money laundering and terrorist financing, and after carrying out an assessment of the necessity and proportionality, Member States should be able to allow or require the further retention of records for a period not exceeding an additional five years, without prejudice to the national criminal law on evidence applicable to ongoing criminal investigations and legal proceedings. Member States should require that specific safeguards be put in place to ensure the security of data and should determine which persons, categories of persons or authorities should have exclusive access to the data retained.

(45) For the purpose of ensuring the appropriate and efficient administration of justice during the period for transposition of this Directive into the Member States' national legal orders, and in order to allow for its smooth interaction with national procedural law, information and documents pertinent to ongoing legal proceedings for

([1]) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

([2]) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

([3]) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60).

the purpose of the prevention, detection or investigation of possible money laundering or terrorist financing, which have been pending in the Member States on the date of entry into force of this Directive, should be retained for a period of five years after that date, and it should be possible to extend that period for a further five years.

(46) The rights of access to data by the data subject are applicable to the personal data processed for the purpose of this Directive. However, access by the data subject to any information related to a suspicious transaction report would seriously undermine the effectiveness of the fight against money laundering and terrorist financing. Exceptions to and restrictions of that right in accordance with Article 13 of Directive 95/46/EC and, where relevant, Article 20 of Regulation (EC) No 45/2001, may therefore be justified. The data subject has the right to request that a supervisory authority referred to in Article 28 of Directive 95/46/EC or, where applicable, the European Data Protection Supervisor, check the lawfulness of the processing and has the right to seek a judicial remedy referred to in Article 22 of that Directive. The supervisory authority referred to in Article 28 of Directive 95/46/EC may also act on an *ex-officio* basis. Without prejudice to the restrictions to the right to access, the supervisory authority should be able to inform the data subject that all necessary verifications by the supervisory authority have taken place, and of the result as regards the lawfulness of the processing in question.

(47) Persons that merely convert paper documents into electronic data and are acting under a contract with a credit institution or a financial institution and persons that provide credit institutions or financial institutions solely with messaging or other support systems for transmitting funds or with clearing and settlement systems do not fall within the scope of this Directive.

(48) Money laundering and terrorist financing are international problems and the effort to combat them should be global. Where Union credit institutions and financial institutions have branches and subsidiaries located in third countries in which the requirements in that area are less strict than those of the Member State, they should, in order to avoid the application of very different standards within the institution or group of institutions, apply to those branches and subsidiaries Union standards or notify the competent authorities of the home Member State if the application of such standards is not possible.

(49) Feedback on the usefulness and follow-up of the suspicious transactions reports they present should, where practicable, be made available to obliged entities. To make this possible, and to be able to review the effectiveness of their systems for combating money laundering and terrorist financing, Member States should maintain, and improve the quality of, relevant statistics. To further enhance the quality and consistency of the statistical data collected at Union level, the Commission should keep track of the Union-wide situation with respect to the fight against money laundering and terrorist financing and should publish regular overviews.

(50) Where Member States require issuers of electronic money and payment service providers which are established in their territory in forms other than a branch and the head office of which is situated in another Member State, to appoint a central contact point in their territory, they should be able to require that such a central contact point, acting on behalf of the appointing institution, ensure the establishments' compliance with AML/CFT rules. They should also ensure that that requirement is proportionate and does not go beyond what is necessary to achieve the aim of compliance with AML/CFT rules, including by facilitating the respective supervision.

(51) Competent authorities should ensure that, with regard to currency exchange offices, cheque cashing offices, trust or company service providers or gambling service providers, the persons who effectively direct the business of such entities and the beneficial owners of such entities are fit and proper. The criteria for determining whether or not a person is fit and proper should, as a minimum, reflect the need to protect such entities from being misused by their managers or beneficial owners for criminal purposes.

(52) Where an obliged entity operates establishments in another Member State, including through a network of agents, the competent authority of the home Member State should be responsible for supervising the obliged entity's application of group-wide AML/CFT policies and procedures. This could involve on-site visits in establishments based in another Member State. The competent authority of the home Member State should cooperate closely with the competent authority of the host Member State and should inform the latter of any issues that could affect their assessment of the establishment's compliance with the host AML/CFT rules.

(53) Where an obliged entity operates establishments in another Member State, including through a network of agents or persons distributing electronic money in accordance with Article 3(4) of Directive 2009/110/EC, the competent authority of the host Member State retains responsibility for enforcing the establishment's compliance with AML/CFT rules, including, where appropriate, by carrying out onsite inspections and offsite monitoring and by taking appropriate and proportionate measures to address serious infringements of those requirements. The competent authority of the host Member State should cooperate closely with the competent authority of the home Member State and should inform the latter of any issues that could affect its assessment of the obliged entity's application of group AML/CFT policies and procedures. In order to remove serious infringements of AML/CFT rules that require immediate remedies, the competent authority of the host Member State should be able to apply appropriate and proportionate temporary remedial measures, applicable under similar circumstances to obliged entities under their competence, to address such serious failings, where appropriate, with the assistance of, or in cooperation with, the competent authority of the home Member State.

(54) Taking into account the transnational nature of money laundering and terrorist financing, coordination and cooperation between FIUs are extremely important. In order to improve such coordination and cooperation, and, in particular, to ensure that suspicious transaction reports reach the FIU of the Member State where the report would be of most use, detailed rules are laid down in this Directive.

(55) The EU Financial Intelligence Units' Platform (the 'EU FIUs Platform'), an informal group composed of representatives from FIUs and active since 2006, is used to facilitate cooperation among FIUs and exchange views on cooperation-related issues such as effective cooperation among FIUs and between FIUs and third-country financial intelligence units, joint analysis of cross-border cases and trends and factors relevant to assessing the risks of money laundering and terrorist financing at national and supranational level.

(56) Improving the exchange of information between FIUs within the Union is particularly important in addressing the transnational character of money laundering and terrorist financing. The use of secure facilities for the exchange of information, in particular the decentralised computer network FIU.net (the 'FIU.net') or its successor and the techniques offered by FIU.net, should be encouraged by Member States. The initial exchange of information between FIUs relating to money laundering or terrorist financing for analytical purposes which is not further processed or disseminated should be permitted unless such exchange of information would be contrary to fundamental principles of national law. The exchange of information on cases identified by FIUs as possibly involving tax crimes should be without prejudice to the exchange of information in the field of taxation in accordance with Council Directive 2011/16/EU [1] or in accordance with international standards on the exchange of information and administrative cooperation in tax matters.

(57) In order to be able to respond fully and rapidly to enquiries from FIUs, obliged entities need to have in place effective systems enabling them to have full and timely access through secure and confidential channels to information about business relationships that they maintain or have maintained with specified persons. In accordance with Union and national law, Member States could, for instance, consider putting in place systems of banking registries or electronic data retrieval systems which would provide FIUs with access to information on bank accounts without prejudice to judicial authorisation where applicable. Member States could also consider establishing mechanisms to ensure that competent authorities have procedures in place to identify assets without prior notification to the owner.

(58) Member States should encourage their competent authorities to provide rapidly, constructively and effectively the widest range of cross-border cooperation for the purposes of this Directive, without prejudice to any rules or procedures applicable to judicial cooperation in criminal matters. Member States should in particular ensure that their FIUs exchange information freely, spontaneously or upon request, with third-country financial intelligence units, having regard to Union law and to the principles relating to information exchange developed by the Egmont Group of Financial Intelligence Units.

(59) The importance of combating money laundering and terrorist financing should result in Member States laying down effective, proportionate and dissuasive administrative sanctions and measures in national law for failure to respect the national provisions transposing this Directive. Member States currently have a diverse range of administrative sanctions and measures for breaches of the key preventative provisions in place. That diversity could be detrimental to the efforts made in combating money laundering and terrorist financing and the Union's

[1] Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC (OJ L 64, 11.3.2011, p. 1).

response is at risk of being fragmented. This Directive should therefore provide for a range of administrative sanctions and measures by Member States at least for serious, repeated or systematic breaches of the requirements relating to customer due diligence measures, record-keeping, reporting of suspicious transactions and internal controls of obliged entities. The range of sanctions and measures should be sufficiently broad to allow Member States and competent authorities to take account of the differences between obliged entities, in particular between credit institutions and financial institutions and other obliged entities, as regards their size, characteristics and the nature of the business. In transposing this Directive, Member States should ensure that the imposition of administrative sanctions and measures in accordance with this Directive, and of criminal sanctions in accordance with national law, does not breach the principle of *ne bis in idem*.

(60) For the purposes of assessing the appropriateness of persons holding a management function in, or otherwise controlling, obliged entities, any exchange of information about criminal convictions should be carried out in accordance with Council Framework Decision 2009/315/JHA ([1]) and Council Decision 2009/316/JHA ([2]), as transposed into national law, and with other relevant provisions of national law.

(61) Regulatory technical standards in financial services should ensure consistent harmonisation and adequate protection of depositors, investors and consumers across the Union. As bodies with highly specialised expertise, it would be efficient and appropriate to entrust the ESAs with the elaboration, for submission to the Commission, of draft regulatory technical standards which do not involve policy choices.

(62) The Commission should adopt the draft regulatory technical standards developed by the ESAs pursuant to this Directive by means of delegated acts pursuant to Article 290 TFEU and in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

(63) Given the very substantial amendments that would need to be made to Directives 2005/60/EC and 2006/70/EC in light of this Directive, they should be merged and replaced for reasons of clarity and consistency.

(64) Since the objective of this Directive, namely the protection of the financial system by means of prevention, detection and investigation of money laundering and terrorist financing, cannot be sufficiently achieved by the Member States, as individual measures adopted by Member States to protect their financial systems could be inconsistent with the functioning of the internal market and with the prescriptions of the rule of law and Union public policy, but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(65) This Directive respects the fundamental rights and observes the principles recognised by the Charter, in particular the right to respect for private and family life, the right to the protection of personal data, the freedom to conduct a business, the prohibition of discrimination, the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence.

(66) In accordance with Article 21 of the Charter, which prohibits discrimination based on any ground, Member States are to ensure that this Directive is implemented, as regards risk assessments in the context of customer due diligence, without discrimination.

(67) In accordance with the Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents ([3]), Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

(68) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 4 July 2013 ([4]),

([1]) Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States (OJ L 93, 7.4.2009, p. 23).
([2]) Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA (OJ L 93, 7.4.2009, p. 33).
([3]) OJ C 369, 17.12.2011, p. 14.
([4]) OJ C 32, 4.2.2014, p. 9.

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

SECTION 1

Subject-matter, scope and definitions

Article 1

1. This Directive aims to prevent the use of the Union's financial system for the purposes of money laundering and terrorist financing.

2. Member States shall ensure that money laundering and terrorist financing are prohibited.

3. For the purposes of this Directive, the following conduct, when committed intentionally, shall be regarded as money laundering:

(a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;

(b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;

(c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;

(d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).

4. Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

5. For the purposes of this Directive, 'terrorist financing' means the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA ([1]).

6. Knowledge, intent or purpose required as an element of the activities referred to in paragraphs 3 and 5 may be inferred from objective factual circumstances.

Article 2

1. This Directive shall apply to the following obliged entities:

(1) credit institutions;

(2) financial institutions;

(3) the following natural or legal persons acting in the exercise of their professional activities:

  (a) auditors, external accountants and tax advisors;

  (b) notaries and other independent legal professionals, where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning the:

    (i) buying and selling of real property or business entities;

    (ii) managing of client money, securities or other assets;

    (iii) opening or management of bank, savings or securities accounts;

([1]) Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3).

(iv) organisation of contributions necessary for the creation, operation or management of companies;

(v) creation, operation or management of trusts, companies, foundations, or similar structures;

(c) trust or company service providers not already covered under point (a) or (b);

(d) estate agents;

(e) other persons trading in goods to the extent that payments are made or received in cash in an amount of EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(f) providers of gambling services.

2. With the exception of casinos, and following an appropriate risk assessment, Member States may decide to exempt, in full or in part, providers of certain gambling services from national provisions transposing this Directive on the basis of the proven low risk posed by the nature and, where appropriate, the scale of operations of such services.

Among the factors considered in their risk assessments, Member States shall assess the degree of vulnerability of the applicable transactions, including with respect to the payment methods used.

In their risk assessments, Member States shall indicate how they have taken into account any relevant findings in the reports issued by the Commission pursuant to Article 6.

Any decision taken by a Member State pursuant to the first subparagraph shall be notified to the Commission, together with a justification based on the specific risk assessment. The Commission shall communicate that decision to the other Member States.

3. Member States may decide that persons that engage in a financial activity on an occasional or very limited basis where there is little risk of money laundering or terrorist financing do not fall within the scope of this Directive, provided that all of the following criteria are met:

(a) the financial activity is limited in absolute terms;

(b) the financial activity is limited on a transaction basis;

(c) the financial activity is not the main activity of such persons;

(d) the financial activity is ancillary and directly related to the main activity of such persons;

(e) the main activity of such persons is not an activity referred to in points (a) to (d) or point (f) of paragraph 1(3);

(f) the financial activity is provided only to the customers of the main activity of such persons and is not generally offered to the public.

The first subparagraph shall not apply to persons engaged in the activity of money remittance as defined in point (13) of Article 4 of Directive 2007/64/EC of the European Parliament and of the Council ([1]).

4. For the purposes of point (a) of paragraph 3, Member States shall require that the total turnover of the financial activity does not exceed a threshold which must be sufficiently low. That threshold shall be established at national level, depending on the type of financial activity.

5. For the purposes of point (b) of paragraph 3, Member States shall apply a maximum threshold per customer and per single transaction, whether the transaction is carried out in a single operation or in several operations which appear to be linked. That maximum threshold shall be established at national level, depending on the type of financial activity. It shall be sufficiently low in order to ensure that the types of transactions in question are an impractical and inefficient method for money laundering or terrorist financing, and shall not exceed EUR 1 000.

6. For the purposes of point (c) of paragraph 3, Member States shall require that the turnover of the financial activity does not exceed 5 % of the total turnover of the natural or legal person concerned.

([1]) Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (OJ L 319, 5.12.2007, p. 1).

7. In assessing the risk of money laundering or terrorist financing for the purposes of this Article, Member States shall pay particular attention to any financial activity which is considered to be particularly likely, by its nature, to be used or abused for the purposes of money laundering or terrorist financing.

8. Decisions taken by Member States pursuant to paragraph 3 shall state the reasons on which they are based. Member States may decide to withdraw such decisions where circumstances change. They shall notify such decisions to the Commission. The Commission shall communicate such decisions to the other Member States.

9. Member States shall establish risk-based monitoring activities or take other adequate measures to ensure that the exemption granted by decisions pursuant to this Article is not abused.

Article 3

For the purposes of this Directive, the following definitions apply:

(1) 'credit institution' means a credit institution as defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council [1], including branches thereof, as defined in point (17) of Article 4(1) of that Regulation, located in the Union, whether its head office is situated within the Union or in a third country;

(2) 'financial institution' means:

(a) an undertaking other than a credit institution, which carries out one or more of the activities listed in points (2) to (12), (14) and (15) of Annex I to Directive 2013/36/EU of the European Parliament and of the Council [2], including the activities of currency exchange offices (bureaux de change);

(b) an insurance undertaking as defined in point (1) of Article 13 of Directive 2009/138/EC of the European Parliament and of the Council [3], insofar as it carries out life assurance activities covered by that Directive;

(c) an investment firm as defined in point (1) of Article 4(1) of Directive 2004/39/EC of the European Parliament and of the Council [4];

(d) a collective investment undertaking marketing its units or shares;

(e) an insurance intermediary as defined in point (5) of Article 2 of Directive 2002/92/EC of the European Parliament and of the Council [5] where it acts with respect to life insurance and other investment-related services, with the exception of a tied insurance intermediary as defined in point (7) of that Article;

(f) branches, when located in the Union, of financial institutions as referred to in points (a) to (e), whether their head office is situated in a Member State or in a third country;

(3) 'property' means assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets;

(4) 'criminal activity' means any kind of criminal involvement in the commission of the following serious crimes:

(a) acts set out in Articles 1 to 4 of Framework Decision 2002/475/JHA;

(b) any of the offences referred in Article 3(1)(a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances;

---

[1] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

[2] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

[3] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (OJ L 335, 17.12.2009, p. 1).

[4] Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC (OJ L 145, 30.4.2004, p. 1).

[5] Directive 2002/92/EC of the European Parliament and of the Council of 9 December 2002 on insurance mediation (OJ L 9, 15.1.2003, p. 3).

(c) the activities of criminal organisations as defined in Article 1 of Council Joint Action 98/733/JHA ([1]);

(d) fraud affecting the Union's financial interests, where it is at least serious, as defined in Article 1(1) and Article 2(1) of the Convention on the protection of the European Communities' financial interests ([2]);

(e) corruption;

(f) all offences, including tax crimes relating to direct taxes and indirect taxes and as defined in the national law of the Member States, which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards Member States that have a minimum threshold for offences in their legal system, all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months;

(5) 'self-regulatory body' means a body that represents members of a profession and has a role in regulating them, in performing certain supervisory or monitoring type functions and in ensuring the enforcement of the rules relating to them;

(6) 'beneficial owner' means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted and includes at least:

(a) in the case of corporate entities:

(i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Union law or subject to equivalent international standards which ensure adequate transparency of ownership information.

A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a natural person shall be an indication of direct ownership. A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership. This applies without prejudice to the right of Member States to decide that a lower percentage may be an indication of ownership or control. Control through other means may be determined, inter alia, in accordance with the criteria in Article 22(1) to (5) of Directive 2013/34/EU of the European Parliament and of the Council ([3]);

(ii) if, after having exhausted all possible means and provided there are no grounds for suspicion, no person under point (i) is identified, or if there is any doubt that the person(s) identified are the beneficial owner(s), the natural person(s) who hold the position of senior managing official(s), the obliged entities shall keep records of the actions taken in order to identify the beneficial ownership under point (i) and this point;

(b) in the case of trusts:

(i) the settlor;

(ii) the trustee(s);

(iii) the protector, if any;

(iv) the beneficiaries, or where the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;

(v) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means;

([1]) Joint Action 98/733/JHA of 21 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union (OJ L 351, 29.12.1998, p. 1).

([2]) OJ C 316, 27.11.1995, p. 49.

([3]) Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC (OJ L 182, 29.6.2013, p. 19).

(c) in the case of legal entities such as foundations, and legal arrangements similar to trusts, the natural person(s) holding equivalent or similar positions to those referred to in point (b);

(7) 'trust or company service provider' means any person that, by way of its business, provides any of the following services to third parties:

(a) the formation of companies or other legal persons;

(b) acting as, or arranging for another person to act as, a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

(c) providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement;

(d) acting as, or arranging for another person to act as, a trustee of an express trust or a similar legal arrangement;

(e) acting as, or arranging for another person to act as, a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements in accordance with Union law or subject to equivalent international standards;

(8) 'correspondent relationship' means:

(a) the provision of banking services by one bank as the correspondent to another bank as the respondent, including providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services;

(b) the relationships between and among credit institutions and financial institutions including where similar services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers;

(9) 'politically exposed person' means a natural person who is or who has been entrusted with prominent public functions and includes the following:

(a) heads of State, heads of government, ministers and deputy or assistant ministers;

(b) members of parliament or of similar legislative bodies;

(c) members of the governing bodies of political parties;

(d) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;

(e) members of courts of auditors or of the boards of central banks;

(f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;

(g) members of the administrative, management or supervisory bodies of State-owned enterprises;

(h) directors, deputy directors and members of the board or equivalent function of an international organisation.

No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials;

(10) 'family members' includes the following:

(a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;

(b) the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;

(c) the parents of a politically exposed person;

(11) 'persons known to be close associates' means:

(a) natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;

(b) natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

(12) 'senior management' means an officer or employee with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors;

(13) 'business relationship' means a business, professional or commercial relationship which is connected with the professional activities of an obliged entity and which is expected, at the time when the contact is established, to have an element of duration;

(14) 'gambling services' means a service which involves wagering a stake with monetary value in games of chance, including those with an element of skill such as lotteries, casino games, poker games and betting transactions that are provided at a physical location, or by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services;

(15) 'group' means a group of undertakings which consists of a parent undertaking, its subsidiaries, and the entities in which the parent undertaking or its subsidiaries hold a participation, as well as undertakings linked to each other by a relationship within the meaning of Article 22 of Directive 2013/34/EU;

(16) 'electronic money' means electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC;

(17) 'shell bank' means a credit institution or financial institution, or an institution that carries out activities equivalent to those carried out by credit institutions and financial institutions, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.

Article 4

1. Member States shall, in accordance with the risk-based approach, ensure that the scope of this Directive is extended in whole or in part to professions and to categories of undertakings, other than the obliged entities referred to in Article 2(1), which engage in activities which are particularly likely to be used for the purposes of money laundering or terrorist financing.

2. Where a Member State extends the scope of this Directive to professions or to categories of undertaking other than those referred to in Article 2(1), it shall inform the Commission thereof.

Article 5

Member States may adopt or retain in force stricter provisions in the field covered by this Directive to prevent money laundering and terrorist financing, within the limits of Union law.

SECTION 2

Risk assessment

Article 6

1. The Commission shall conduct an assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities.

To that end, the Commission shall, by 26 June 2017, draw up a report identifying, analysing and evaluating those risks at Union level. Thereafter, the Commission shall update its report every two years, or more frequently if appropriate.

2. The report referred to in paragraph 1 shall cover at least the following:

(a) the areas of the internal market that are at greatest risk;

(b) the risks associated with each relevant sector;

(c) the most widespread means used by criminals by which to launder illicit proceeds.

3. The Commission shall make the report referred to in paragraph 1 available to the Member States and obliged entities in order to assist them to identify, understand, manage and mitigate the risk of money laundering and terrorist financing, and to allow other stakeholders, including national legislators, the European Parliament, the ESAs, and representatives from FIUs to better understand the risks.

4. The Commission shall make recommendations to Member States on the measures suitable for addressing the identified risks. In the event that Member States decide not to apply any of the recommendations in their national AML/CFT regimes, they shall notify the Commission thereof and provide a justification for such a decision.

5. By 26 December 2016, the ESAs, through the Joint Committee, shall issue an opinion on the risks of money laundering and terrorist financing affecting the Union's financial sector (the 'joint opinion'). Thereafter, the ESAs, through the Joint Committee, shall issue an opinion every two years.

6. In conducting the assessment referred to in paragraph 1, the Commission shall organise the work at Union level, shall take into account the joint opinions referred to in paragraph 5 and shall involve the Member States' experts in the area of AML/CFT, representatives from FIUs and other Union level bodies where appropriate. The Commission shall make the joint opinions available to the Member States and obliged entities in order to assist them to identify, manage and mitigate the risk of money laundering and terrorist financing.

7. Every two years, or more frequently if appropriate, the Commission shall submit a report to the European Parliament and to the Council on the findings resulting from the regular risk assessments and the action taken based on those findings.

Article 7

1. Each Member State shall take appropriate steps to identify, assess, understand and mitigate the risks of money laundering and terrorist financing affecting it, as well as any data protection concerns in that regard. It shall keep that risk assessment up to date.

2. Each Member State shall designate an authority or establish a mechanism by which to coordinate the national response to the risks referred to in paragraph 1. The identity of that authority or the description of the mechanism shall be notified to the Commission, the ESAs, and other Member States.

3. In carrying out the risk assessments referred to in paragraph 1 of this Article, Member States shall make use of the findings of the report referred to in Article 6(1).

4. As regards the risk assessment referred to in paragraph 1, each Member State shall:

(a) use it to improve its AML/CFT regime, in particular by identifying any areas where obliged entities are to apply enhanced measures and, where appropriate, specifying the measures to be taken;

(b) identify, where appropriate, sectors or areas of lower or greater risk of money laundering and terrorist financing;

(c) use it to assist it in the allocation and prioritisation of resources to combat money laundering and terrorist financing;

(d) use it to ensure that appropriate rules are drawn up for each sector or area, in accordance with the risks of money laundering and terrorist financing;

(e) make appropriate information available promptly to obliged entities to facilitate the carrying out of their own money laundering and terrorist financing risk assessments.

5. Member States shall make the results of their risk assessments available to the Commission, the ESAs and the other Member States.

Article 8

1. Member States shall ensure that obliged entities take appropriate steps to identify and assess the risks of money laundering and terrorist financing, taking into account risk factors including those relating to their customers, countries or geographic areas, products, services, transactions or delivery channels. Those steps shall be proportionate to the nature and size of the obliged entities.

2. The risk assessments referred to in paragraph 1 shall be documented, kept up-to-date and made available to the relevant competent authorities and self-regulatory bodies concerned. Competent authorities may decide that individual documented risk assessments are not required where the specific risks inherent in the sector are clear and understood.

3. Member States shall ensure that obliged entities have in place policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified at the level of the Union, the Member State and the obliged entity. Those policies, controls and procedures shall be proportionate to the nature and size of the obliged entities.

4. The policies, controls and procedures referred to in paragraph 3 shall include:

(a) the development of internal policies, controls and procedures, including model risk management practices, customer due diligence, reporting, record-keeping, internal control, compliance management including, where appropriate with regard to the size and nature of the business, the appointment of a compliance officer at management level, and employee screening;

(b) where appropriate with regard to the size and nature of the business, an independent audit function to test the internal policies, controls and procedures referred to in point (a).

5. Member States shall require obliged entities to obtain approval from their senior management for the policies, controls and procedures that they put in place and to monitor and enhance the measures taken, where appropriate.

SECTION 3

Third-country policy

Article 9

1. Third-country jurisdictions which have strategic deficiencies in their national AML/CFT regimes that pose significant threats to the financial system of the Union ('high-risk third countries') shall be identified in order to protect the proper functioning of the internal market.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 64 in order to identify high-risk third countries, taking into account strategic deficiencies, in particular in relation to:

(a) the legal and institutional AML/CFT framework of the third country, in particular:

  (i) criminalisation of money laundering and terrorist financing;

  (ii) measures relating to customer due diligence;

  (iii) requirements relating to record-keeping; and

  (iv) requirements to report suspicious transactions;

(b) the powers and procedures of the third country's competent authorities for the purposes of combating money laundering and terrorist financing;

(c) the effectiveness of the AML/CFT system in addressing money laundering or terrorist financing risks of the third country.

3. The delegated acts referred to in paragraph 2 shall be adopted within one month after the identification of the strategic deficiencies referred to in that paragraph.

4. The Commission shall take into account, as appropriate, when drawing up the delegated acts referred to in paragraph 2, relevant evaluations, assessments or reports drawn up by international organisations and standard setters with competence in the field of preventing money laundering and combating terrorist financing, in relation to the risks posed by individual third countries.

CHAPTER II

CUSTOMER DUE DILIGENCE

SECTION 1

General provisions

Article 10

1. Member States shall prohibit their credit institutions and financial institutions from keeping anonymous accounts or anonymous passbooks. Member States shall, in any event, require that the owners and beneficiaries of existing anonymous accounts or anonymous passbooks be subject to customer due diligence measures as soon as possible and in any event before such accounts or passbooks are used in any way.

2. Member States shall take measures to prevent misuse of bearer shares and bearer share warrants.

Article 11

Member States shall ensure that obliged entities apply customer due diligence measures in the following circumstances:

(a) when establishing a business relationship;

(b) when carrying out an occasional transaction that:

(i) amounts to EUR 15 000 or more, whether that transaction is carried out in a single operation or in several operations which appear to be linked; or

(ii) constitutes a transfer of funds, as defined in point (9) of Article 3 of Regulation (EU) 2015/847 of the European Parliament and of the Council [1], exceeding EUR 1 000;

(c) in the case of persons trading in goods, when carrying out occasional transactions in cash amounting to EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(d) for providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(e) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;

(f) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

Article 12

1. By way of derogation from points (a), (b) and (c) of the first subparagraph of Article 13(1) and Article 14, and based on an appropriate risk assessment which demonstrates a low risk, a Member State may allow obliged entities not to apply certain customer due diligence measures with respect to electronic money, where all of the following risk-mitigating conditions are met:

(a) the payment instrument is not reloadable, or has a maximum monthly payment transactions limit of EUR 250 which can be used only in that Member State;

(b) the maximum amount stored electronically does not exceed EUR 250;

[1] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (see page 1 of this Official Journal).

(c) the payment instrument is used exclusively to purchase goods or services;

(d) the payment instrument cannot be funded with anonymous electronic money;

(e) the issuer carries out sufficient monitoring of the transactions or business relationship to enable the detection of unusual or suspicious transactions.

For the purposes of point (b) of the first subparagraph, a Member State may increase the maximum amount to EUR 500 for payment instruments that can be used only in that Member State.

2. Member States shall ensure that the derogation provided for in paragraph 1 is not applicable in the case of redemption in cash or cash withdrawal of the monetary value of the electronic money where the amount redeemed exceeds EUR 100.

Article 13

1. Customer due diligence measures shall comprise:

(a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

(b) identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer;

(c) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;

(d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.

When performing the measures referred to in points (a) and (b) of the first subparagraph, obliged entities shall also verify that any person purporting to act on behalf of the customer is so authorised and identify and verify the identity of that person.

2. Member States shall ensure that obliged entities apply each of the customer due diligence requirements laid down in paragraph 1. However, obliged entities may determine the extent of such measures on a risk-sensitive basis.

3. Member States shall require that obliged entities take into account at least the variables set out in Annex I when assessing the risks of money laundering and terrorist financing.

4. Member States shall ensure that obliged entities are able to demonstrate to competent authorities or self-regulatory bodies that the measures are appropriate in view of the risks of money laundering and terrorist financing that have been identified.

5. For life or other investment-related insurance business, Member States shall ensure that, in addition to the customer due diligence measures required for the customer and the beneficial owner, credit institutions and financial institutions conduct the following customer due diligence measures on the beneficiaries of life insurance and other investment-related insurance policies, as soon as the beneficiaries are identified or designated:

(a) in the case of beneficiaries that are identified as specifically named persons or legal arrangements, taking the name of the person;

(b) in the case of beneficiaries that are designated by characteristics or by class or by other means, obtaining sufficient information concerning those beneficiaries to satisfy the credit institutions or financial institution that it will be able to establish the identity of the beneficiary at the time of the payout.

With regard to points (a) and (b) of the first subparagraph, the verification of the identity of the beneficiaries shall take place at the time of the payout. In the case of assignment, in whole or in part, of the life or other investment-related insurance to a third party, credit institutions and financial institutions aware of the assignment shall identify the beneficial owner at the time of the assignment to the natural or legal person or legal arrangement receiving for its own benefit the value of the policy assigned.

6. In the case of beneficiaries of trusts or of similar legal arrangements that are designated by particular characteristics or class, an obliged entity shall obtain sufficient information concerning the beneficiary to satisfy the obliged entity that it will be able to establish the identity of the beneficiary at the time of the payout or at the time of the exercise by the beneficiary of its vested rights.

Article 14

1. Member States shall require that verification of the identity of the customer and the beneficial owner take place before the establishment of a business relationship or the carrying out of the transaction.

2. By way of derogation from paragraph 1, Member States may allow verification of the identity of the customer and the beneficial owner to be completed during the establishment of a business relationship if necessary so as not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing. In such situations, those procedures shall be completed as soon as practicable after initial contact.

3. By way of derogation from paragraph 1, Member States may allow the opening of an account with a credit institution or financial institution, including accounts that permit transactions in transferable securities, provided that there are adequate safeguards in place to ensure that transactions are not carried out by the customer or on its behalf until full compliance with the customer due diligence requirements laid down in points (a) and (b) of the first subparagraph of Article 13(1) is obtained.

4. Member States shall require that, where an obliged entity is unable to comply with the customer due diligence requirements laid down in point (a), (b) or (c) of the first subparagraph of Article 13(1), it shall not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, and shall terminate the business relationship and consider making a suspicious transaction report to the FIU in relation to the customer in accordance with Article 33.

Member States shall not apply the first subparagraph to notaries, other independent legal professionals, auditors, external accountants and tax advisors only to the strict extent that those persons ascertain the legal position of their client, or perform the task of defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings.

5. Member States shall require that obliged entities apply the customer due diligence measures not only to all new customers but also at appropriate times to existing customers on a risk-sensitive basis, including at times when the relevant circumstances of a customer change.

SECTION 2

Simplified customer due diligence

Article 15

1. Where a Member State or an obliged entity identifies areas of lower risk, that Member State may allow obliged entities to apply simplified customer due diligence measures.

2. Before applying simplified customer due diligence measures, obliged entities shall ascertain that the business relationship or the transaction presents a lower degree of risk.

3. Member States shall ensure that obliged entities carry out sufficient monitoring of the transactions and business relationships to enable the detection of unusual or suspicious transactions.

Article 16

When assessing the risks of money laundering and terrorist financing relating to types of customers, geographic areas, and particular products, services, transactions or delivery channels, Member States and obliged entities shall take into account at least the factors of potentially lower risk situations set out in Annex II.

Article 17

By 26 June 2017, the ESAs shall issue guidelines addressed to competent authorities and the credit institutions and financial institutions in accordance with Article 16 of Regulations (EU) No 1093/2010, (EU) No 1094/2010, and (EU) No 1095/2010 on the risk factors to be taken into consideration and the measures to be taken in situations where simplified customer due diligence measures are appropriate. Specific account shall be taken of the nature and size of the business, and, where appropriate and proportionate, specific measures shall be laid down.

SECTION 3

Enhanced customer due diligence

Article 18

1. In the cases referred to in Articles 19 to 24, and when dealing with natural persons or legal entities established in the third countries identified by the Commission as high-risk third countries, as well as in other cases of higher risk that are identified by Member States or obliged entities, Member States shall require obliged entities to apply enhanced customer due diligence measures to manage and mitigate those risks appropriately.

Enhanced customer due diligence measures need not be invoked automatically with respect to branches or majority-owned subsidiaries of obliged entities established in the Union which are located in high-risk third countries, where those branches or majority-owned subsidiaries fully comply with the group-wide policies and procedures in accordance with Article 45. Member States shall ensure that those cases are handled by obliged entities by using a risk-based approach.

2. Member States shall require obliged entities to examine, as far as reasonably possible, the background and purpose of all complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. In particular, obliged entities shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious.

3. When assessing the risks of money laundering and terrorist financing, Member States and obliged entities shall take into account at least the factors of potentially higher-risk situations set out in Annex III.

4. By 26 June 2017, the ESAs shall issue guidelines addressed to competent authorities and the credit institutions and financial institutions, in accordance with Article 16 of Regulations (EU) No 1093/2010, (EU) No 1094/2010, and (EU) No 1095/2010 on the risk factors to be taken into consideration and the measures to be taken in situations where enhanced customer due diligence measures are appropriate. Specific account shall be taken of the nature and size of the business, and, where appropriate and proportionate, specific measures shall be laid down.

Article 19

With respect to cross-border correspondent relationships with a third-country respondent institution, Member States shall, in addition to the customer due diligence measures laid down in Article 13, require their credit institutions and financial institutions to:

(a) gather sufficient information about the respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision;

(b) assess the respondent institution's AML/CFT controls;

(c) obtain approval from senior management before establishing new correspondent relationships;

(d) document the respective responsibilities of each institution;

(e) with respect to payable-through accounts, be satisfied that the respondent institution has verified the identity of, and performed ongoing due diligence on, the customers having direct access to accounts of the correspondent institution, and that it is able to provide relevant customer due diligence data to the correspondent institution, upon request.

Article 20

With respect to transactions or business relationships with politically exposed persons, Member States shall, in addition to the customer due diligence measures laid down in Article 13, require obliged entities to:

(a) have in place appropriate risk management systems, including risk-based procedures, to determine whether the customer or the beneficial owner of the customer is a politically exposed person;

(b) apply the following measures in cases of business relationships with politically exposed persons:

(i) obtain senior management approval for establishing or continuing business relationships with such persons;

(ii) take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons;

(iii) conduct enhanced, ongoing monitoring of those business relationships.

Article 21

Member States shall require obliged entities to take reasonable measures to determine whether the beneficiaries of a life or other investment-related insurance policy and/or, where required, the beneficial owner of the beneficiary are politically exposed persons. Those measures shall be taken no later than at the time of the payout or at the time of the assignment, in whole or in part, of the policy. Where there are higher risks identified, in addition to applying the customer due diligence measures laid down in Article 13, Member States shall require obliged entities to:

(a) inform senior management before payout of policy proceeds;

(b) conduct enhanced scrutiny of the entire business relationship with the policyholder.

Article 22

Where a politically exposed person is no longer entrusted with a prominent public function by a Member State or a third country, or with a prominent public function by an international organisation, obliged entities shall, for at least 12 months, be required to take into account the continuing risk posed by that person and to apply appropriate and risk-sensitive measures until such time as that person is deemed to pose no further risk specific to politically exposed persons.

Article 23

The measures referred to in Articles 20 and 21 shall also apply to family members or persons known to be close associates of politically exposed persons.

Article 24

Member States shall prohibit credit institutions and financial institutions from entering into, or continuing, a correspondent relationship with a shell bank. They shall require that those institutions take appropriate measures to ensure that they do not engage in or continue correspondent relationships with a credit institution or financial institution that is known to allow its accounts to be used by a shell bank.

SECTION 4

Performance by third parties

Article 25

Member States may permit obliged entities to rely on third parties to meet the customer due diligence requirements laid down in points (a), (b) and (c) of the first subparagraph of Article 13(1). However, the ultimate responsibility for meeting those requirements shall remain with the obliged entity which relies on the third party.

Article 26

1. For the purposes of this Section, 'third parties' means obliged entities listed in Article 2, the member organisations or federations of those obliged entities, or other institutions or persons situated in a Member State or third country that:

(a) apply customer due diligence requirements and record-keeping requirements that are consistent with those laid down in this Directive; and

(b) have their compliance with the requirements of this Directive supervised in a manner consistent with Section 2 of Chapter VI.

2. Member States shall prohibit obliged entities from relying on third parties established in high-risk third countries. Member States may exempt branches and majority-owned subsidiaries of obliged entities established in the Union from that prohibition where those branches and majority-owned subsidiaries fully comply with the group-wide policies and procedures in accordance with Article 45.

Article 27

1. Member States shall ensure that obliged entities obtain from the third party relied upon the necessary information concerning the customer due diligence requirements laid down in points (a), (b) and (c) of the first subparagraph of Article 13(1).

2. Member States shall ensure that obliged entities to which the customer is referred take adequate steps to ensure that the third party provides, immediately, upon request, relevant copies of identification and verification data and other relevant documentation on the identity of the customer or the beneficial owner.

Article 28

Member States shall ensure that the competent authority of the home Member State (for group-wide policies and procedures) and the competent authority of the host Member State (for branches and subsidiaries) may consider an obliged entity to comply with the provisions adopted pursuant to Articles 26 and 27 through its group programme, where all of the following conditions are met:

(a) the obliged entity relies on information provided by a third party that is part of the same group;

(b) that group applies customer due diligence measures, rules on record-keeping and programmes against money laundering and terrorist financing in accordance with this Directive or equivalent rules;

(c) the effective implementation of the requirements referred to in point (b) is supervised at group level by a competent authority of the home Member State or of the third country.

Article 29

This Section shall not apply to outsourcing or agency relationships where, on the basis of a contractual arrangement, the outsourcing service provider or agent is to be regarded as part of the obliged entity.

CHAPTER III

BENEFICIAL OWNERSHIP INFORMATION

Article 30

1. Member States shall ensure that corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership, including the details of the beneficial interests held.

Member States shall ensure that those entities are required to provide, in addition to information about their legal owner, information on the beneficial owner to obliged entities when the obliged entities are taking customer due diligence measures in accordance with Chapter II.

2. Member States shall require that the information referred to in paragraph 1 can be accessed in a timely manner by competent authorities and FIUs.

3. Member States shall ensure that the information referred to in paragraph 1 is held in a central register in each Member State, for example a commercial register, companies register as referred to in Article 3 of Directive 2009/101/EC of the European Parliament and of the Council ([1]), or a public register. Member States shall notify to the Commission the characteristics of those national mechanisms. The information on beneficial ownership contained in that database may be collected in accordance with national systems.

4. Member States shall require that the information held in the central register referred to in paragraph 3 is adequate, accurate and current.

5. Member States shall ensure that the information on the beneficial ownership is accessible in all cases to:

(a) competent authorities and FIUs, without any restriction;

(b) obliged entities, within the framework of customer due diligence in accordance with Chapter II;

(c) any person or organisation that can demonstrate a legitimate interest.

The persons or organisations referred to in point (c) shall access at least the name, the month and year of birth, the nationality and the country of residence of the beneficial owner as well as the nature and extent of the beneficial interest held.

For the purposes of this paragraph, access to the information on beneficial ownership shall be in accordance with data protection rules and may be subject to online registration and to the payment of a fee. The fees charged for obtaining the information shall not exceed the administrative costs thereof.

6. The central register referred to in paragraph 3 shall ensure timely and unrestricted access by competent authorities and FIUs, without alerting the entity concerned. It shall also allow timely access by obliged entities when taking customer due diligence measures.

7. Member States shall ensure that competent authorities and FIUs are able to provide the information referred to in paragraphs 1 and 3 to the competent authorities and to the FIUs of other Member States in a timely manner.

8. Member States shall require that obliged entities do not rely exclusively on the central register referred to in paragraph 3 to fulfil their customer due diligence requirements in accordance with Chapter II. Those requirements shall be fulfilled by using a risk-based approach.

9. Member States may provide for an exemption to the access referred to in points (b) and (c) of paragraph 5 to all or part of the information on the beneficial ownership on a case-by-case basis in exceptional circumstances, where such access would expose the beneficial owner to the risk of fraud, kidnapping, blackmail, violence or intimidation, or where the beneficial owner is a minor or otherwise incapable. Exemptions granted pursuant to this paragraph shall not apply to the credit institutions and financial institutions, and to obliged entities referred to in point (3)(b) of Article 2(1) that are public officials.

10. By 26 June 2019, the Commission shall submit a report to the European Parliament and to the Council assessing the conditions and the technical specifications and procedures for ensuring the safe and efficient interconnection of the central registers referred to in paragraph 3 via the European central platform established by Article 4a(1) of Directive 2009/101/EC. Where appropriate, that report shall be accompanied by a legislative proposal.

Article 31

1. Member States shall require that trustees of any express trust governed under their law obtain and hold adequate, accurate and up-to-date information on beneficial ownership regarding the trust. That information shall include the identity of:

(a) the settlor;

(b) the trustee(s);

(c) the protector (if any);

([1]) Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent (OJ L 258, 1.10.2009, p. 11).

(d) the beneficiaries or class of beneficiaries; and

(e) any other natural person exercising effective control over the trust.

2. Member States shall ensure that trustees disclose their status and provide the information referred to in paragraph 1 to obliged entities in a timely manner where, as a trustee, the trustee forms a business relationship or carries out an occasional transaction above the thresholds set out in points (b), (c) and (d) of Article 11.

3. Member States shall require that the information referred to in paragraph 1 can be accessed in a timely manner by competent authorities and FIUs.

4. Member States shall require that the information referred to in paragraph 1 is held in a central register when the trust generates tax consequences. The central register shall ensure timely and unrestricted access by competent authorities and FIUs, without alerting the parties to the trust concerned. It may also allow timely access by obliged entities, within the framework of customer due diligence in accordance with Chapter II. Member States shall notify to the Commission the characteristics of those national mechanisms.

5. Member States shall require that the information held in the central register referred to in paragraph 4 is adequate, accurate and up-to-date.

6. Member States shall ensure that obliged entities do not rely exclusively on the central register referred to in paragraph 4 to fulfil their customer due diligence requirements as laid down in Chapter II. Those requirements shall be fulfilled by using a risk-based approach.

7. Member States shall ensure that competent authorities and FIUs are able to provide the information referred to in paragraphs 1 and 4 to the competent authorities and to the FIUs of other Member States in a timely manner.

8. Member States shall ensure that the measures provided for in this Article apply to other types of legal arrangements having a structure or functions similar to trusts.

9. By 26 June 2019, the Commission shall submit a report to the European Parliament and to the Council assessing the conditions and the technical specifications and procedures for ensuring safe and efficient interconnection of the central registers. Where appropriate, that report shall be accompanied by a legislative proposal.

CHAPTER IV

REPORTING OBLIGATIONS

SECTION 1

General provisions

Article 32

1. Each Member State shall establish an FIU in order to prevent, detect and effectively combat money laundering and terrorist financing.

2. Member States shall notify the Commission in writing of the name and address of their respective FIUs.

3. Each FIU shall be operationally independent and autonomous, which means that the FIU shall have the authority and capacity to carry out its functions freely, including the ability to take autonomous decisions to analyse, request and disseminate specific information. The FIU as the central national unit shall be responsible for receiving and analysing suspicious transaction reports and other information relevant to money laundering, associated predicate offences or terrorist financing. The FIU shall be responsible for disseminating the results of its analyses and any additional relevant information to the competent authorities where there are grounds to suspect money laundering, associated predicate offences or terrorist financing. It shall be able to obtain additional information from obliged entities.

Member States shall provide their FIUs with adequate financial, human and technical resources in order to fulfil their tasks.

4. Member States shall ensure that their FIUs have access, directly or indirectly, in a timely manner, to the financial, administrative and law enforcement information that they require to fulfil their tasks properly. FIUs shall be able to respond to requests for information by competent authorities in their respective Member States when such requests for information are motivated by concerns relating to money laundering, associated predicate offences or terrorist financing. The decision on conducting the analysis or dissemination of information shall remain with the FIU.

5. Where there are objective grounds for assuming that the provision of such information would have a negative impact on ongoing investigations or analyses, or, in exceptional circumstances, where disclosure of the information would be clearly disproportionate to the legitimate interests of a natural or legal person or irrelevant with regard to the purposes for which it has been requested, the FIU shall be under no obligation to comply with the request for information.

6. Member States shall require competent authorities to provide feedback to the FIU about the use made of the information provided in accordance with this Article and about the outcome of the investigations or inspections performed on the basis of that information.

7. Member States shall ensure that the FIU is empowered to take urgent action, directly or indirectly, where there is a suspicion that a transaction is related to money laundering or terrorist financing, to suspend or withhold consent to a transaction that is proceeding, in order to analyse the transaction, confirm the suspicion and disseminate the results of the analysis to the competent authorities. The FIU shall be empowered to take such action, directly or indirectly, at the request of an FIU from another Member State for the periods and under the conditions specified in the national law of the FIU receiving the request.

8. The FIU's analysis function shall consist of the following:

(a) an operational analysis which focuses on individual cases and specific targets or on appropriate selected information, depending on the type and volume of the disclosures received and the expected use of the information after dissemination; and

(b) a strategic analysis addressing money laundering and terrorist financing trends and patterns.

Article 33

1. Member States shall require obliged entities, and, where applicable, their directors and employees, to cooperate fully by promptly:

(a) informing the FIU, including by filing a report, on their own initiative, where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing, and by promptly responding to requests by the FIU for additional information in such cases; and

(b) providing the FIU, directly or indirectly, at its request, with all necessary information, in accordance with the procedures established by the applicable law.

All suspicious transactions, including attempted transactions, shall be reported.

2. The person appointed in accordance with point (a) of Article 8(4) shall transmit the information referred to in paragraph 1 of this Article to the FIU of the Member State in whose territory the obliged entity transmitting the information is established.

Article 34

1. By way of derogation from Article 33(1), Member States may, in the case of obliged entities referred to in point (3)(a), (b) and (d) of Article 2(1), designate an appropriate self-regulatory body of the profession concerned as the authority to receive the information referred to in Article 33(1).

Without prejudice to paragraph 2, the designated self-regulatory body shall, in cases referred to in the first subparagraph of this paragraph, forward the information to the FIU promptly and unfiltered.

2. Member States shall not apply the obligations laid down in Article 33(1) to notaries, other independent legal professionals, auditors, external accountants and tax advisors only to the strict extent that such exemption relates to information that they receive from, or obtain on, one of their clients, in the course of ascertaining the legal position of their client, or performing their task of defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings, whether such information is received or obtained before, during or after such proceedings.

Article 35

1. Member States shall require obliged entities to refrain from carrying out transactions which they know or suspect to be related to proceeds of criminal activity or to terrorist financing until they have completed the necessary action in accordance with point (a) of the first subparagraph of Article 33(1) and have complied with any further specific instructions from the FIU or the competent authorities in accordance with the law of the relevant Member State.

2. Where refraining from carrying out transactions referred to in paragraph 1 is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected operation, the obliged entities concerned shall inform the FIU immediately afterwards.

Article 36

1. Member States shall ensure that if, in the course of checks carried out on the obliged entities by the competent authorities referred to in Article 48, or in any other way, those authorities discover facts that could be related to money laundering or to terrorist financing, they shall promptly inform the FIU.

2. Member States shall ensure that supervisory bodies empowered by law or regulation to oversee the stock, foreign exchange and financial derivatives markets inform the FIU if they discover facts that could be related to money laundering or terrorist financing.

Article 37

Disclosure of information in good faith by an obliged entity or by an employee or director of such an obliged entity in accordance with Articles 33 and 34 shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the obliged entity or its directors or employees in liability of any kind even in circumstances where they were not precisely aware of the underlying criminal activity and regardless of whether illegal activity actually occurred.

Article 38

Member States shall ensure that individuals, including employees and representatives of the obliged entity, who report suspicions of money laundering or terrorist financing internally or to the FIU, are protected from being exposed to threats or hostile action, and in particular from adverse or discriminatory employment actions.

SECTION 2

Prohibition of disclosure

Article 39

1. Obliged entities and their directors and employees shall not disclose to the customer concerned or to other third persons the fact that information is being, will be or has been transmitted in accordance with Article 33 or 34 or that a money laundering or terrorist financing analysis is being, or may be, carried out.

2. The prohibition laid down in paragraph 1 shall not include disclosure to the competent authorities, including the self-regulatory bodies, or disclosure for law enforcement purposes.

3. The prohibition laid down in paragraph 1 shall not prevent disclosure between the credit institutions and financial institutions or between those institutions and their branches and majority-owned subsidiaries located in third countries, provided that those branches and majority-owned subsidiaries fully comply with the group-wide policies and procedures, including procedures for sharing information within the group, in accordance with Article 45, and that the group-wide policies and procedures comply with the requirements laid down in this Directive.

4. The prohibition laid down in paragraph 1 shall not prevent disclosure between the obliged entities as referred to in point (3)(a) and (b) of Article 2(1), or entities from third countries which impose requirements equivalent to those laid down in this Directive, who perform their professional activities, whether as employees or not, within the same legal person or a larger structure to which the person belongs and which shares common ownership, management or compliance control.

5. For obliged entities referred to in points (1), (2), (3)(a) and (b) of Article 2(1) in cases relating to the same customer and the same transaction involving two or more obliged entities, the prohibition laid down in paragraph 1 of this Article shall not prevent disclosure between the relevant obliged entities provided that they are from a Member State, or entities in a third country which imposes requirements equivalent to those laid down in this Directive, and that they are from the same professional category and are subject to obligations as regards professional secrecy and personal data protection.

6. Where the obliged entities referred to in point (3)(a) and (b) of Article 2(1) seek to dissuade a client from engaging in illegal activity, that shall not constitute disclosure within the meaning of paragraph 1 of this Article.

CHAPTER V

DATA PROTECTION, RECORD-RETENTION AND STATISTICAL DATA

Article 40

1. Member States shall require obliged entities to retain the following documents and information in accordance with national law for the purpose of preventing, detecting and investigating, by the FIU or by other competent authorities, possible money laundering or terrorist financing:

(a) in the case of customer due diligence, a copy of the documents and information which are necessary to comply with the customer due diligence requirements laid down in Chapter II, for a period of five years after the end of the business relationship with their customer or after the date of an occasional transaction;

(b) the supporting evidence and records of transactions, consisting of the original documents or copies admissible in judicial proceedings under the applicable national law, which are necessary to identify transactions, for a period of five years after the end of a business relationship with their customer or after the date of an occasional transaction.

Upon expiry of the retention periods referred to in the first subparagraph, Member States shall ensure that obliged entities delete personal data, unless otherwise provided for by national law, which shall determine under which circumstances obliged entities may or shall further retain data. Member States may allow or require further retention after they have carried out a thorough assessment of the necessity and proportionality of such further retention and consider it to be justified as necessary for the prevention, detection or investigation of money laundering or terrorist financing. That further retention period shall not exceed five additional years.

2. Where, on 25 June 2015, legal proceedings concerned with the prevention, detection, investigation or prosecution of suspected money laundering or terrorist financing are pending in a Member State, and an obliged entity holds information or documents relating to those pending proceedings, the obliged entity may retain that information or those documents, in accordance with national law, for a period of five years from 25 June 2015. Member States may, without prejudice to national criminal law on evidence applicable to ongoing criminal investigations and legal proceedings, allow or require the retention of such information or documents for a further period of five years where the necessity and proportionality of such further retention has been established for the prevention, detection, investigation or prosecution of suspected money laundering or terrorist financing.

Article 41

1. The processing of personal data under this Directive is subject to Directive 95/46/EC, as transposed into national law. Personal data that is processed pursuant to this Directive by the Commission or by the ESAs is subject to Regulation (EC) No 45/2001.

2. Personal data shall be processed by obliged entities on the basis of this Directive only for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 and shall not be further processed in a way that is incompatible with those purposes. The processing of personal data on the basis of this Directive for any other purposes, such as commercial purposes, shall be prohibited.

3. Obliged entities shall provide new clients with the information required pursuant to Article 10 of Directive 95/46/EC before establishing a business relationship or carrying out an occasional transaction. That information shall, in particular, include a general notice concerning the legal obligations of obliged entities under this Directive to process personal data for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 of this Directive.

4. In applying the prohibition of disclosure laid down in Article 39(1), Member States shall adopt legislative measures restricting, in whole or in part, the data subject's right of access to personal data relating to him or her to the extent that such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned to:

(a) enable the obliged entity or competent national authority to fulfil its tasks properly for the purposes of this Directive; or

(b) avoid obstructing official or legal inquiries, analyses, investigations or procedures for the purposes of this Directive and to ensure that the prevention, investigation and detection of money laundering and terrorist financing is not jeopardised.

Article 42

Member States shall require that their obliged entities have systems in place that enable them to respond fully and speedily to enquiries from their FIU or from other authorities, in accordance with their national law, as to whether they are maintaining or have maintained, during a five-year period prior to that enquiry a business relationship with specified persons, and on the nature of that relationship, through secure channels and in a manner that ensures full confidentiality of the enquiries.

Article 43

The processing of personal data on the basis of this Directive for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 shall be considered to be a matter of public interest under Directive 95/46/EC.

Article 44

1. Member States shall, for the purposes of contributing to the preparation of risk assessments pursuant to Article 7, ensure that they are able to review the effectiveness of their systems to combat money laundering or terrorist financing by maintaining comprehensive statistics on matters relevant to the effectiveness of such systems.

2. The statistics referred to in paragraph 1 shall include:

(a) data measuring the size and importance of the different sectors which fall within the scope of this Directive, including the number of entities and persons and the economic importance of each sector;

(b) data measuring the reporting, investigation and judicial phases of the national AML/CFT regime, including the number of suspicious transaction reports made to the FIU, the follow-up given to those reports and, on an annual basis, the number of cases investigated, the number of persons prosecuted, the number of persons convicted for money laundering or terrorist financing offences, the types of predicate offences, where such information is available, and the value in euro of property that has been frozen, seized or confiscated;

(c) if available, data identifying the number and percentage of reports resulting in further investigation, together with the annual report to obliged entities detailing the usefulness and follow-up of the reports they presented;

(d) data regarding the number of cross-border requests for information that were made, received, refused and partially or fully answered by the FIU.

3. Member States shall ensure that a consolidated review of their statistics is published.

4. Member States shall transmit to the Commission the statistics referred to in paragraph 2.

CHAPTER VI

POLICIES, PROCEDURES AND SUPERVISION

SECTION 1

Internal procedures, training and feedback

Article 45

1. Member States shall require obliged entities that are part of a group to implement group-wide policies and procedures, including data protection policies and policies and procedures for sharing information within the group for AML/CFT purposes. Those policies and procedures shall be implemented effectively at the level of branches and majority-owned subsidiaries in Member States and third countries.

2. Member States shall require that obliged entities that operate establishments in another Member State ensure that those establishments respect the national provisions of that other Member State transposing this Directive.

3. Member States shall ensure that where obliged entities have branches or majority-owned subsidiaries located in third countries where the minimum AML/CFT requirements are less strict than those of the Member State, their branches and majority-owned subsidiaries located in the third country implement the requirements of the Member State, including data protection, to the extent that the third country's law so allows.

4. The Member States and the ESAs shall inform each other of instances in which a third country's law does not permit the implementation of the policies and procedures required under paragraph 1. In such cases, coordinated action may be taken to pursue a solution.

5. Member States shall require that, where a third country's law does not permit the implementation of the policies and procedures required under paragraph 1, obliged entities ensure that branches and majority-owned subsidiaries in that third country apply additional measures to effectively handle the risk of money laundering or terrorist financing, and inform the competent authorities of their home Member State. If the additional measures are not sufficient, the competent authorities of the home Member State shall exercise additional supervisory actions, including requiring that the group does not establish or that it terminates business relationships, and does not undertake transactions and, where necessary, requesting the group to close down its operations in the third country.

6. The ESAs shall develop draft regulatory technical standards specifying the type of additional measures referred to in paragraph 5 and the minimum action to be taken by credit institutions and financial institutions where a third country's law does not permit the implementation of the measures required under paragraphs 1 and 3.

The ESAs shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by 26 December 2016.

7. Power is delegated to the Commission to adopt the regulatory technical standards referred to in paragraph 6 of this Article in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

8. Member States shall ensure that the sharing of information within the group is allowed. Information on suspicions that funds are the proceeds of criminal activity or are related to terrorist financing reported to the FIU shall be shared within the group, unless otherwise instructed by the FIU.

9. Member States may require electronic money issuers as defined in point (3) of Article 2 of Directive 2009/110/EC and payment service providers as defined in point (9) of Article 4 of Directive 2007/64/EC established on their territory in forms other than a branch, and whose head office is situated in another Member State, to appoint a central contact point in their territory to ensure, on behalf of the appointing institution, compliance with AML/CFT rules and to facilitate supervision by competent authorities, including by providing competent authorities with documents and information on request.

10. The ESAs shall develop draft regulatory technical standards on the criteria for determining the circumstances in which the appointment of a central contact point pursuant to paragraph 9 is appropriate, and what the functions of the central contact points should be.

The ESAs shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by 26 June 2017.

11. Power is delegated to the Commission to adopt the regulatory technical standards referred to in paragraph 10 of this Article in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

Article 46

1. Member States shall require that obliged entities take measures proportionate to their risks, nature and size so that their employees are aware of the provisions adopted pursuant to this Directive, including relevant data protection requirements.

Those measures shall include participation of their employees in special ongoing training programmes to help them recognise operations which may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases.

Where a natural person falling within any of the categories listed in point (3) of Article 2(1) performs professional activities as an employee of a legal person, the obligations in this Section shall apply to that legal person rather than to the natural person.

2. Member States shall ensure that obliged entities have access to up-to-date information on the practices of money launderers and financers of terrorism and on indications leading to the recognition of suspicious transactions.

3. Member States shall ensure that, where practicable, timely feedback on the effectiveness of and follow-up to reports of suspected money laundering or terrorist financing is provided to obliged entities.

4. Member States shall require that, where applicable, obliged entities identify the member of the management board who is responsible for the implementation of the laws, regulations and administrative provisions necessary to comply with this Directive.

SECTION 2

Supervision

Article 47

1. Member States shall provide that currency exchange and cheque cashing offices and trust or company service providers be licensed or registered and providers of gambling services be regulated.

2. Member States shall require competent authorities to ensure that the persons who hold a management function in the entities referred to in paragraph 1, or are the beneficial owners of such entities, are fit and proper persons.

3. With respect to the obliged entities referred to in point (3)(a), (b) and (d) of Article 2(1), Member States shall ensure that competent authorities take the necessary measures to prevent criminals convicted in relevant areas or their associates from holding a management function in or being the beneficial owners of those obliged entities.

Article 48

1. Member States shall require the competent authorities to monitor effectively, and to take the measures necessary to ensure, compliance with this Directive.

2. Member States shall ensure that the competent authorities have adequate powers, including the power to compel the production of any information that is relevant to monitoring compliance and perform checks, and have adequate financial, human and technical resources to perform their functions. Member States shall ensure that staff of those authorities maintain high professional standards, including standards of confidentiality and data protection, that they are of high integrity and are appropriately skilled.

3. In the case of credit institutions, financial institutions, and providers of gambling services, competent authorities shall have enhanced supervisory powers.

4. Member States shall ensure that competent authorities of the Member State in which the obliged entity operates establishments supervise that those establishments respect the national provisions of that Member State transposing this Directive. In the case of the establishments referred to in Article 45(9), such supervision may include the taking of appropriate and proportionate measures to address serious failings that require immediate remedies. Those measures shall be temporary and be terminated when the failings identified are addressed, including with the assistance of or in cooperation with the competent authorities of the home Member State of the obliged entity, in accordance with Article 45(2).

5. Member States shall ensure that the competent authorities of the Member State in which the obliged entity operates establishments shall cooperate with the competent authorities of the Member State in which the obliged entity has its head office, to ensure effective supervision of the requirements of this Directive.

6. Member States shall ensure that when applying a risk-based approach to supervision, the competent authorities:

(a) have a clear understanding of the risks of money laundering and terrorist financing present in their Member State;

(b) have on-site and off-site access to all relevant information on the specific domestic and international risks associated with customers, products and services of the obliged entities; and

(c) base the frequency and intensity of on-site and off-site supervision on the risk profile of obliged entities, and on the risks of money laundering and terrorist financing in that Member State.

7. The assessment of the money laundering and terrorist financing risk profile of obliged entities, including the risks of non-compliance, shall be reviewed both periodically and when there are major events or developments in their management and operations.

8. Member States shall ensure that competent authorities take into account the degree of discretion allowed to the obliged entity, and appropriately review the risk assessments underlying this discretion, and the adequacy and implementation of its internal policies, controls and procedures.

9. In the case of the obliged entities referred to in point (3)(a), (b) and (d) of Article 2(1), Member States may allow the functions referred to in paragraph 1 of this Article to be performed by self-regulatory bodies, provided that those self-regulatory bodies comply with paragraph 2 of this Article.

10. By 26 June 2017, the ESAs shall issue guidelines addressed to competent authorities in accordance with Article 16 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 on the characteristics of a risk-based approach to supervision and the steps to be taken when conducting supervision on a risk-based basis. Specific account shall be taken of the nature and size of the business, and, where appropriate and proportionate, specific measures shall be laid down.

SECTION 3

Cooperation

Subsection I

National cooperation

Article 49

Member States shall ensure that policy makers, the FIUs, supervisors and other competent authorities involved in AML/CFT have effective mechanisms to enable them to cooperate and coordinate domestically concerning the development and implementation of policies and activities to combat money laundering and terrorist financing, including with a view to fulfilling their obligation under Article 7.

Subsection II

Cooperation with the ESAs

Article 50

The competent authorities shall provide the ESAs with all the information necessary to allow them to carry out their duties under this Directive.

Subsection III

Cooperation between FIUs and with the Commission

Article 51

The Commission may lend such assistance as may be needed to facilitate coordination, including the exchange of information between FIUs within the Union. It may regularly convene meetings of the EU FIUs' Platform composed of representatives from Member States' FIUs, in order to facilitate cooperation among FIUs, exchange views and provide advice on implementation issues relevant for FIUs and reporting entities as well as on cooperation-related issues such as effective FIU cooperation, the identification of suspicious transactions with a cross-border dimension, the standardisation of reporting formats through the FIU.net or its successor, the joint analysis of cross-border cases, and the identification of trends and factors relevant to assessing the risks of money laundering and terrorist financing at national and supranational level.

Article 52

Member States shall ensure that FIUs cooperate with each other to the greatest extent possible, regardless of their organisational status.

Article 53

1. Member States shall ensure that FIUs exchange, spontaneously or upon request, any information that may be relevant for the processing or analysis of information by the FIU related to money laundering or terrorist financing and the natural or legal person involved, even if the type of predicate offences that may be involved is not identified at the time of the exchange.

A request shall contain the relevant facts, background information, reasons for the request and how the information sought will be used. Different exchange mechanisms may apply if so agreed between the FIUs, in particular as regards exchanges through the FIU.net or its successor.

When an FIU receives a report pursuant to point (a) of the first subparagraph of Article 33(1) which concerns another Member State, it shall promptly forward it to the FIU of that Member State.

2. Member States shall ensure that the FIU to whom the request is made is required to use the whole range of its available powers which it would normally use domestically for receiving and analysing information when it replies to a request for information referred to in paragraph 1 from another FIU. The FIU to whom the request is made shall respond in a timely manner.

When an FIU seeks to obtain additional information from an obliged entity established in another Member State which operates on its territory, the request shall be addressed to the FIU of the Member State in whose territory the obliged entity is established. That FIU shall transfer requests and answers promptly.

3. An FIU may refuse to exchange information only in exceptional circumstances where the exchange could be contrary to fundamental principles of its national law. Those exceptions shall be specified in a way which prevents misuse of, and undue limitations on, the free exchange of information for analytical purposes.

Article 54

Information and documents received pursuant to Articles 52 and 53 shall be used for the accomplishment of the FIU's tasks as laid down in this Directive. When exchanging information and documents pursuant to Articles 52 and 53, the transmitting FIU may impose restrictions and conditions for the use of that information. The receiving FIU shall comply with those restrictions and conditions.

Article 55

1. Member States shall ensure that the information exchanged pursuant to Articles 52 and 53 is used only for the purpose for which it was sought or provided and that any dissemination of that information by the receiving FIU to any other authority, agency or department, or any use of this information for purposes beyond those originally approved, is made subject to the prior consent by the FIU providing the information.

2. Member States shall ensure that the requested FIU's prior consent to disseminate the information to competent authorities is granted promptly and to the largest extent possible. The requested FIU shall not refuse its consent to such dissemination unless this would fall beyond the scope of application of its AML/CFT provisions, could lead to impairment of a criminal investigation, would be clearly disproportionate to the legitimate interests of a natural or legal person or the Member State of the requested FIU, or would otherwise not be in accordance with fundamental principles of national law of that Member State. Any such refusal to grant consent shall be appropriately explained.

Article 56

1. Member States shall require their FIUs to use protected channels of communication between themselves and encourage the use of the FIU.net or its successor.

2. Member States shall ensure that, in order to fulfil their tasks as laid down in this Directive, their FIUs cooperate in the application of state-of-the-art technologies in accordance with their national law. Those technologies shall allow FIUs to match their data with that of other FIUs in an anonymous way by ensuring full protection of personal data with the aim of detecting subjects of the FIU's interests in other Member States and identifying their proceeds and funds.

Article 57

Differences between national law definitions of tax crimes shall not impede the ability of FIUs to exchange information or provide assistance to another FIU, to the greatest extent possible under their national law.

SECTION 4

Sanctions

Article 58

1. Member States shall ensure that obliged entities can be held liable for breaches of national provisions transposing this Directive in accordance with this Article and Articles 59 to 61. Any resulting sanction or measure shall be effective, proportionate and dissuasive.

2. Without prejudice to the right of Member States to provide for and impose criminal sanctions, Member States shall lay down rules on administrative sanctions and measures and ensure that their competent authorities may impose such sanctions and measures with respect to breaches of the national provisions transposing this Directive, and shall ensure that they are applied.

Member States may decide not to lay down rules for administrative sanctions or measures for breaches which are subject to criminal sanctions in their national law. In that case, Member States shall communicate to the Commission the relevant criminal law provisions.

3. Member States shall ensure that where obligations apply to legal persons in the event of a breach of national provisions transposing this Directive, sanctions and measures can be applied to the members of the management body and to other natural persons who under national law are responsible for the breach.

4. Member States shall ensure that the competent authorities have all the supervisory and investigatory powers that are necessary for the exercise of their functions.

5. Competent authorities shall exercise their powers to impose administrative sanctions and measures in accordance with this Directive, and with national law, in any of the following ways:

(a) directly;

(b) in collaboration with other authorities;

(c) under their responsibility by delegation to such other authorities;

(d) by application to the competent judicial authorities.

In the exercise of their powers to impose administrative sanctions and measures, competent authorities shall cooperate closely in order to ensure that those administrative sanctions or measures produce the desired results and coordinate their action when dealing with cross-border cases.

Article 59

1. Member States shall ensure that this Article applies at least to breaches on the part of obliged entities that are serious, repeated, systematic, or a combination thereof, of the requirements laid down in:

(a) Articles 10 to 24 (customer due diligence);

(b) Articles 33, 34 and 35 (suspicious transaction reporting);

(c) Article 40 (record-keeping); and

(d) Articles 45 and 46 (internal controls).

2. Member States shall ensure that in the cases referred to in paragraph 1, the administrative sanctions and measures that can be applied include at least the following:

(a) a public statement which identifies the natural or legal person and the nature of the breach;

(b) an order requiring the natural or legal person to cease the conduct and to desist from repetition of that conduct;

(c) where an obliged entity is subject to an authorisation, withdrawal or suspension of the authorisation;

(d) a temporary ban against any person discharging managerial responsibilities in an obliged entity, or any other natural person, held responsible for the breach, from exercising managerial functions in obliged entities;

(e) maximum administrative pecuniary sanctions of at least twice the amount of the benefit derived from the breach where that benefit can be determined, or at least EUR 1 000 000.

3. Member States shall ensure that, by way of derogation from paragraph 2(e), where the obliged entity concerned is a credit institution or financial institution, the following sanctions can also be applied:

(a) in the case of a legal person, maximum administrative pecuniary sanctions of at least EUR 5 000 000 or 10 % of the total annual turnover according to the latest available accounts approved by the management body; where the obliged entity is a parent undertaking or a subsidiary of a parent undertaking which is required to prepare consolidated financial accounts in accordance with Article 22 of Directive 2013/34/EU, the relevant total annual turnover shall be the total annual turnover or the corresponding type of income in accordance with the relevant accounting Directives according to the last available consolidated accounts approved by the management body of the ultimate parent undertaking;

(b) in the case of a natural person, maximum administrative pecuniary sanctions of at least EUR 5 000 000, or in the Member States whose currency is not the euro, the corresponding value in the national currency on 25 June 2015.

4. Member States may empower competent authorities to impose additional types of administrative sanctions in addition to those referred to in points (a) to (d) of paragraph 2 or to impose administrative pecuniary sanctions exceeding the amounts referred to in point (e) of paragraph 2 and in paragraph 3.

Article 60

1. Member States shall ensure that a decision imposing an administrative sanction or measure for breach of the national provisions transposing this Directive against which there is no appeal shall be published by the competent authorities on their official website immediately after the person sanctioned is informed of that decision. The publication shall include at least information on the type and nature of the breach and the identity of the persons responsible. Member States shall not be obliged to apply this subparagraph to decisions imposing measures that are of an investigatory nature.

Where the publication of the identity of the persons responsible as referred to in the first subparagraph or the personal data of such persons is considered by the competent authority to be disproportionate following a case-by-case assessment conducted on the proportionality of the publication of such data, or where publication jeopardises the stability of financial markets or an on-going investigation, competent authorities shall:

(a) delay the publication of the decision to impose an administrative sanction or measure until the moment at which the reasons for not publishing it cease to exist;

(b) publish the decision to impose an administrative sanction or measure on an anonymous basis in a manner in accordance with national law, if such anonymous publication ensures an effective protection of the personal data concerned; in the case of a decision to publish an administrative sanction or measure on an anonymous basis, the publication of the relevant data may be postponed for a reasonable period of time if it is foreseen that within that period the reasons for anonymous publication shall cease to exist;

(c) not publish the decision to impose an administrative sanction or measure at all in the event that the options set out in points (a) and (b) are considered insufficient to ensure:

(i) that the stability of financial markets would not be put in jeopardy; or

(ii) the proportionality of the publication of the decision with regard to measures which are deemed to be of a minor nature.

2. Where Member States permit publication of decisions against which there is an appeal, competent authorities shall also publish, immediately, on their official website such information and any subsequent information on the outcome of such appeal. Moreover, any decision annulling a previous decision to impose an administrative sanction or a measure shall also be published.

3. Competent authorities shall ensure that any publication in accordance with this Article shall remain on their official website for a period of five years after its publication. However, personal data contained in the publication shall only be kept on the official website of the competent authority for the period which is necessary in accordance with the applicable data protection rules.

4. Member States shall ensure that when determining the type and level of administrative sanctions or measures, the competent authorities shall take into account all relevant circumstances, including where applicable:

(a) the gravity and the duration of the breach;

(b) the degree of responsibility of the natural or legal person held responsible;

(c) the financial strength of the natural or legal person held responsible, as indicated for example by the total turnover of the legal person held responsible or the annual income of the natural person held responsible;

(d) the benefit derived from the breach by the natural or legal person held responsible, insofar as it can be determined;

(e) the losses to third parties caused by the breach, insofar as they can be determined;

(f) the level of cooperation of the natural or legal person held responsible with the competent authority;

(g) previous breaches by the natural or legal person held responsible.

5. Member States shall ensure that legal persons can be held liable for the breaches referred to in Article 59(1) committed for their benefit by any person, acting individually or as part of an organ of that legal person, and having a leading position within the legal person based on any of the following:

(a) power to represent the legal person;

(b) authority to take decisions on behalf of the legal person; or

(c) authority to exercise control within the legal person.

6. Member States shall also ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 5 of this Article has made it possible to commit one of the breaches referred to in Article 59(1) for the benefit of that legal person by a person under its authority.

Article 61

1. Member States shall ensure that competent authorities establish effective and reliable mechanisms to encourage the reporting to competent authorities of potential or actual breaches of the national provisions transposing this Directive.

2. The mechanisms referred to in paragraph 1 shall include at least:

(a) specific procedures for the receipt of reports on breaches and their follow-up;

(b) appropriate protection for employees or persons in a comparable position, of obliged entities who report breaches committed within the obliged entity;

(c) appropriate protection for the accused person;

(d) protection of personal data concerning both the person who reports the breaches and the natural person who is allegedly responsible for a breach, in compliance with the principles laid down in Directive 95/46/EC;

(e) clear rules that ensure that confidentiality is guaranteed in all cases in relation to the person who reports the breaches committed within the obliged entity, unless disclosure is required by national law in the context of further investigations or subsequent judicial proceedings.

3. Member States shall require obliged entities to have in place appropriate procedures for their employees, or persons in a comparable position, to report breaches internally through a specific, independent and anonymous channel, proportionate to the nature and size of the obliged entity concerned.

Article 62

1. Member States shall ensure that their competent authorities inform the ESAs of all administrative sanctions and measures imposed in accordance with Articles 58 and 59 on credit institutions and financial institutions, including of any appeal in relation thereto and the outcome thereof.

2. Member States shall ensure that their competent authorities, in accordance with their national law, check the existence of a relevant conviction in the criminal record of the person concerned. Any exchange of information for those purposes shall be carried out in accordance with Decision 2009/316/JHA and Framework Decision 2009/315/JHA as implemented in national law.

3. The ESAs shall maintain a website with links to each competent authority's publication of administrative sanctions and measures imposed in accordance with Article 60 on credit institutions and financial institutions, and shall show the time period for which each Member State publishes administrative sanctions and measures.

CHAPTER VII

FINAL PROVISIONS

Article 63

Point (d) of paragraph 2 of Article 25 of Regulation (EU) No 648/2012 of the European Parliament and the Council ([1]) is replaced by the following:

'(d) the CCP is established or authorised in a third country that is not considered, by the Commission in accordance with Directive (EU) 2015/849 of the European Parliament and of the Council (*), as having strategic deficiencies in its national anti-money laundering and counter financing of terrorism regime that poses significant threats to the financial system of the Union.

(*) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73).'.

Article 64

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 9 shall be conferred on the Commission for an indeterminate period of time from 25 June 2015.

3. The power to adopt delegated acts referred to in Article 9 may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect on the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 9 shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of one month of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by one month at the initiative of the European Parliament or of the Council.

Article 65

By 26 June 2019, the Commission shall draw up a report on the implementation of this Directive and submit it to the European Parliament and to the Council.

Article 66

Directives 2005/60/EC and 2006/70/EC are repealed with effect from 26 June 2017.

References to the repealed Directives shall be construed as references to this Directive and shall be read in accordance with the correlation table set out in Annex IV.

Article 67

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 26 June 2017. They shall immediately communicate the text of those measures to the Commission.

When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

([1]) Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

Article 68

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Article 69

This Directive is addressed to the Member States.

Done at Strasbourg, 20 May 2015.

For the European Parliament	*For the Council*
The President	*The President*
M. SCHULZ	Z. KALNIŅA-LUKAŠEVICA

ANNEX I

The following is a non-exhaustive list of risk variables that obliged entities shall consider when determining to what extent to apply customer due diligence measures in accordance with Article 13(3):

(i) the purpose of an account or relationship;

(ii) the level of assets to be deposited by a customer or the size of transactions undertaken;

(iii) the regularity or duration of the business relationship.

ANNEX II

The following is a non-exhaustive list of factors and types of evidence of potentially lower risk referred to in Article 16:

(1) Customer risk factors:

(a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;

(b) public administrations or enterprises;

(c) customers that are resident in geographical areas of lower risk as set out in point (3);

(2) Product, service, transaction or delivery channel risk factors:

(a) life insurance policies for which the premium is low;

(b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;

(c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;

(d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;

(e) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money);

(3) Geographical risk factors:

(a) Member States;

(b) third countries having effective AML/CFT systems;

(c) third countries identified by credible sources as having a low level of corruption or other criminal activity;

(d) third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements.

ANNEX III

The following is a non-exhaustive list of factors and types of evidence of potentially higher risk referred to in Article 18(3):

(1) Customer risk factors:

(a) the business relationship is conducted in unusual circumstances;

(b) customers that are resident in geographical areas of higher risk as set out in point (3);

(c) legal persons or arrangements that are personal asset-holding vehicles;

(d) companies that have nominee shareholders or shares in bearer form;

(e) businesses that are cash-intensive;

(f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

(2) Product, service, transaction or delivery channel risk factors:

(a) private banking;

(b) products or transactions that might favour anonymity;

(c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;

(d) payment received from unknown or unassociated third parties;

(e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;

(3) Geographical risk factors:

(a) without prejudice to Article 9, countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;

(b) countries identified by credible sources as having significant levels of corruption or other criminal activity;

(c) countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;

(d) countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

ANNEX IV

Correlation table

This Directive	Directive 2005/60/EC	Directive 2006/70/EC
—		Article 1
—		Article 3
—		Article 5
—		Article 6
—		Article 7
Article 1	Article 1	
Article 2	Article 2	
Article 2(3) to (9)		Article 4
Article 3	Article 3	
Article 3(9), (10) and (11)		Article 2(1), (2) and (3)
Article 4	Article 4	
Article 5	Article 5	
Articles 6 to 8	—	
Article 10	Article 6	
Article 11	Article 7	
Article 13	Article 8	
Article 14	Article 9	
Article 11(d)	Article 10(1)	
—	Article 10(2)	
Articles 15, 16 and 17	Article 11	
—	Article 12	
Articles 18 to 24	Article 13	
Article 22		Article 2(4)
Article 25	Article 14	
—	Article 15	
Article 26	Article 16	
—	Article 17	
Article 27	Article 18	
Article 28	—	
Article 29	Article 19	
Article 30	—	
Article 31	—	
—	Article 20	
Article 32	Article 21	
Article 33	Article 22	

This Directive	Directive 2005/60/EC	Directive 2006/70/EC
Article 34	Article 23	
Article 35	Article 24	
Article 36	Article 25	
Article 37	Article 26	
Article 38	Article 27	
Article 39	Article 28	
—	Article 29	
Article 40	Article 30	
Article 45	Article 31	
Article 42	Article 32	
Article 44	Article 33	
Article 45	Article 34	
Article 46	Article 35	
Article 47	Article 36	
Article 48	Article 37	
Article 49	—	
Article 50	Article 37a	
Article 51	Article 38	
Articles 52 to 57	—	
Articles 58 to 61	Article 39	
—	Article 40	
—	Article 41	
—	Article 41a	
—	Article 41b	
Article 65	Article 42	
—	Article 43	
Article 66	Article 44	
Article 67	Article 45	
Article 68	Article 46	
Article 69	Article 47	

Exhibit 5

View the 2019 Nevada Revised Statutes | View Previous Versions of the Nevada Revised Statutes

2015 Nevada Revised Statutes
Chapter 463 - Licensing and Control of Gaming
NRS 463.01595 - “Gaming salon” defined.

Universal Citation: NV Rev Stat § 463.01595 (2015)

“Gaming salon” means an enclosed gaming facility which is located anywhere on the property of a resort hotel that holds a nonrestricted license, admission to which facility is based upon the financial criteria of a patron as established by the licensee and approved by the Board.

(Added to NRS by 2003, 1169)

View the 2019 Nevada Revised Statutes | View Previous Versions of the Nevada Revised Statutes

2015 Nevada Revised Statutes
Chapter 463 - Licensing and Control of Gaming
NRS 463.4071 - Application for license to operate gaming salon; fee; costs for investigation.

Universal Citation: NV Rev Stat § 463.4071 (2015)

1. A licensee may apply to the Board, on forms prescribed by the Board, for a license to operate a gaming salon.

2. A nonrefundable application fee in the amount of $5,000 must accompany the application for a license to operate a gaming salon.

3. An applicant must pay the costs incurred by the Board for investigation of an application.

(Added to NRS by 2001, 896; A 2003, 1170)

View the 2019 Nevada Revised Statutes | View Previous Versions of the Nevada Revised Statutes

2015 Nevada Revised Statutes
Chapter 463 - Licensing and Control of Gaming
NRS 463.4073 - Regulations establishing policies and procedures for approval of license to operate gaming salon and standards of operation.

Universal Citation: NV Rev Stat § 463.4073 (2015)

The Commission shall, with the advice and assistance of the Board, adopt regulations setting forth:

1. The policies and procedures for approval of a license to operate a gaming salon.

2. The standards of operation for a gaming salon, including, without limitation, policies and procedures governing:

(a) Surveillance and security systems.

(b) The games offered. The regulations must provide that the games offered must include table games and may include slot machines.

(c) Minimum wagers for any game offered. The regulations must provide that minimum wagers for slot machines must not be less than $500.

(Added to NRS by 2001, 896; A 2003, 1171)

View the 2019 Nevada Revised Statutes | View Previous Versions of the Nevada Revised Statutes

2015 Nevada Revised Statutes
Chapter 463 - Licensing and Control of Gaming
NRS 463.4076 - Admission of patrons to gaming salon: Conditions; restrictions; resolution of disputes.

Universal Citation: NV Rev Stat § 463.4076 (2015)

1. The admission of a patron to a gaming salon:

(a) May be restricted on the basis of the financial criteria of the patron as established by the licensee and approved by the Board; and

(b) Must not be restricted on the basis of the race, color, religion, national origin, ancestry, physical disability or sex of the patron.

2. Any unresolved dispute with a patron concerning restriction of admission to a gaming salon shall be deemed a dispute as to the manner in which a game is conducted pursuant to NRS 463.362 and must be resolved pursuant to NRS 463.362 to 463.366, inclusive.

(Added to NRS by 2001, 896; A 2003, 1171)