The CPD Fest 2020

Anti-Money Laundering for 2021

Presenter:
Mike O'Halloran, Des O'Neill - OmniPro

Sponsored by :-

www.CPDStore.com

Core Technical Online CPD for Irish Accountants
Tax, Audit, Financial Reporting, Insolvency, Company Law, Regulation, Management Accounting & Business Skills

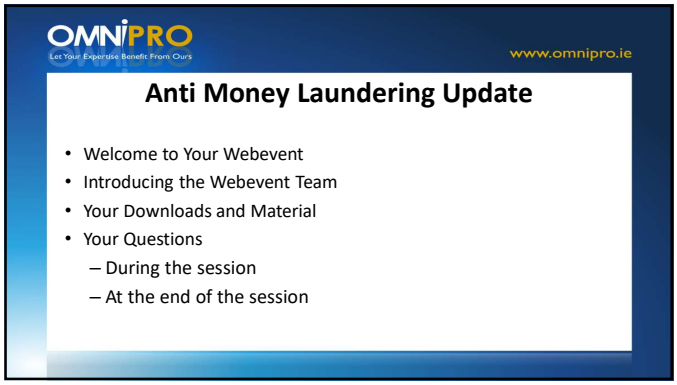
OmniPro Education & Training
Main Street, Ferns, Enniscorthy, Co. Wexford
053 910 0000
www.omnipro.ie info@omnipro.ie

A Personalised CPD Certificate of Completion will be forwarded to you upon completion of this course.
These notes do not serve as proof of completion alone.

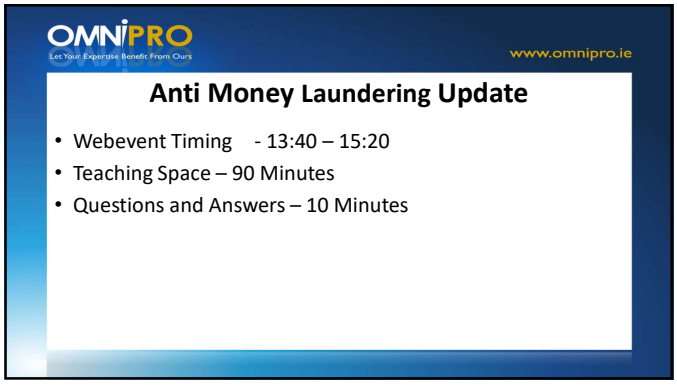
Table of Contents:


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

1


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Anti Money Laundering Update
• Welcome to Your Webevent
• Introducing the Webevent Team
• Your Downloads and Material
• Your Questions
– During the session
– At the end of the session

2


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Anti Money Laundering Update
• Webevent Timing - 13:40 – 15:20
• Teaching Space – 90 Minutes
• Questions and Answers – 10 Minutes

3

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

Anti Money Laundering Update

- **Topic 1:** Applicable legislation and what is money laundering
- **Topic 2:** Role of the MLRO
- **Topic 3:** Reporting Procedures and Privilege Exemption
- **Topic 4**: Risk Assessment and Customer Due Diligence
- **Topic 5:** Update on COVID-19 and legislative updates

4

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

What is Money Laundering

- Defined under the 2010 Act as:
  - All forms of handling or possessing the proceeds of criminal conduct where the person knows or believes such proceeds is or represents the proceeds of criminal conduct
  - The proceeds of criminal conduct means any "property that is derived from or obtained through criminal conduct, whether directly or indirectly, or in whole or in part" **(Reg 6, 2010 Act)**

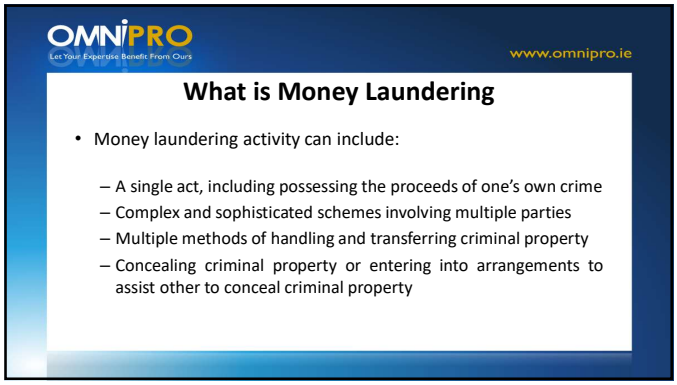
5

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

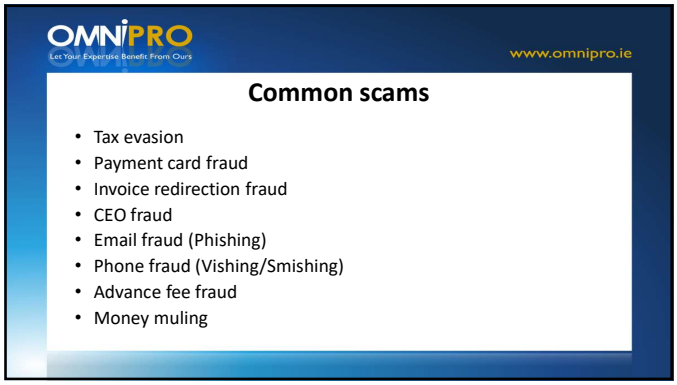
What is Money Laundering

- The proceeds of criminal conduct may take any form, including money, securities, tangible property and intangible property
- For a matter to be money laundering there must not only be criminal conduct, but also proceeds of criminal conduct
- Extends to facilitating the use or possession of proceeds
- Punishment on conviction unlimited fine and up to 14 years in prison

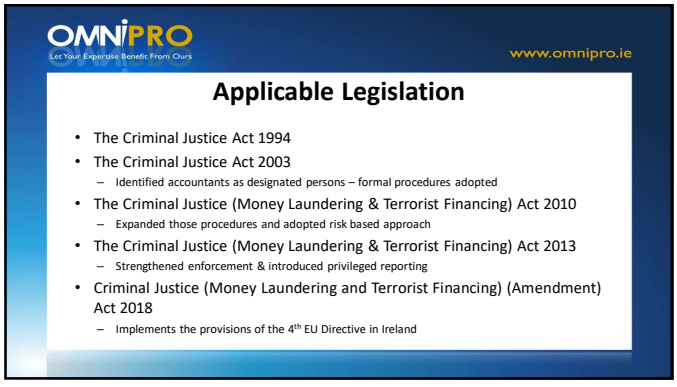
6


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
What is Money Laundering
• Money laundering activity can include:
– A single act, including possessing the proceeds of one's own crime
– Complex and sophisticated schemes involving multiple parties
– Multiple methods of handling and transferring criminal property
– Concealing criminal property or entering into arrangements to assist other to conceal criminal property

7


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Common scams
• Tax evasion
• Payment card fraud
• Invoice redirection fraud
• CEO fraud
• Email fraud (Phishing)
• Phone fraud (Vishing/Smishing)
• Advance fee fraud
• Money muling

8


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Applicable Legislation
• The Criminal Justice Act 1994
• The Criminal Justice Act 2003
– Identified accountants as designated persons – formal procedures adopted
• The Criminal Justice (Money Laundering & Terrorist Financing) Act 2010
– Expanded those procedures and adopted risk based approach
• The Criminal Justice (Money Laundering & Terrorist Financing) Act 2013
– Strengthened enforcement & introduced privileged reporting
• Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018
– Implements the provisions of the 4th EU Directive in Ireland

9

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

Applicable Legislation

- European Union (MLTF) Regulations 2019
  - Brought in whistleblowing legislation
- SI 110 of 2019 (RBO)
  - Brought in a reporting requirement for designated persons

10

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

People and businesses lose a record €9m to scammers
Elaborate email fraudsters conned €300k from buyer in final payment on house deal

€1.2m cash seized at checkpoint

Students tricked into laundering money

Seven held in swoop on €250m money-laundering operation

Three men arrested as guns, drugs and cash are seized in Garda operations in three counties

Man denies charges in €1.75m deception case

Irishman investigated over alleged multimillion-euro facemask scam

Law Society reports 41 solicitors to Garda
Figures show five solicitors were reported to gardaí last year for money laundering

Boylesports fined £2.8m over risk assessment

Gardaí hold two people as €14m fraud probe progresses

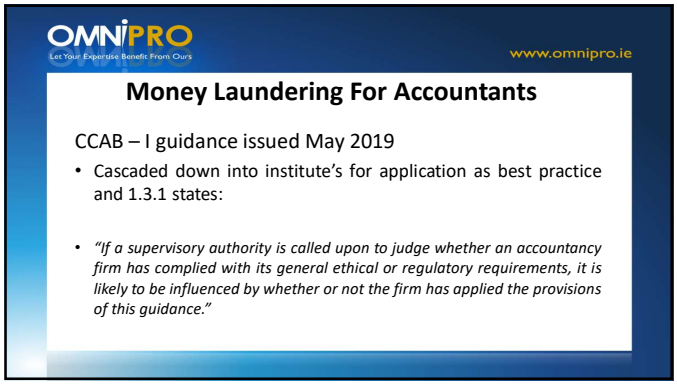
11

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

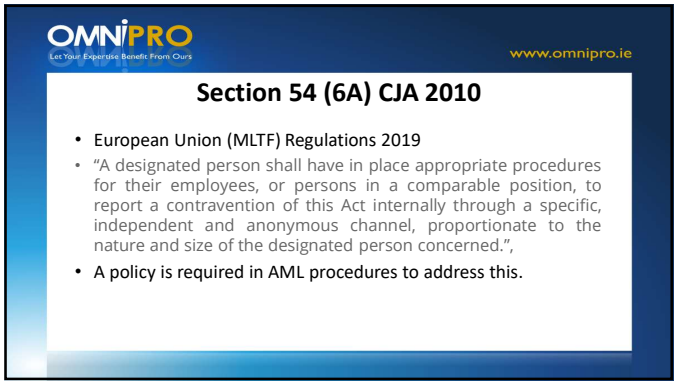
Guidance material

- CCAB-I Technical release 01/2019- Anti-Money Laundering Guidance for Members of the Bodies affiliated to the Consultative Committee of Accountancy Bodies in Ireland (CCAB-I) .
- Firm's own tailored policies and procedures.
- AML Guidance Manual on the Accountant's Resource Centre (ARC).

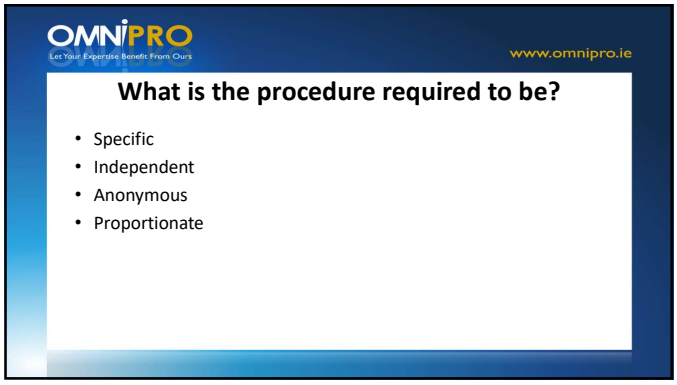
12


OMNiPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Money Laundering For Accountants
CCAB – I guidance issued May 2019
• Cascaded down into institute's for application as best practice and 1.3.1 states:
• "If a supervisory authority is called upon to judge whether an accountancy firm has complied with its general ethical or regulatory requirements, it is likely to be influenced by whether or not the firm has applied the provisions of this guidance."

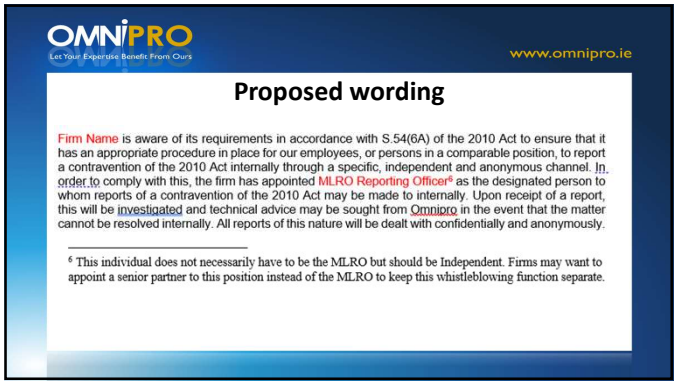
13


OMNiPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Section 54 (6A) CJA 2010
• European Union (MLTF) Regulations 2019
• "A designated person shall have in place appropriate procedures for their employees, or persons in a comparable position, to report a contravention of this Act internally through a specific, independent and anonymous channel, proportionate to the nature and size of the designated person concerned.",
• A policy is required in AML procedures to address this.

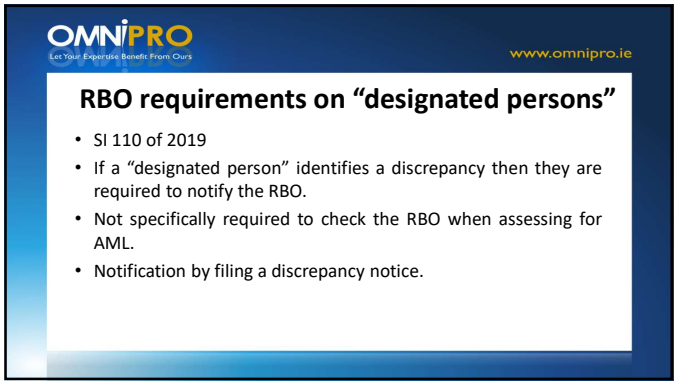
14


OMNiPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
What is the procedure required to be?
• Specific
• Independent
• Anonymous
• Proportionate

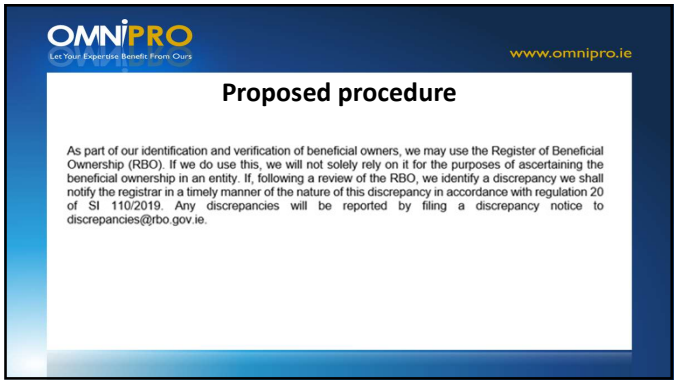
15


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Proposed wording
Firm Name is aware of its requirements in accordance with S.54(6A) of the 2010 Act to ensure that it has an appropriate procedure in place for our employees, or persons in a comparable position, to report a contravention of the 2010 Act internally through a specific, independent and anonymous channel. In order to comply with this, the firm has appointed MLRO Reporting Officer[6] as the designated person to whom reports of a contravention of the 2010 Act may be made to internally. Upon receipt of a report, this will be investigated and technical advice may be sought from Omnipro in the event that the matter cannot be resolved internally. All reports of this nature will be dealt with confidentially and anonymously.
[6] This individual does not necessarily have to be the MLRO but should be Independent. Firms may want to appoint a senior partner to this position instead of the MLRO to keep this whistleblowing function separate.

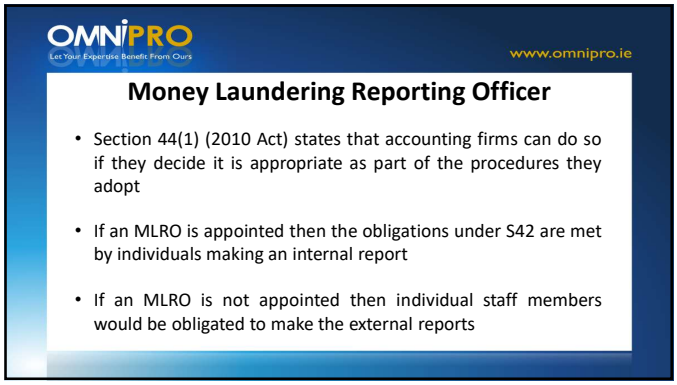
16


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
RBO requirements on "designated persons"
• SI 110 of 2019
• If a "designated person" identifies a discrepancy then they are required to notify the RBO.
• Not specifically required to check the RBO when assessing for AML.
• Notification by filing a discrepancy notice.

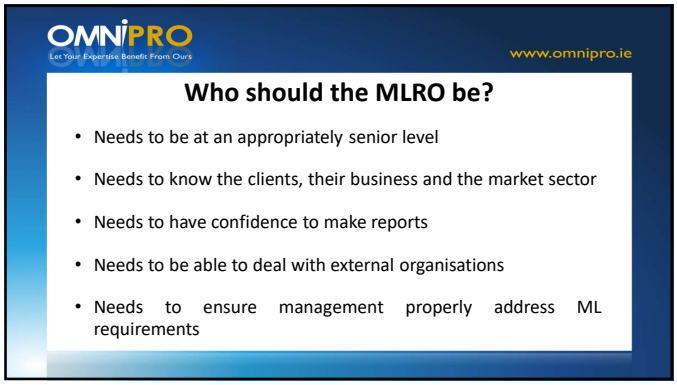
17


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Proposed procedure
As part of our identification and verification of beneficial owners, we may use the Register of Beneficial Ownership (RBO). If we do use this, we will not solely rely on it for the purposes of ascertaining the beneficial ownership in an entity. If, following a review of the RBO, we identify a discrepancy we shall notify the registrar in a timely manner of the nature of this discrepancy in accordance with regulation 20 of SI 110/2019. Any discrepancies will be reported by filing a discrepancy notice to discrepancies@rbo.gov.ie.

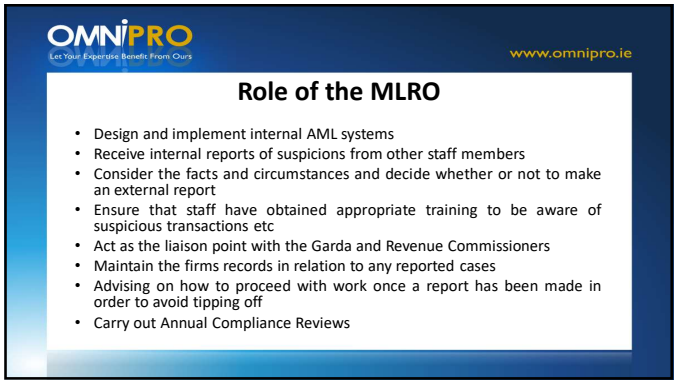
18


OMNiPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Money Laundering Reporting Officer
• Section 44(1) (2010 Act) states that accounting firms can do so if they decide it is appropriate as part of the procedures they adopt
• If an MLRO is appointed then the obligations under S42 are met by individuals making an internal report
• If an MLRO is not appointed then individual staff members would be obligated to make the external reports

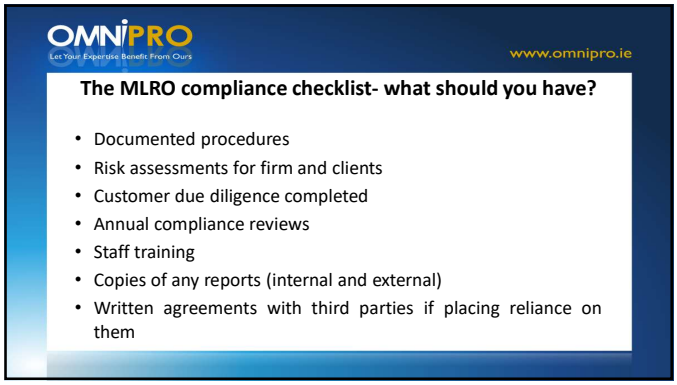
19


OMNiPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Who should the MLRO be?
• Needs to be at an appropriately senior level
• Needs to know the clients, their business and the market sector
• Needs to have confidence to make reports
• Needs to be able to deal with external organisations
• Needs to ensure management properly address ML requirements

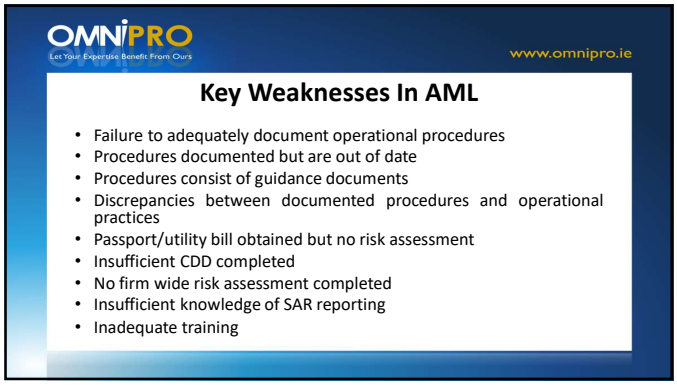
20


OMNiPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Role of the MLRO
• Design and implement internal AML systems
• Receive internal reports of suspicions from other staff members
• Consider the facts and circumstances and decide whether or not to make an external report
• Ensure that staff have obtained appropriate training to be aware of suspicious transactions etc
• Act as the liaison point with the Garda and Revenue Commissioners
• Maintain the firms records in relation to any reported cases
• Advising on how to proceed with work once a report has been made in order to avoid tipping off
• Carry out Annual Compliance Reviews

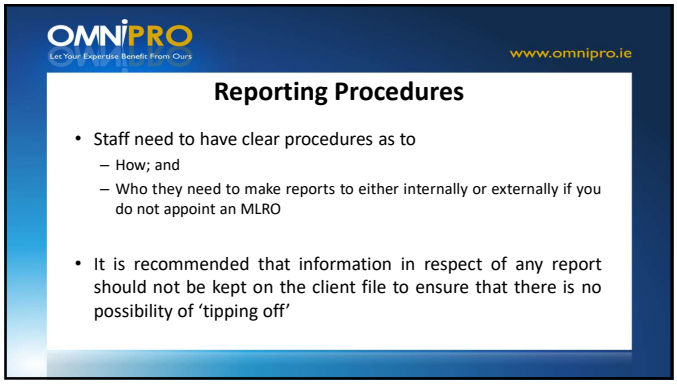
21


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
The MLRO compliance checklist- what should you have?
• Documented procedures
• Risk assessments for firm and clients
• Customer due diligence completed
• Annual compliance reviews
• Staff training
• Copies of any reports (internal and external)
• Written agreements with third parties if placing reliance on them

22


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Key Weaknesses In AML
• Failure to adequately document operational procedures
• Procedures documented but are out of date
• Procedures consist of guidance documents
• Discrepancies between documented procedures and operational practices
• Passport/utility bill obtained but no risk assessment
• Insufficient CDD completed
• No firm wide risk assessment completed
• Insufficient knowledge of SAR reporting
• Inadequate training

23


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Reporting Procedures
• Staff need to have clear procedures as to
– How; and
– Who they need to make reports to either internally or externally if you do not appoint an MLRO
• It is recommended that information in respect of any report should not be kept on the client file to ensure that there is no possibility of 'tipping off'

24

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

Reporting suspicions

- Accounting firms need to submit external reports to the Garda and the Revenue Commissioners where
  - You have knowledge
  - Suspicions
  - Or reasonable grounds to suspect that another person has been, or is engaged in money laundering or terrorist financing
- This knowledge or suspicion must arise 'in the course of carrying on business as an accounting firm'
- Can only arise where you have scrutinised the information
- Where doubt exists seek legal advice

25

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

What are "knowledge" and "suspicion"?

- Knowledge is actually knowing something.
- Suspicion is subjective and some guidance can be obtained from case law.
- See section 6.1.12 of the CCAB-I Technical release 01/2019 for guidance.

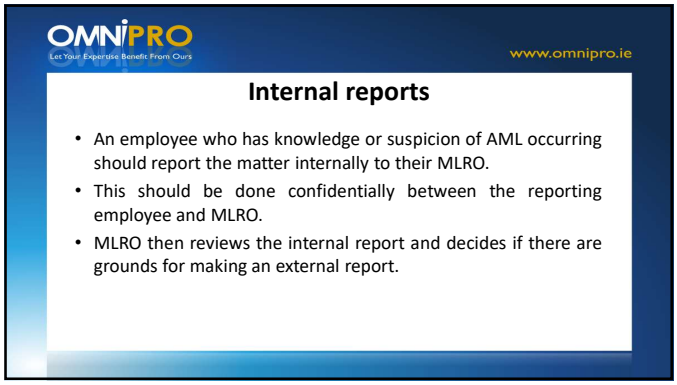
26

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

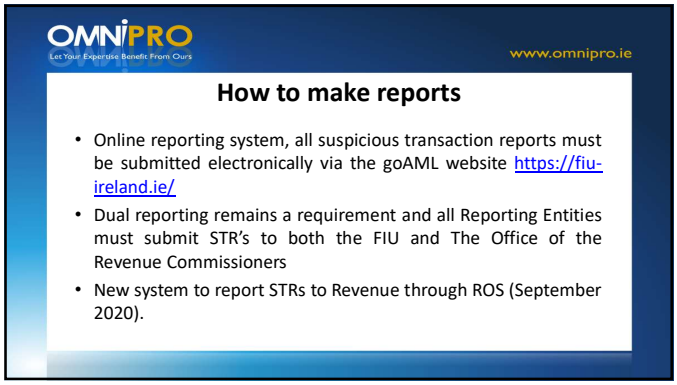
What needs to be reported

- The information on which the knowledge or suspicion has arisen
- The identity of the suspect, their address
- The whereabouts of the laundered property
- Details of banks accounts
- Details of transactions in question – amount, date
- Any other relevant information eg names of associates etc

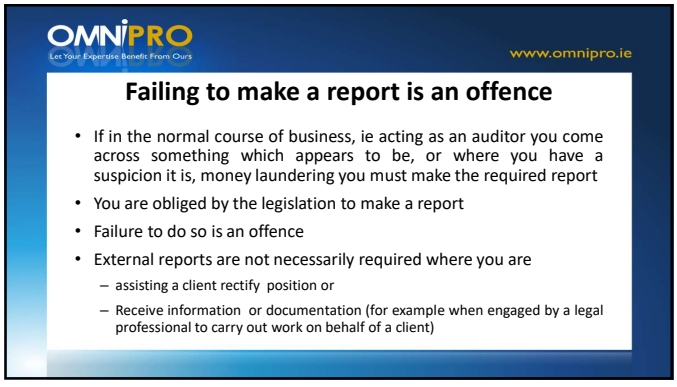
27


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Internal reports
• An employee who has knowledge or suspicion of AML occurring should report the matter internally to their MLRO.
• This should be done confidentially between the reporting employee and MLRO.
• MLRO then reviews the internal report and decides if there are grounds for making an external report.

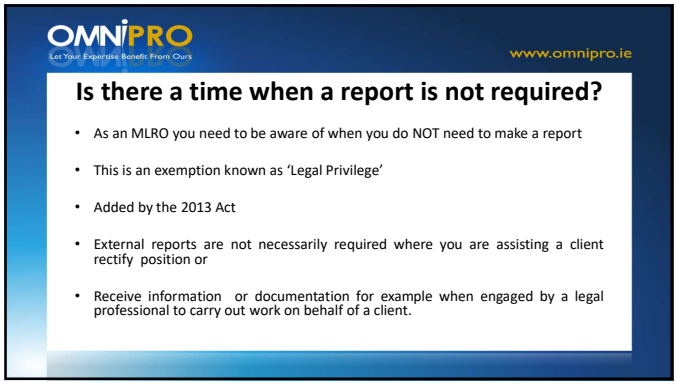
28


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
How to make reports
• Online reporting system, all suspicious transaction reports must be submitted electronically via the goAML website https://fiu-ireland.ie/
• Dual reporting remains a requirement and all Reporting Entities must submit STR's to both the FIU and The Office of the Revenue Commissioners
• New system to report STRs to Revenue through ROS (September 2020).

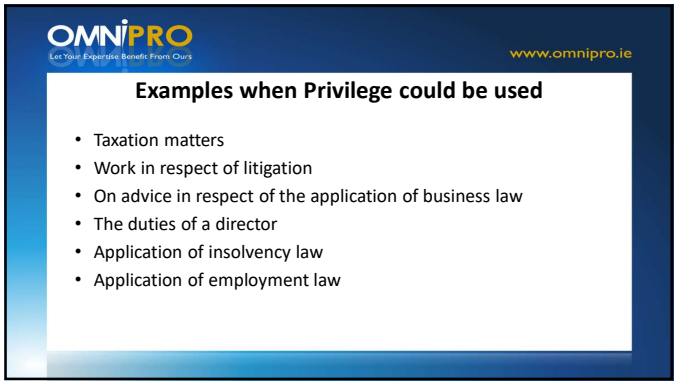
29


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Failing to make a report is an offence
• If in the normal course of business, ie acting as an auditor you come across something which appears to be, or where you have a suspicion it is, money laundering you must make the required report
• You are obliged by the legislation to make a report
• Failure to do so is an offence
• External reports are not necessarily required where you are
– assisting a client rectify position or
– Receive information or documentation (for example when engaged by a legal professional to carry out work on behalf of a client)

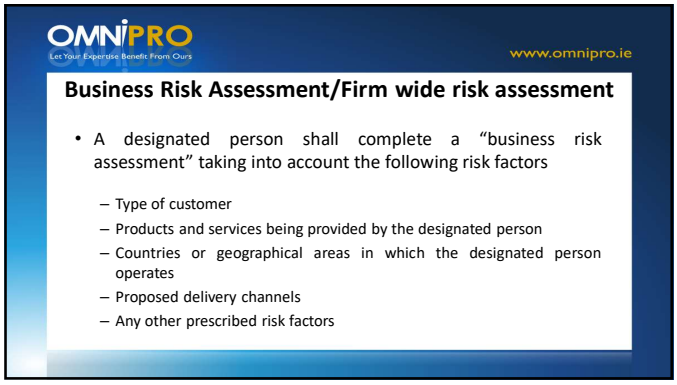
30


OMNiPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Is there a time when a report is not required?
• As an MLRO you need to be aware of when you do NOT need to make a report
• This is an exemption known as 'Legal Privilege'
• Added by the 2013 Act
• External reports are not necessarily required where you are assisting a client rectify position or
• Receive information or documentation for example when engaged by a legal professional to carry out work on behalf of a client.

31


OMNiPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Examples when Privilege could be used
• Taxation matters
• Work in respect of litigation
• On advice in respect of the application of business law
• The duties of a director
• Application of insolvency law
• Application of employment law

32


OMNiPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Business Risk Assessment/Firm wide risk assessment
• A designated person shall complete a "business risk assessment" taking into account the following risk factors
– Type of customer
– Products and services being provided by the designated person
– Countries or geographical areas in which the designated person operates
– Proposed delivery channels
– Any other prescribed risk factors

33

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

Risk Assessment

- Customer Risk – overall money laundering risk posed by a client based on key risk categories
- Service Risk – perceived risk that certain products or services present an increased level of vulnerability in being used for money laundering purposes
- Geographic risk – increased level of risk that a country poses in respect of money laundering

34

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

Risk Assessment

- Sector Risk – risks associated with certain sectors that more likely to be exposed to increased levels of money laundering
- Delivery Channel Risk – risk can be increased where services are provided to clients who have not been met face to face
- Firms must be able to demonstrate how they assess and seek to mitigate money laundering risks

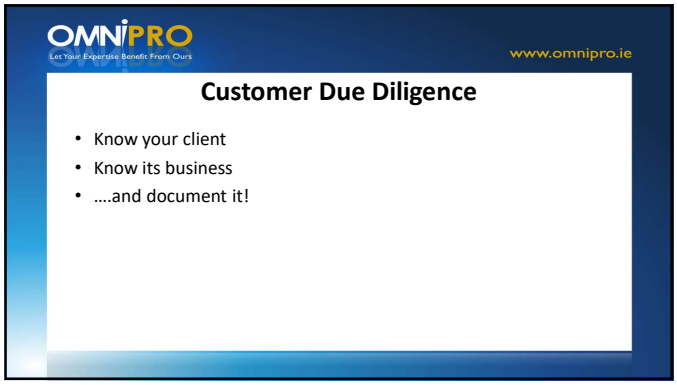
35

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

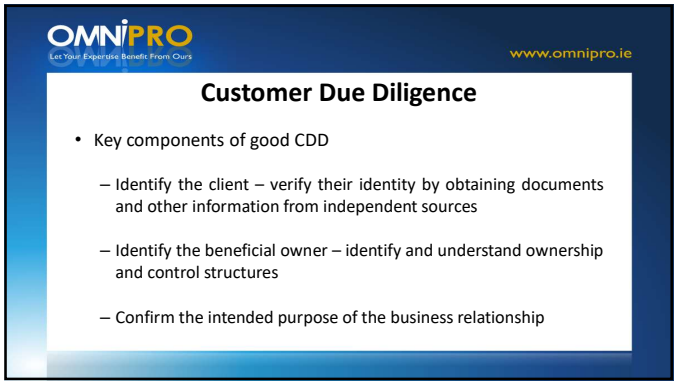
Customer Due Diligence

Information gathering → Risk Assessment → Evidence gathering

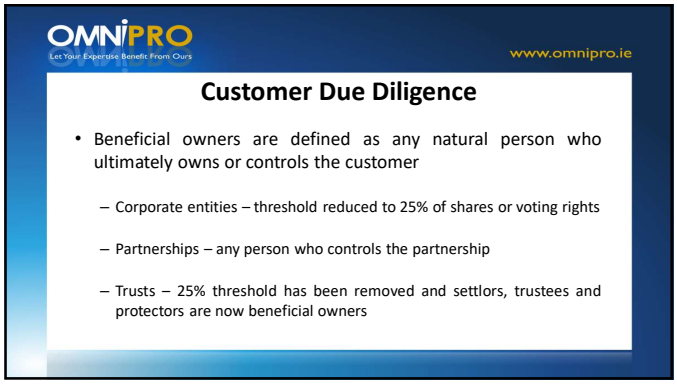
36


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Customer Due Diligence
• Know your client
• Know its business
• ….and document it!

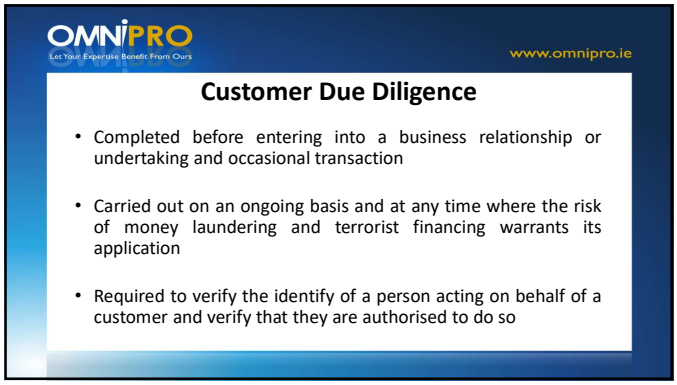
37


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Customer Due Diligence
• Key components of good CDD
– Identify the client – verify their identity by obtaining documents and other information from independent sources
– Identify the beneficial owner – identify and understand ownership and control structures
– Confirm the intended purpose of the business relationship

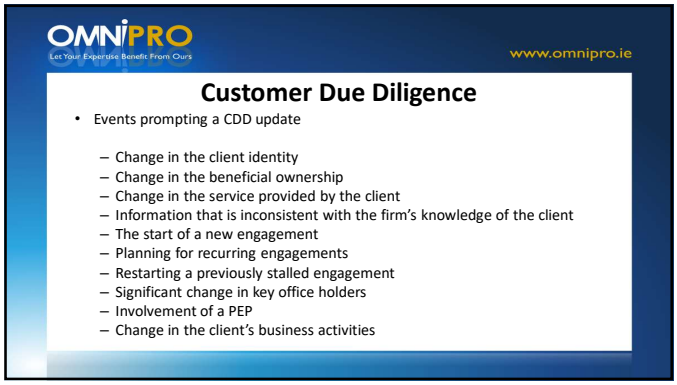
38


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Customer Due Diligence
• Beneficial owners are defined as any natural person who ultimately owns or controls the customer
– Corporate entities – threshold reduced to 25% of shares or voting rights
– Partnerships – any person who controls the partnership
– Trusts – 25% threshold has been removed and settlors, trustees and protectors are now beneficial owners

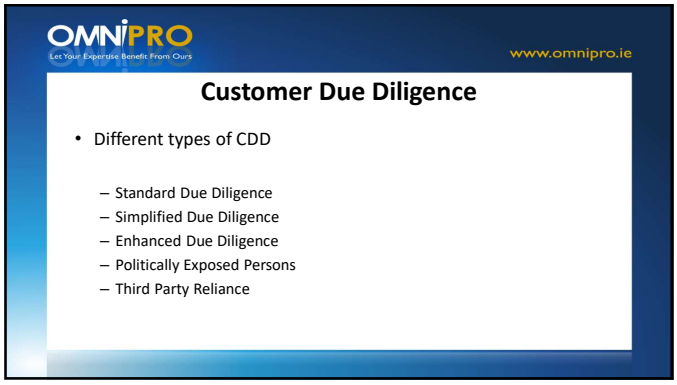
39


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Customer Due Diligence
• Completed before entering into a business relationship or undertaking and occasional transaction
• Carried out on an ongoing basis and at any time where the risk of money laundering and terrorist financing warrants its application
• Required to verify the identify of a person acting on behalf of a customer and verify that they are authorised to do so

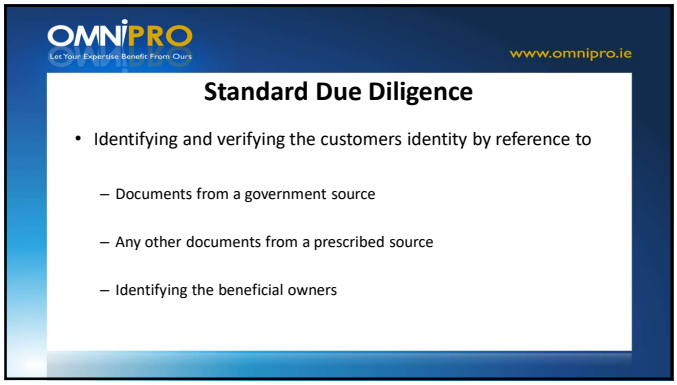
40


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Customer Due Diligence
• Events prompting a CDD update
– Change in the client identity
– Change in the beneficial ownership
– Change in the service provided by the client
– Information that is inconsistent with the firm's knowledge of the client
– The start of a new engagement
– Planning for recurring engagements
– Restarting a previously stalled engagement
– Significant change in key office holders
– Involvement of a PEP
– Change in the client's business activities

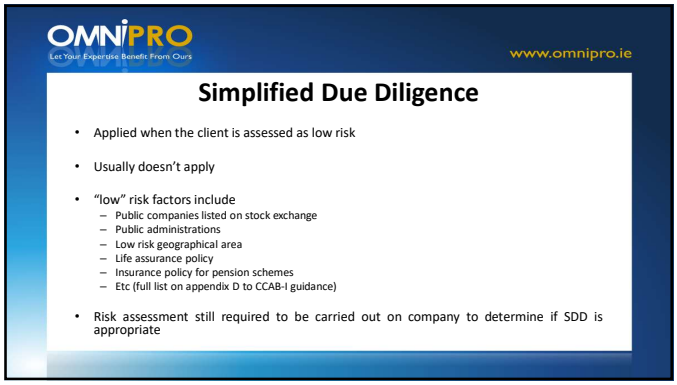
41


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Customer Due Diligence
• Different types of CDD
– Standard Due Diligence
– Simplified Due Diligence
– Enhanced Due Diligence
– Politically Exposed Persons
– Third Party Reliance

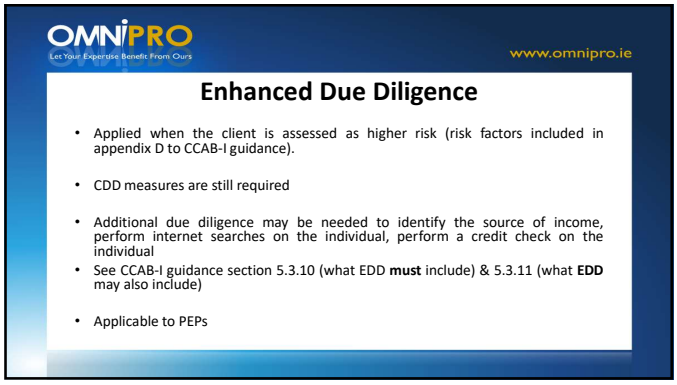
42


OMNiPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Standard Due Diligence
• Identifying and verifying the customers identity by reference to
– Documents from a government source
– Any other documents from a prescribed source
– Identifying the beneficial owners

43


OMNiPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Simplified Due Diligence
• Applied when the client is assessed as low risk
• Usually doesn't apply
• "low" risk factors include
– Public companies listed on stock exchange
– Public administrations
– Low risk geographical area
– Life assurance policy
– Insurance policy for pension schemes
– Etc (full list on appendix D to CCAB-I guidance)
• Risk assessment still required to be carried out on company to determine if SDD is appropriate

44


OMNiPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Enhanced Due Diligence
• Applied when the client is assessed as higher risk (risk factors included in appendix D to CCAB-I guidance).
• CDD measures are still required
• Additional due diligence may be needed to identify the source of income, perform internet searches on the individual, perform a credit check on the individual
• See CCAB-I guidance section 5.3.10 (what EDD **must** include) & 5.3.11 (what **EDD** may also include)
• Applicable to PEPs

45

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

Politically Exposed Persons

- Defined under legislation as:
  - A head of State, head of Government, Government minister
  - A member of Parliament
  - High level member of the judiciary
  - High level member of the armed forces
  - A senior member of a state owned enterprise

46

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

Politically Exposed Persons

- Definition expanded to include domestic PEPs, family members (spouse, children and their spouses) and known close associates
- Section 37 (10) CJA- defined.
- Must apply Enhanced procedures when a PEP is identified
- PEPs are still considered PEPs for at least 12 months after they cease to hold a public appointment

47

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

Third Party Reliance

- Firms are permitted to rely on certain other parties to complete all or part of their CDD
- Must have written agreement in place
- Permitted if the third party is also a designated person

48

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

Copies or Originals

- Where the person has sighted the original document they should note on the copy that they have sighted the original and the date of review
- Where a copy of a document has been provided (internet search) the firm should annotate the document to confirm this

49

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

COVID-19

- COVID-19 presents several new challenges from an AML perspective
- Spike in "Covid-19 SARs"- 27 in a 3 day period in UK
- Exploitation of COVID-19 to account for money movements
- Exploiting changes in behaviour patterns during COVID-19.
  - Large cash deposits to companies citing COVID-19 as reason for payment
  - Lodgement to company claiming to be refund of flights as a result of COVID-19
  - Business owners making deposits for staff wages
  - Businesses that should be closed have continued to trade

50

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

COVID-19

- NCA- COVID-19 press releases
  - https://www.nationalcrimeagency.gov.uk/who-we-are/publications/453-covid-19-suspicious-activity-reporting/file
  - https://www.nationalcrimeagency.gov.uk/who-we-are/publications/444-ukfiu-covid-19-communications-product-april-2020/file

51

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

COVID-19

- Travel restrictions & an inability to meet the client face to face may impact a firm's ability to conduct an effective client risk assessment.
- Increased levels of caution resulting in the need to gather more evidence in the third stage of CDD to verify the client's identity.
- Firms should always consider how they will demonstrate the provenance of document copies.
- Certified copies can be treated as a reliable source if you are satisfied with the standing of the certifier

52

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

COVID-19

- Can a firm defer the normal client due diligence checks if the staff member responsible for conducting them is self-isolating?
- CDD should normally be completed before entering into relationship
- AML legislation does recognise that CDD will occasionally need to be completed while the business relationship is established, rather than before. However, delays like this are only allowed when there is little risk of money laundering.

53

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

5th Money Laundering Directive

- Approved by European Council 14 May 2018
- Builds further on the 4th Directive and intends to increase transparency in financial transactions
- Estimated deadline for transposition in January 2020 (we are already late in implementing)
- 6th Directive also due for implementation by December

54

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

5th Money Laundering Directive

- Key Features
  - More bodies/industries defined as designated persons
  - Centralised beneficial ownership register
  - Enhanced due diligence for nationals from risky countries
  - Limit the use of electronic money currencies
  - Anonymous safe deposit boxed
  - Enhance the powers of the EU FIUs
  - Provide protection for whistleblowers

55

OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

Q&A

??

56

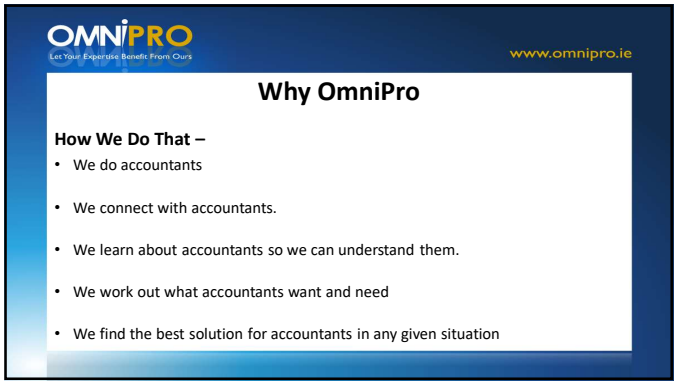
OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie

Why OmniPro

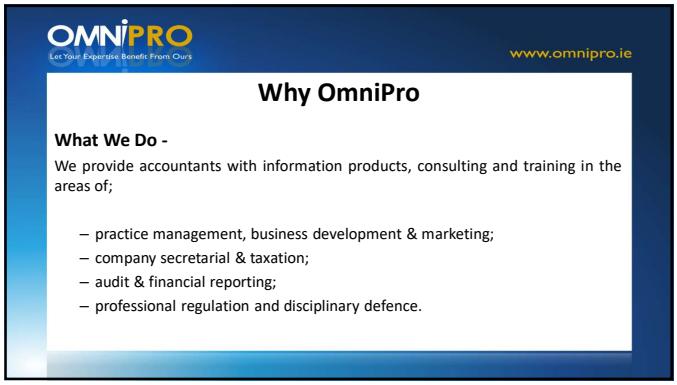
Our Why -

To facilitate accountants achieve extraordinary results in their business so they can help their clients achieve extraordinary results in theirs.

57


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Why OmniPro
How We Do That –
• We do accountants
• We connect with accountants.
• We learn about accountants so we can understand them.
• We work out what accountants want and need
• We find the best solution for accountants in any given situation

58


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
Why OmniPro
What We Do -
We provide accountants with information products, consulting and training in the areas of;
– practice management, business development & marketing;
– company secretarial & taxation;
– audit & financial reporting;
– professional regulation and disciplinary defence.

59


OMNIPRO
Let Your Expertise Benefit From Ours
www.omnipro.ie
OmniPro
Supporting Irish Accountants
Main Street,
Ferns,
Enniscorthy,
Co. Wexford.
053 9100000

60

Number 6 *of* 2010

CRIMINAL JUSTICE (MONEY LAUNDERING AND TERRORIST FINANCING) ACT 2010

REVISED

Updated to 26 November 2018

This Revised Act is an administrative consolidation of the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010*. It is prepared by the Law Reform Commission in accordance with its function under the *Law Reform Commission Act 1975* (3/1975) to keep the law under review and to undertake revision and consolidation of statute law.

All Acts up to and including *Children's Health Act 2018* (27/2018), enacted 20 November 2018, and all statutory instruments up to and including *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Section 25) (Prescribed Class of Designated Person) Regulations 2018* (S.I. No. 487 of 2018), made 22 November 2018, were considered in the preparation of this Revised Act.

Number 6 *of* 2010

CRIMINAL JUSTICE (MONEY LAUNDERING AND TERRORIST FINANCING) ACT 2010

REVISED

Updated to 26 November 2018

Introduction

This Revised Act presents the text of the Act as it has been amended since enactment, and preserves the format in which it was passed.

Related legislation

Criminal Justice (Money Laundering and Terrorist Financing) Acts 2010 to 2018: this Act is one of a group of Acts included in this collective citation (*Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 1(3)). The Acts in this group are:

- *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010* (6/2010)
- *Criminal Justice Act 2013* (19/2013), Part 2
- *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018)

Annotations

This Revised Act is annotated and includes textual and non-textual amendments, statutory instruments made pursuant to the Act and previous affecting provisions.

An explanation of how to read annotations is available at www.lawreform.ie/annotations.

Material not updated in this revision

Where other legislation is amended by this Act, those amendments may have been superseded by other amendments in other legislation, or the amended legislation may have been repealed or revoked. This information is not represented in this revision but will be reflected in a revision of the amended legislation if one is available.

Where legislation or a fragment of legislation is referred to in annotations, changes to this legislation or fragment may not be reflected in this revision but will be reflected in a revision of the legislation referred to if one is available.

A list of legislative changes to any Act, and to statutory instruments from 1980, may be found linked from the page of the Act or statutory instrument at www.irishstatutebook.ie.

Acts which affect or previously affected this revision

- *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018)
- *Criminal Justice (Corruption Offences) Act 2018* (9/2018)
- *Data Protection Act 2018* (7/2018)
- *Legal Services Regulation Act 2015* (65/2015)
- *Merchant Shipping (Registration of Ships) Act 2014* (43/2014)
- *Criminal Justice Act 2013* (19/2013)
- *Road Safety Authority (Commercial Vehicle Roadworthiness)Act 2012* (16/2012)
- *Road Transport Act 2011* (31/2011)
- *Criminal Justice Act 2011* (22/2011)
- *Central Bank Reform Act 2010* (23/2010)

All Acts up to and including *Children's Health Act 2018* (22/2018), enacted 20 November 2018, were considered in the preparation of this revision.

Statutory instruments which affect or previously affected this revision

- *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Section 25) (Prescribed Class of Designated Person) Regulations 2018* (S.I. No. 487 of 2018)
- *Trust or Company Service Provider Authorisation (Appeal Tribunal) (Establishment) (No. 2) Order 2018* (S.I. No. 475 of 2018)
- *Trust or Company Service Provider Authorisation (Appeal Tribunal) (Establishment) Order 2018* (S.I. No. 474 of 2018)
- *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Competent Authority and State Competent Authority) Regulations 2016* (S.I. No. 453 of 2016)
- *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Competent Authority) Regulations 2014* (S.I. No. 79 of 2014)
- *Trust or Company Service Provider Authorisation (Appeal Tribunal) (Establishment) Order 2013* (S.I. No. 167 of 2013)
- *Public Expenditure and Reform (Transfer of Departmental Administration and Ministerial Functions) Order 2011* (S.I. No. 647 of 2011)
- *Finance (Transfer of Departmental Administration and Ministerial Functions) Order 2011* (S.I. No. 418 of 2011)
- *Trust or Company Service Provider (Authorisation) (Fees) Regulations 2010* (S.I. No. 348 of 2010)
- *European Communities (Trust or Company Service Providers) (Temporary Authorisation) Regulations 2010* (S.I. No. 347of 2010)
- *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Section 31) Order 2010* (S. I. No. 343 of 2010)
- *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Commencement) Order 2010* (S. I. No. 342 of 2010)

All statutory instruments up to and including *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Section 25) (Prescribed Class of Designated Person) Regulations 2018* (S.I. No. 487 of 2018), made 22 November 2018, were considered in the preparation of this revision.

Number 6 *of* 2010

CRIMINAL JUSTICE (MONEY LAUNDERING AND TERRORIST FINANCING) ACT 2010

REVISED

Updated to 26 November 2018

ARRANGEMENT OF SECTIONS

DIRECTIONS, ORDERS AND AUTHORISATIONS RELATING TO INVESTIGATIONS

PART 4

PROVISIONS RELATING TO FINANCE SERVICES INDUSTRY, PROFESSIONAL SERVICE PROVIDERS AND OTHERS

Chapter 1

Interpretation (Part 4)

Chapter 1A

Risk assessment by designated persons

Chapter 2

Designation of places other than Member States — procedures for detecting money laundering or terrorist financing

Chapter 3

Customer Due Diligence

Chapter 10

Other

PART 5

MISCELLANEOUS

SCHEDULE 1

REVOCATIONS OF STATUTORY INSTRUMENTS

SCHEDULE 2

ANNEX I TO DIRECTIVE 2013/36/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 26 JUNE 201313 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

LIST OF ACTIVITIES SUBJECT TO MUTUAL RECOGNITION

SCHEDULE 3

NON-EXHAUSTIVE LIST OF FACTORS SUGGESTING POTENTIALLY LOWER RISK

SCHEDULE 4

NON-EXHAUSTIVE LIST OF FACTORS SUGGESTING POTENTIALLY HIGHER RISK

ACTS REFERRED TO

Bail Act 1997	1997, No. 16
Central Bank Act 1942	1942, No. 22
Central Bank Act 1997	1997, No. 8
Central Bank and Financial Services Authority of Ireland Act 2003	2003, No. 12
Central Bank and Financial Services Authority of Ireland Act 2004	2004, No. 21
Civil Service Regulation Act 1956	1956, No. 46
Companies Acts	
Companies (Auditing and Accounting) Act 2003	2003, No. 44
Courts (Supplemental Provisions) Act 1961	1961, No. 39
Credit Union Act 1997	1997, No. 15
Criminal Justice Act 1994	1994, No. 15
Criminal Justice Act 2006	2006, No. 26
Criminal Justice (Mutual Assistance) Act 2008	2008, No. 7
Criminal Justice (Miscellaneous Provisions) Act 2009	2009, No. 28
Criminal Justice (Surveillance) Act 2009	2009, No. 19
Criminal Justice (Terrorist Offences) Act 2005	2005, No. 2
Criminal Justice (Theft and Fraud Offences) Act 2001	2001, No. 50
Criminal Law Act 1997	1997, No. 14
Data Protection Acts 1988 and 2003	
European Arrest Warrant Act 2003	2003, No. 45
Extradition Act 1965	1965, No. 17
Finance Act 2004	2004, No. 8
Finance Act 2006	2006, No. 6
Freedom of Information Act 1997	1997, No. 13
Investment Intermediaries Act 1995	1995, No. 11
Investor Compensation Act 1998	1998, No. 37

Mercantile Marine Act 1955	1955, No. 29
Partnership Act 1890	53 & 54 Vic., c. 39
Solicitors (Amendment) Act 1994	1994, No. 27
Taxes Consolidation Act 1997	1997, No. 39
Taxi Regulation Act 2003	2003, No. 25

Number 6 *of* 2010

CRIMINAL JUSTICE (MONEY LAUNDERING AND TERRORIST FINANCING) ACT 2010

REVISED

Updated to 26 November 2018

AN ACT TO PROVIDE FOR OFFENCES OF, AND RELATED TO, MONEY LAUNDERING IN AND OUTSIDE THE STATE; TO GIVE EFFECT TO 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; TO PROVIDE FOR THE REGISTRATION OF PERSONS DIRECTING PRIVATE MEMBERS' CLUBS; TO PROVIDE FOR THE AMENDMENT OF THE CENTRAL BANK ACT 1942 AND THE COURTS (SUPPLEMENTAL PROVISIONS) ACT 1961; TO PROVIDE FOR THE CONSEQUENTIAL REPEAL OF CERTAIN PROVISIONS OF THE CRIMINAL JUSTICE ACT 1994; THE CONSEQUENTIAL AMENDMENT OF CERTAIN ENACTMENTS AND THE REVOCATION OF CERTAIN STATUTORY INSTRUMENTS; AND TO PROVIDE FOR RELATED MATTERS.

[5*th May*, 2010]

BE IT ENACTED BY THE OIREACHTAS AS FOLLOWS:

Annotations

Modifications (not altering text):

C1 Functions transferred and references to "Department of Public Expenditure and Reform" and "Minister for Public Expenditure and Reform" construed (14.12.2011) by the *Public Expenditure and Reform (Transfer of Departmental Administration and Ministerial Functions) Order 2011* (S.I. No. 647 of 2011), in effect as per art. 1(2).

2. (1) The administration and business in connection with the exercise, performance or execution of any functions transferred by this Order are transferred to the Department of Finance.

(2) References to the Department of Public Expenditure and Reform contained in any Act or instrument made under an act and relating to the administration and business transferred by paragraph (1) shall, from the commencement of this Order, be construed as references to the Department of Finance.

3. The functions conferred on the Minister for Public Expenditure and Reform by or under sections 3 and 107(1) of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (No. 6 of 2010) are transferred to the Minister for Finance.

4. References to the Minister for Public Expenditure and Reform contained in any Act or instrument made under an Act and relating to any functions transferred by this Order shall, from the commencement of this Order, be construed as references to the Minister for Finance.

C2 Functions transferred and references to "Department of Finance" and "Minister for Finance" construed (29.07.2011) by *Finance (Transfer of Departmental Administration and Ministerial*

Functions) Order 2011 (S.I. No. 418 of 2011), arts. 2, 3, 5 and sch. 1 part 2, in effect as per art. 1(2).

2. (1) The administration and business in connection with the performance of any functions transferred by this Order are transferred to the Department of Public Expenditure and Reform.

(2) References to the Department of Finance contained in any Act or instrument made thereunder and relating to the administration and business transferred by paragraph (1) shall, on and after the commencement of this Order, be construed as references to the Department of Public Expenditure and Reform.

3. The functions conferred on the Minister for Finance by or under the provisions of —

(a) the enactments specified in Schedule 1, and

(b) the statutory instruments specified in Schedule 2,

are transferred to the Minister for Public Expenditure and Reform.

...

5. References to the Minister for Finance contained in any Act or instrument under an Act and relating to any functions transferred by this Order shall, from the commencement of this Order, be construed as references to the Minister for Public Expenditure and Reform.

...

Schedule 1

Enactments

...

Part 2

1922 to 2011 Enactments

Number and Year (1)	Short Title (2)	Provision (3)
...	...	...
No. 6 of 2010	Criminal Justice (Money Laundering and Terrorist Financing) Act 2010	Sections 3, 101(4) and 107(1)
...	...	...

Editorial Notes:

E1 Offences under ss. 7, 8, 9, 10, 35, 37, 38, 42 and 49 prescribed as "relevant offences" for purposes of *Criminal Justice Act 2011* (22/2011) (9.08.2011) by *Criminal Justice Act 2011* (22/2011), s. 3(1) and sch. 1 par. 21, S.I. No. 411 of 2011.

PART 1

Preliminary

Short title and commencement.

1.— (1) This Act may be cited as the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010.

(2) This Act shall come into operation on such day or days as may be appointed by order or orders made by the Minister, either generally or with reference to a particular purpose or provision, and different days may be so appointed for different purposes and different provisions.

(3) An order under *subsection (2)* may, in respect of the repeal of the provisions of the Criminal Justice Act 1994 specified in *section 4*, and the revocation of the statutory instruments specified in *Schedule 1* effected by *section 4(2)*, appoint different days for the repeal of different provisions of the Criminal Justice Act 1994 and the revocation of different statutory instruments or different provisions of them.

Annotations

Editorial Notes:

E2 Power pursuant to section exercised (15.07.2010) by *Criminal Justice (Money Laundering and Terrorist Financing) (Commencement) Order 2010* (S.I. No. 342 of 2010).

2. The 15th day of July 2010 is appointed as the day on which the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (No. 6 of 2010) shall come into operation.

Interpretation.

2.— (1) In this Act—

F1**[**'Data Protection Regulation' means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016[38] on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);**]**

F2**[**'Fourth Money Laundering Directive' means Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015[2] 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;**]**

F3**[**...**]**

"Minister" means the Minister for Justice, Equality and Law Reform;

"money laundering" means an offence under *Part 2*;

F1**[**'personal data' means personal data within the meaning of—

(i) the Data Protection Act 1988,

(ii) the Data Protection Regulation, or

(iii) Part 5 of the Data Protection Act 2018;**]**

"prescribed" means prescribed by the Minister by regulations made under this Act;

"property" means all real or personal property, whether or not heritable or moveable, and includes money and choses in action and any other intangible or incorporeal property;

"terrorist financing" means an offence under section 13 of the Criminal Justice (Terrorist Offences) Act 2005;

"Third Money Laundering Directive" means 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 [2], as amended by the following:

[38] OJ No. L 119, 4.5.2016, p.1

[2] OJ No. L 141, 5.6.2015, p. 73

[2] OJ L 309, 25.11.2005, p.15

(*a*) 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 [3];

(*b*) 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 [4].

F4**[**(2) A word or expression used in this Act and also used in the Fourth Money Laundering Directive has, unless the contrary intention appears, the same meaning in this Act as in that Directive.**]**

Annotations

Amendments:

F1 Inserted (25.05.2018) by *Data Protection Act 2018* (7/2018), s. 213(a), S.I. No. 174 of 2018.

F2 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 3(a)(ii), S.I. No. 486 of 2018.

F3 Deleted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 3(a)(i), S.I. No. 486 of 2018.

F4 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 3(b), S.I. No. 486 of 2018.

Regulations.

3.— (1) The Minister may, after consulting with the Minister for Finance, by regulations provide for any matter referred to in this Act as prescribed or to be prescribed.

(2) Regulations under this Act may contain such incidental, supplementary and consequential provisions as appear to the Minister to be necessary or expedient for the purposes of the regulations.

(3) Every regulation made under this Act shall be laid before each House of the Oireachtas as soon as may be after it is made and, if a resolution annulling the regulation is passed by either such House within the next 21 days on which that House has sat after the regulation is laid before it, the regulation shall be annulled accordingly, but without prejudice to the validity of anything previously done under the regulation.

Annotations

Editorial Notes:

E3 Power pursuant to subs. (1) exercised (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Section 25) (Prescribed Class of Designated Person) Regulations 2018* (S.I. No. 487 of 2018), in effect as per reg. 1(2).

E4 Power pursuant to subs. (1) exercised (1.09.2016) by *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Competent Authority and State Competent Authority) Regulations 2016* (S.I. No. 453 of 2016), in effect as per reg. 2.

E5 Power pursuant to subs. (1) exercised (3.03.2014) by *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Competent Authority) Regulations 2014* (S.I. No. 79 of 2014), in effect as per reg. 2.

[3] OJ L 319, 5.12.2007, p.1
[4] OJ L 267, 10.10.2009, p.7

E6 Power pursuant to subs. (1) exercised (15.07.2010) by *Trust or Company Service Provider (Authorisation) (Fees) Regulations 2010* (S.I. No. 348 of 2010), in effect as per reg. 1(2).

Repeals and revocations.

4.— (1) Sections 31, 32, 32A, 57(1) to (6) and (7)(*a*), 57A and 58(2) of the Criminal Justice Act 1994 are repealed.

(2) The statutory instruments specified in *column (1)* of *Schedule 1* are revoked to the extent specified in *column (3)* of that Schedule.

Expenses.

5.— The expenses incurred by the Minister in the administration of this Act shall, to such extent as may be sanctioned by the Minister for Finance, be paid out of moneys provided by the Oireachtas and the expenses incurred by the Minister for Finance in the administration of this Act shall be paid out of moneys provided by the Oireachtas.

PART 2

Money Laundering Offences

Annotations

Editorial Notes:

E7 Obligation imposed on an applicant for, or the holder of, an authorisation (as a commercial vehicle roadworthiness test operator under *Road Safety Authority (Commercial Vehicle Roadworthiness) Act 2012* (16/2012), s. 9 or 10, or as a commercial vehicle roadworthiness tester under *Road Safety Authority (Commercial Vehicle Roadworthiness) Act 2012* (16/2012), s. 17), or in the case of an authorisation applied for or held by a company, each director and the secretary of that company, to notify the Minister for Transport, Tourism and Sport in writing if he or she is, or has been, convicted of an offence under Part (27.03.2013) by *Road Safety Authority (Commercial Vehicle Roadworthiness) Act 2012* (16/2012), s. 12, S.I. No. 105 of 2013.

E8 Power granted to Minister for Transport, Tourism and Sport, in determining whether an operator has satisfied or continues to satisfy the requirement of good repute, to consider whether the operator, a person who holds a specified position, a shadow operator, or, in the case of a road passenger transport operator, a driver with that operator, has been convicted of an offence under Part (2.12.2011) by *Road Transport Act 2011* (31/2011), s. 4, commenced on enactment.

E9 Obligation imposed on person who holds a specified position, a shadow operator, and, in the case of a road passenger transport operator, a driver with that operator, to inform the operator in writing in the event that he or she is or has been convicted of an offence under Part (2.12.2011) by *Road Transport Act 2011* (31/2011), s. 3, commenced on enactment.

E10 Obligation imposed on holder of, or applicant for, an operator's licence to notify the Minister for Transport, Tourism and Sport if a person who holds a specified position, a shadow operator, or, in the case of a road passenger transport operator, a driver with that operator, has been or is convicted an offence under Part (2.12.2011) by *Road Transport Act 2011* (31/2011), s. 2, commenced on enactment.

Interpretation (*Part 2*).

6.— In this Part—

F5**[**'criminal conduct' means—

(a) conduct that constitutes an offence,

(b) conduct occurring in a place outside the State that constitutes an offence under the law of the place and would constitute an offence if it were to occur in the State, or

(c) conduct occurring in a place outside the State that would constitute an offence under section 5(1) or 6(1) of the Criminal Justice (Corruption Offences) Act 2018 if it were to occur in the State and the person or official, as the case may be, concerned doing the act, or making the omission, concerned in relation to his or her office, employment, position or business is a foreign official within the meaning of that Act;**]**

"proceeds of criminal conduct" means any property that is derived from or obtained through criminal conduct, whether directly or indirectly, or in whole or in part, and whether that criminal conduct occurs before, on or after the commencement of this Part.

Annotations

Amendments:

F5 Substituted (30.07.2018) by *Criminal Justice (Corruption Offences) Act 2018* (9/2018), s. 26, S.I. No. 298 of 2018.

Money laundering occurring in State.

7.— (1) A person commits an offence if—

(*a*) the person engages in any of the following acts in relation to property that is the proceeds of criminal conduct:

(i) concealing or disguising the true nature, source, location, disposition, movement or ownership of the property, or any rights relating to the property;

(ii) converting, transferring, handling, acquiring, possessing or using the property;

(iii) removing the property from, or bringing the property into, the State,

and

(*b*) the person knows or believes (or is reckless as to whether or not) the property is the proceeds of criminal conduct.

(2) A person who attempts to commit an offence under *subsection (1)* commits an offence.

(3) A person who commits an offence under this section is liable—

(*a*) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 14 years (or both).

(4) A reference in this section to knowing or believing that property is the proceeds of criminal conduct includes a reference to knowing or believing that the property probably comprises the proceeds of criminal conduct.

(5) For the purposes of *subsections (1)* and *(2)*, a person is reckless as to whether or not property is the proceeds of criminal conduct if the person disregards, in relation to property, a risk of such anature and degree that, considering the circumstances in which the person carries out any act referred to in *subsection (1)* or *(2)*, the disregard of that risk involves culpability of a high degree.

(6) For the purposes of *subsections (1)* and *(2)*, a person handles property if the person—

(*a*) receives, or arranges to receive, the property, or

(*b*) retains, removes, disposes of or realises the property, or arranges to do any of those things, for the benefit of another person.

(7) A person does not commit an offence under this section in relation to the doing of any thing in relation to property that is the proceeds of criminal conduct so long as—

(*a*) the person does the thing in accordance with a direction, order or authorisation given under *Part 3,* or

(*b*) without prejudice to the generality of *paragraph (a)*, the person is a designated person, within the meaning of *Part 4,* who makes a report in relation to the property, and does the thing, in accordance with *section 42*.

Money laundering outside State in certain circumstances.

8.— (1) A person who, in a place outside the State, engages in conduct that would, if the conduct occurred in the State, constitute an offence under *section 7* commits an offence if any of the following circumstances apply:

(*a*) the conduct takes place on board an Irish ship, within the meaning of section 9 of the Mercantile Marine Act 1955,

(*b*) the conduct takes place on an aircraft registered in the State,

(*c*) the conduct constitutes an offence under the law of that place and the person is—

(i) an individual who is a citizen of Ireland or ordinarily resident in the State, or

(ii) a body corporate established under the law of the State or a company registered under the Companies Acts,

(*d*) a request for the person's surrender, for the purpose of trying him or her for an offence in respect of the conduct, has been made under Part II of the Extradition Act 1965 by any country and the request has been finally refused (whether or not as a result of a decision of a court), or

(*e*) a European arrest warrant has been received from an issuing state for the purpose of bringing proceedings against the person for an offence in respect of the conduct, and a final determination has been made that—

(i) the European arrest warrant should not be endorsed for execution in the State under the European Arrest Warrant Act 2003, or

(ii) the person should not be surrendered to the issuing state.

(2) A person who commits an offence under this section is liable—

(*a*) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 14 years (or both).

(3) A person who has his or her principal residence in the State for the 12 months immediately preceding the commission of an offence under this section is, in a case where *subsection (1)(c)* applies, taken to be ordinarily resident in the State on the date of the commission of the offence.

(4) In this section, "European arrest warrant" and "issuing state" have the same meanings as they have in the European Arrest Warrant Act 2003.

Annotations

Amendments:

F6 Substituted by *Merchant Shipping (Registration of Ships) Act 2014* (43/2014), s. 68 and sch. 4, not commenced as of date of revision.

Modifications (not altering text):

C3 Prospective affecting provision: subs. (1)(a) amended by *Merchant Shipping (Registration of Ships) Act 2014* (43/2014), s. 68 and sch. 4, not commenced as of date of revision.

Money laundering outside State in certain circumstances.

8.— (1) A person who, in a place outside the State, engages in conduct that would, if the conduct occurred in the State, constitute an offence under *section 7* commits an offence if any of the following circumstances apply:

(*a*) the conduct takes place on board an Irish ship, within the meaning of F6**[**section 33 of the Merchant Shipping (Registration of Ships) Act 2014**]**,

...

Attempts, outside State, to commit offence in State.

9.— (1) A person who attempts, in a place outside the State, to commit an offence under *section 7(1)* is guilty of an offence.

(2) A person who commits an offence under this section is liable—

(*a*) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 14 years (or both).

Aiding, abetting, counselling or procuring outside State commission of offence in State.

10.— (1) A person who, in a place outside the State, aids, abets, counsels or procures the commission of an offence under *section 7* is guilty of an offence.

(2) A person who commits an offence under this section is liable—

(*a*) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 14 years (or both).

(3) This section is without prejudice to section 7(1) of the Criminal Law Act 1997.

Presumptions and other matters.

11.— (1) In this section "specified conduct" means any of the following acts referred to in *section 7(1)* (including *section 7(1)* as applied by *section 8*or *9*):

(*a*) concealing or disguising the true nature, source, location, disposition, movement or ownership of property, or any rights relating to property;

(*b*) converting, transferring, handling, acquiring, possessing or using property;

(*c*) removing property from, or bringing property into, the State or a place outside the State.

(2) In proceedings for an offence under *section 7, 8* or *9*, where an accused has engaged, or attempted to engage, in specified conduct in relation to property that is the proceeds of criminal conduct, in circumstances in which it is reasonable to conclude that the accused—

(*a*) knew or believed the property was the proceeds of criminal conduct, or

(*b*) was reckless as to whether or not the property was the proceeds of criminal conduct,

the accused is presumed to have so known or believed, or been so reckless, unless the court or jury, as the case may be, is satisfied, having regard to the whole of the evidence, that there is a reasonable doubt that the accused so knew or believed or was so reckless.

(3) In proceedings for an offence under *section 7, 8* or *9*, where an accused has engaged in, or attempted to engage in, specified conduct in relation to property in circumstances in which it is reasonable to conclude that the property is the proceeds of criminal conduct, those circumstances are evidence that the property is the proceeds of criminal conduct.

(4) For the purposes of *subsection (3)*, circumstances in which it is reasonable to conclude that property is the proceeds of criminal conduct include any of the following:

(*a*) the value of the property concerned is, it is reasonable to conclude, out of proportion to the income and expenditure of the accused or another person in a case where the accused engaged in the specified conduct concerned on behalf of, or at the request of, the other person;

(*b*) the specified conduct concerned involves the actual or purported purchase or sale of goods or services for an amount that is, it is reasonable to conclude, out of proportion to the market value of the goods or services (whether the amount represents an overvaluation or an undervaluation);

(*c*) the specified conduct concerned involves one or more transactions using false names;

(*d*) the accused has stated that he or she engaged in the specified conduct concerned on behalf of, or at the request of, another person and has not provided information to the Garda Síochána enabling the other person to be identified and located;

(*e*) where an accused has concealed or disguised the true nature, source, location, disposition, movement or ownership of the property, or any rights relating to the property, the accused has no reasonable explanation for that concealment or disguise.

(5) Nothing in *subsection (4)* limits the circumstances in which it is reasonable to conclude, for the purposes of *subsection (3)*, that property is the proceeds of criminal conduct.

(6) Nothing in this section prevents *subsections (2)* and *(3)* being applied in the same proceedings.

(7) *Subsections (2)* to *(6)* extend to proceedings for an offence under—

(*a*) *section 10*, or

(*b*) section 7(1) of the Criminal Law Act 1997 of aiding, abetting, counselling or procuring the commission of an offence under *section 7*, *8* or *9*,

and for that purpose any reference to an accused in *subsections (2)* to *(6)* is to be construed as a reference to a person who committed, or is alleged to have committed, the offence concerned.

(8) In proceedings for an offence under this Part, or an offence under section 7(1) of the Criminal Law Act 1997 referred to in *subsection (7)(b)*, it is not necessary, in order to prove that property is the proceeds of criminal conduct, to establish that—

(*a*) a particular offence or a particular class of offence comprising criminal conduct was committed in relation to the property, or

(*b*) a particular person committed an offence comprising criminal conduct in relation to the property.

(9) In proceedings for an offence under this Part, or an offence under section 7(1) of the Criminal Law Act 1997 referred to in *subsection (7)(b)*, it is not a defence for the accused to show that the accused believed the property concerned to be the proceeds of a particular offence comprising criminal conduct when in fact the property was the proceeds of another offence.

Location of proceedings relating to offences committed outside State.

12.— Proceedings for an offence under *section 8, 9* or *10* may be taken in any place in the State and the offence may for all incidental purposes be treated as having been committed in that place.

Consent of DPP required for proceedings for offences committed outside State.

13.— If a person is charged with an offence under *section 8, 9* or *10*, no further proceedings in the matter (other than any remand in custody or on bail) may be taken except by, or with the consent of, the Director of Public Prosecutions.

Certificate may be evidence in proceedings under this Part.

14.— (1) In any proceedings for an offence under this Part in which it is alleged that property the subject of the offence is the proceeds of criminal conduct occurring in a place outside the State, a certificate—

(*a*) purporting to be signed by a lawyer practising in the place, and

(*b*) stating that such conduct is an offence in that place,

is evidence of the matters referred to in that certificate, unless the contrary is shown.

(2) A certificate referred to in *subsection (1)* is taken to have been signed by the person purporting to have signed it, unless the contrary is shown.

(3) In a case where a certificate referred to in *subsection (1)* is written in a language other than the Irish language or the English language, unless the contrary is shown—

(*a*) a document purporting to be a translation of that certificate into the Irish language or the English language, as the case may be, and that is certified as correct by a person appearing to be competent to so certify, is taken—

(i) to be a correct translation of the certificate, and

(ii) to have been certified by the person purporting to have certified it,

and

(*b*) the person is taken to be competent to so certify.

(4) In any proceedings for an offence under *section 8* committed in the circumstances referred to in *section 8(1)(c),* a certificate purporting to be signed by an officer of the Department of Foreign Affairs and stating that—

(*a*) a passport was issued by that Department to a person on a specified date, and

(*b*) to the best of the officer's knowledge and belief, the person has not ceased to be an Irish citizen,

is evidence that the person was an Irish citizen on the date on which the offence is alleged to have been committed, and is taken to have been signed by the person purporting to have signed it, unless the contrary is shown.

(5) In any proceedings for an offence under *section 8* committed in the circumstances referred to in *section 8 (1) (d)* or *(e)*, a certificate purporting to be signed by the Minister and stating any of the matters referred to in that paragraph is evidence of those matters, and is taken to have been signed by the Minister, unless the contrary is shown.

Double jeopardy.

15.— A person who has been acquitted or convicted of an offence in a place outside the State shall not be proceeded against for an offence under *section 8, 9* or *10* consisting of the conduct, or substantially the same conduct, that constituted the offence of which the person has been acquitted or convicted.

Revenue offence committed outside State.

16.— For the avoidance of doubt, a reference in this Part to an offence under the law of a place outside the State includes a reference to an offence in connection with taxes, duties, customs or exchange regulation.

PART 3

Directions, Orders and Authorisations Relating to Investigations

Direction or order not to carry out service or transaction.

17.— (1) A member of the Garda Síochána not below the rank of superintendent may, by notice in writing, direct a person not to carry out any specified service or transaction during the period specified in the direction, not exceeding 7 days, if the member is satisfied that, on the basis of information that the Garda Síochána has obtained or received (whether or not in a report made under *Chapter 4* of *Part 4*), such a direction is reasonably necessary to enable the Garda Síochána to carry out preliminary investigations into whether or not there are reasonable grounds to suspect that the service or transaction would, if it were to proceed, comprise or assist in money laundering or terrorist financing.

(2) A judge of the District Court may order a person not to carry out any specified service or transaction during the period specified in the order, not exceeding 28 days, if satisfied by information on oath of a member of the Garda Síochána, that—

(*a*) there are reasonable grounds to suspect that the service or transaction would, if it were to proceed, comprise or assist in money laundering or terrorist financing, and

(*b*) an investigation of a person for that money laundering or terrorist financing is taking place.

(3) An order may be made, under *subsection (2)*, in relation to a particular service or transaction, on more than one occasion.

F7**[**(4) An application for an order under subsection (2)—

(a) shall be made *ex parte* and shall be heard otherwise than in public,

and

(b) shall be made to a judge of the District Court assigned to the district in which the order is proposed to be served.**]**

(5) A person who fails to comply with a direction or order under this section commits an offence and is liable—

(*a*) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).

(6) Any act or omission by a person in compliance with a direction or order under this section shall not be treated, for any purpose, as a breach of any requirement or restriction imposed by any other enactment or rule of law.

Annotations

Amendments:

F7 Substituted (14.06.2013) by *Criminal Justice Act 2013* (19/2013), s. 3, S.I. No. 196 of 2013.

Notice of direction or order.

18.— (1) As soon as practicable after a direction is given or order is made under *section 17*, the member of the Garda Síochána who gave the direction or applied for the order shall ensure that any person who the member is aware is affected by the direction or order is given notice, in writing, of the direction or order unless—

(*a*) it is not reasonably practicable to ascertain the whereabouts of the person, or

(*b*) there are reasonable grounds for believing that disclosure to the person would prejudice the investigation in respect of which the direction or order is given.

(2) Notwithstanding *subsection (1)(b)*, a member of the Garda Síochána shall give notice, in writing, of a direction or order under this section to any person who is, or appears to be, affected by it as soon as practicable after the Garda Síochána becomes aware that the person is aware that the direction has been given or order has been made.

(3) Nothing in *subsection (1)* or *(2)* requires notice to be given to a person to whom a direction is given or order is addressed under this section.

(4) A notice given under this section shall include the reasons for the direction or order concerned and advise the person to whom the notice is given of the person's right to make an application under *section 19* or *20*.

(5) The reasons given in the notice need not include details the disclosure of which there are reasonable grounds for believing would prejudice the investigation in respect of which the direction is given or order is made.

Revocation of direction or order on application.

19.— (1) At any time while a direction or order is in force under *section 17*, a judge of the District Court may revoke the direction or order if the judge is satisfied, on the application of a person affected by the direction or order, as the case may be, that the matters referred to in *section 17(1)* or *(2)* do not, or no longer, apply.

(2) Such an application may be made only if notice has been given to the Garda Síochána in accordance with any applicable rules of court.

Order in relation to property subject of direction or order.

20.— (1) At any time while a direction or order is in force under *section 17*, in relation to property, a judge of the District Court may, on application by any person affected by the direction or order concerned, as the case may be, make any order that the judge considers appropriate in relation to any of the property concerned if satisfied that it is necessary to do so for the purpose of enabling the person—

(*a*) to discharge the reasonable living and other necessary expenses, including legal expenses in or in relation to legal proceedings, incurred or to be incurred in respect of the person or the person's dependants, or

(*b*) to carry on a business, trade, profession or other occupation to which any of the property relates.

(2) Such an application may be made only if notice has been given to the Garda Síochána in accordance with any applicable rules of court.

Cessation of direction or order on cessation of investigation.

21.— (1) A direction or order under *section 17* ceases to have effect on the cessation of an investigation into whether the service or transaction the subject of the direction or order would, if it were to proceed, comprise or assist in money laundering or terrorist financing.

(2) As soon as practicable after a direction or order under *section 17* ceases, as a result of *subsection (1)*, to have effect, a member of the Garda Síochána shall give notice in writing of the fact that the direction or order has ceased to have effect to—

(*a*) the person to whom the direction or order has been given, and

(*b*) any other person who the member is aware is affected by the direction or order.

Suspicious transaction report not to be disclosed.

22.— A report made under *Chapter 4* of *Part 4* shall not be disclosed, in the course of proceedings under *section 17* or *19*, to any person other than the judge of the District Court concerned.

Authorisation to proceed with act that would otherwise comprise money laundering.

23.— (1) A member of the Garda Síochána not below the rank of superintendent may, by notice in writing, authorise a person to do a thing referred to in *section 7(1)* if the member is satisfied that the thing is necessary for the purposes of an investigation into an offence.

(2) The doing of any thing in accordance with an authorisation under this section shall not be treated, for any purpose, as a breach of any requirement or restriction imposed by any other enactment or rule of law.

(3) *Subsection (2)* is without prejudice to *section 7 (7)*.

PART 4

Provisions Relating to Finance Services Industry, Professional Service Providers and Others

Chapter 1

Interpretation (Part 4)

Annotations

Editorial Notes:

E11 Part included in definition of "designated enactments" for purposes of *Central Bank Act 1942* (22/1942) by *Central Bank Act 1942* (22/1942), s. 2(1) and sch. 2 part 1 item 37, as substituted (1.10.2010) by *Central Bank Reform Act 2010* (23/2010), s. 14(1) and sch. part 1 items 6 and 82, S.I. No. 469 of 2010.

Definitions.

24.— (1) In this Part—

"barrister" means a practising barrister;

"beneficial owner" has the meaning assigned to it by *sections 26* to *30*;

"business relationship", in relation to a designated person and a customer of the person, means a business, professional or commercial relationship between the person and the customer that the person expects to be ongoing;

F8**[**'business risk assessment' has the meaning given to it by *section 30A*;**]**

F8**[**'Capital Requirements Regulation' means Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013[3] on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012;**]**

F8**[**'collective investment undertaking' means—

(*a*) an undertaking for collective investment in transferable securities authorised in accordance with the European Communities (Undertakings for Collective Investment in Transferable Securities) Regulations 2011 (S.I. No. 352 of 2011) or otherwise in accordance with the Directive of 2009,

(*b*) an alternative investment fund within the meaning of the European Union (Alternative Investment Fund Managers) Regulations 2013 (S.I. No. 257 of 2013),

(*c*) a management company authorised in accordance with the European Communities (Undertakings for Collective Investment in Transferable Securities) Regulations 2011 or otherwise in accordance with the Directive of 2009, or

(*d*) an alternative investment fund manager within the meaning of the European Union (Alternative Investment Fund Managers) Regulations 2013;**]**

"competent authority" has the meaning assigned to it by *sections 60* and *61*;

F9**[**'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, or

(*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;**]**

"credit institution" means—

F10**[**(*a*) a credit institution within the meaning of point (1) of Article 4(1) of the Capital Requirements Regulation, or**]**

(*b*) An Post in respect of any activity that it carries out, whether as principal or agent, that would render it, or a principal for whom it is an agent, a credit institution as a result of the application of *paragraph (a)*;

"customer"—

(*a*) in relation to an auditor, means—

[3] OJ No. L 176, 27.6.2013 p. 1

(i) a body corporate to which the auditor has been appointed as an auditor, or

(ii) in the case of an auditor appointed to audit the accounts of an unincorporated body of persons or of an individual, the unincorporated body or the individual,

(*b*) in relation to a relevant independent legal professional, includes, in the case of the provision of services by a barrister, a person who is a client of a solicitor seeking advice from the barrister for or on behalf of the client and does not, in that case, include the solicitor, or

(*c*) in relation to a trust or company service provider, means a person with whom the trust or company service provider has an arrangement to provide services as such a service provider;

"Department" means the Department of Justice, Equality and Law Reform;

"designated accountancy body" means a prescribed accountancy body, within the meaning of Part 2 of the Companies (Auditing and Accounting) Act 2003;

"designated person" has the meaning assigned to it by *section 25*;

F11**[**'Directive of 2009' means Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009[4] on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS);**]**

"EEA State" means a state that is a Contracting Party to the Agreement on the European Economic Area signed at Oporto on 2 May 1992, as adjusted by the Protocol signed at Brussels on 17 March 1993;

F11**[**'electronic money' means electronic money within the meaning of the European Communities (Electronic Money) Regulations 2011 (S.I. No. 183 of 2011);**]**

F12**[**...**]**

"external accountant" means a person who by way of business provides accountancy services (other than when providing such services to the employer of the person) whether or not the person holds accountancy qualifications or is a member of a designated accountancy body;

F13**[**'financial institution' means—

(*a*) an undertaking that carries out one or more of the activities set out at reference numbers 2 to 12, 14 and 15 of the Schedule to the European Union (Capital Requirements) Regulations 2014 (S.I. No. 158 of 2014) or foreign exchange services, but does not include an undertaking—

(i) that does not carry out any of the activities set out at those reference numbers other than one or more of the activities set out at reference number 7, and

(ii) whose only customers (if any) are members of the same group as the undertaking,

(*b*) an insurance undertaking within the meaning of Regulation 3 of the European Union (Insurance and Reinsurance) Regulations 2015 (S.I. No. 485 of 2015), in so far as it carries out life assurance activities,

(*c*) a person, other than a person falling within Regulation 4(1) of the European Union (Markets in Financial Instruments) Regulations 2017 (S.I. No. 375 of 2017), whose regular occupation or business is—

[4] OJ No. L 302, 17.11.2009, p. 32

(i) the provision to other persons, or the performance, of investment services and activities within the meaning of those Regulations, or

(ii) bidding directly in auctions in accordance with Commission Regulation (EU) No 1031/2010 of 12 November 2010[5] on the timing, administration and other aspects of auctioning of greenhouse gas emission allowances pursuant to Directive 2003/87/EC of the European Parliament and of the Council establishing a scheme for greenhouse gas emission allowances trading within the Community on behalf of its clients,

(*d*) an investment business firm within the meaning of the Investment Intermediaries Act 1995 (other than a non-life insurance intermediary within the meaning of that Act),

(*e*) a collective investment undertaking that markets or otherwise offers its units or shares,

(*f*) an insurance intermediary within the meaning of the Insurance Mediation Directive (other than a tied insurance intermediary within the meaning of that Directive) that provides life assurance or other investment-related services, or

(*g*) An Post, in respect of any activity it carries out, whether as principal or agent—

(i) that would render it, or a principal for whom it is an agent, a financial institution as a result of the application of any of the foregoing paragraphs,

(ii) that is set out at reference number 1 in the Schedule to the European Union (Capital Requirements) Regulations 2014, or

(iii) that would render it, or a principal for whom it is an agent, an investment business firm within the meaning of the Investment Intermediaries Act 1995 (other than a non-life insurance intermediary within the meaning of that Act) if section 2(6) of that Act did not apply;**]**

F13**[**'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 of the European Parliament and of the Council of 26 June 2013[6] on the annual 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;**]**

F11**[**'high-risk third country' means a jurisdiction identified by the European Commission in accordance with Article 9 of the Fourth Money Laundering Directive;**]**

"Insurance Mediation Directive" means Directive 2002/92/EC of the European Parliament and of the Council of 9 December 2002 on insurance mediation [7];

F12**[**...**]**

"Markets in Financial Instruments Directive" means 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 [9];

[5] OJ No. L 302, 18.11.2010, p. 1
[6] OJ No. L 182, 29.6.2013, p. 19
[7] OJ L 9, 15.1.2003, p. 3
[9] OJ L 145, 30.4.2004, p. 1

"member", in relation to a designated accountancy body, means a member, within the meaning of Part 2 of the Companies (Auditing and Accounting) Act 2003, of a designated accountancy body;

"member", in relation to the Irish Taxation Institute, means a person who is subject to the professional and ethical standards of the Institute, including its investigation and disciplinary procedures, but does not include a person who is admitted to its membership as a student;

F11**[**'monitoring', in relation to a business relationship between a designated person and a customer, means the designated person, on an ongoing basis—

(*a*) scrutinising transactions, and the source of wealth or of funds for those transactions, undertaken during the relationship in order to determine if the transactions are consistent with the designated person's knowledge of—

(i) the customer,

(ii) the customer's business and pattern of transactions, and

(iii) the customer's risk profile (as determined under section 30B),

and

(*b*) ensuring that documents, data and information on customers are kept up to date in accordance with its internal policies, controls and procedures adopted in accordance with section 54;**]**

F11**[**'national risk assessment' means the assessment carried out by the State in accordance with paragraph 1 of Article 7 of the Fourth Money Laundering Directive;**]**

F14**[**'occasional transaction' means, in relation to a customer of a designated person where the designated person does not have a business relationship with the customer, a single transaction, or a series of transactions that are or appear to be linked to each other, and—

(*a*) in a case where the designated person concerned is a person referred to in section 25(1)(h), that the amount of money or the monetary value concerned—

(i) paid to the designated person by the customer, or

(ii) paid to the customer by the designated person,

is in aggregate not less than €2,000,

F15**[**(*b*) in a case where the transaction concerned consists of a transfer of funds (within the meaning of Regulation (EU) No. 2015/847 of the European Parliament and of the Council of 20 May 2015[7]) that the amount of money to be transferred is in aggregate not less than €1,000,**]**

F16**[**(*bb*) in a case where the designated person concerned is a person referred to in *section 25(1)(i)*, that the amount concerned—

(i) paid to the designated person by the customer, or

(ii) paid to the customer by the designated person,

is in aggregate not less than €10,000, and**]**

(*c*) in a case other than one referred to in *paragraphs* F15**[***(a), (b)* or *(bb)***]**, that the amount or aggregate of amounts concerned is not less than €15,000;**]**

"payment service" has the same meaning as in the Payment Services Directive;

[7] OJ No. L 141, 5.6.2015, p. 1

"Payment Services Directive" means 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 [10];

"professional service provider" means an auditor, external accountant, tax adviser, relevant independent legal professional or trust or company service provider;

"property service provider" means a person who by way of business carries out any of the following services in respect of property located in or outside the State:

(*a*) the auction of property other than land;

(*b*) the purchase or sale, by whatever means, of land;

but does not include a service provided by a local authority in the course of the performance of its statutory functions under any statutory provision;

F13**[**'public body' means an FOI body within the meaning of the Freedom of Information Act 2014;**]**

F12**[**...**]**

F13**[**'regulated market' means—

(*a*) a regulated market with the meaning of point (21) of Article 4(1) of Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014[8] on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, located within the EEA, or

(*b*) a regulated market that subjects companies whose securities are admitted to trading to disclosure obligations which are equivalent to the following:

(i) disclosure obligations set out in Articles 17 and 19 of Regulation (EU) No. 596/2014 of the European Parliament and of the Council of 16 April 2014[9] on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC,

(ii) disclosure obligations consistent with Articles 3, 5, 7, 8, 10, 14 and 16 of Directive 2003/71/EC of the European Parliament and of the Council of 4 November 2003[10] on the prospectuses to be published when securities are offered to the public or admitted to trading and amending Directive 2001/34/EC,

(iii) disclosure obligations consistent with Articles 4 to 6, 14, 16 to 19 and 30 of Directive 2004/109/EC of the European Parliament and of the Council of 15 December 2004[11] on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC, and

(iv) disclosure requirements consistent with EU legislation made under the provisions mentioned in *subparagraphs (i)* to *(iii)*;**]**

F11**[**'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;**]**

[10] OJ L 319, 5.12.2007, p.1
[8] OJ No. L 173, 12.6.2014, p. 349
[9] OJ No. L 173, 12.6.2014, p. 1
[10] OJ No. L 345, 31.12.2003, p. 64
[11] OJ No. L 390, 31.12.2004, p. 38

"solicitor" means a practising solicitor;

"State competent authority" has the meaning assigned to it by *section 62*;

"tax adviser" means a person who by way of business provides advice about the tax affairs of other persons;

"transaction" means—

(*a*) in relation to a professional service provider, any transaction that is carried out in connection with a customer of the provider and that is—

(i) in the case of a provider acting as an auditor, the subject of an audit carried out by the provider in respect of the accounts of the customer,

(ii) in the case of a provider acting as an external accountant or tax adviser, or as a trust or company service provider, the subject of a service carried out by the provider for the customer, or

(iii) in the case of a provider acting as a relevant independent legal professional, the subject of a service carried out by the professional for the customer of a kind referred to in *paragraph (a)* or *(b)* of the definition of "relevant independent legal professional" in this subsection;

and

(*b*) in relation to a casino or private members' club, a transaction, such as the purchase or exchange of tokens or chips, or the placing of a bet, carried out in connection with gambling activities carried out on the premises of the casino or club by a customer of the casino or club;

F11**[**'transferable securities' means transferable securities within the meaning of the European Union (Markets in Financial Instruments) Regulations 2017;**]**

"trust or company service provider" means any person whose business it is to provide any of the following services:

(*a*) forming companies or other bodies corporate;

(*b*) acting as a director or secretary of a company under an arrangement with a person other than the company;

(*c*) arranging for another person to act as a director or secretary of a company;

(*d*) acting, or arranging for a person to act, as a partner of a partnership;

(*e*) providing a registered office, business address, correspondence or administrative address or other related services for a body corporate or partnership;

(*f*) acting, or arranging for another person to act, as a trustee of a trust;

(*g*) acting, or arranging for another person to act, as a nominee shareholder for a person other than a company whose securities are listed on a regulated market.

(2) The Minister may prescribe a regulated financial market for the purposes of the definition of "regulated market" in *subsection (1)* only if the Minister is satisfied that the market is in a place other than an EEA State that imposes, on companies whose securities are admitted to trading on the market, disclosure requirements consistent with legislation of the European Communities.

Annotations

Amendments:

F8 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 4(a), S.I. No. 486 of 2018.

F9 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 3(b), S.I. No. 486 of 2018.

F10 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 4(c), S.I. No. 486 of 2018.

F11 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 4(d), (e), (i), (k), (p), (q), S.I. No. 486 of 2018.

F12 Deleted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 4(f), (j), (n), S.I. No. 486 of 2018.

F13 Substituted Deleted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 4(g), (h), (m), (o), S.I. No. 486 of 2018.

F14 Substituted (14.06.2013) by *Criminal Justice Act 2013* (19/2013), s. 4, S. I. No. 196 of 2013.

F15 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 4(l)(i), (iii), S.I. No. 486 of 2018.

F16 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 4(l)(ii), S.I. No. 486 of 2018.

Modifications (not altering text):

C4 Definition of "occasional transaction" modified (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Section 25) (Prescribed Class of Designated Person) Regulations 2018* (S.I. No. 487 of 2018), reg. 4, in effect as per reg. 1(2).

3. (1) Providers of gambling services are prescribed as a class of persons for the purposes of section 25(1)(j) of the Act of 2010.

(2) In this Regulation, "gambling services" means gambling services within the meaning of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 20151 other than—

(a) poker games provided at a physical location other than a casino or private members' club,

(b) lotteries within the meaning of the Gaming and Lotteries Act 1956 (No. 2 of 1956), and

(c) gaming machines (within the meaning of section 43 of the Finance Act 1975 (No. 6 of 1975)) or amusement machines (within the meaning of section 120 of the Finance Act 1992 (No. 9 of 1992)) provided in accordance with section 14 of the Gaming and Lotteries Act 1956 .

4. Insofar as a person is a designated person by virtue of being a member of the class of persons prescribed in Regulation 3, the definition of "occasional transaction" in section 24 of the Act of 2010 shall be modified so that the reference in paragraph (a) of that definition to "a person referred to in section 25(1)(h)" be read as a reference to a member of the class of persons prescribed in Regulation 3.

Meaning of "designated person".

25.— (1) In this Part, "designated person" means any person, acting in the State in the course of business carried on by the person in the State, who or that is—

(*a*) a credit institution, except as provided by *subsection (4)*,

(*b*) a financial institution, except as provided by *subsection (4)*,

(*c*) an auditor, external accountant or tax adviser,

F17**[**(d) subject to *subsection (1A)*, a relevant independent legal professional,**]**

(*e*) a trust or company service provider,

(*f*) a property service provider,

(*g*) a casino,

(*h*) a person who effectively directs a private members' club at which gambling activities are carried on, but only in respect of those gambling activities,

(*i*) any person trading in goods, but only in respect of transactions involving payments, to the person F18**[**or by the person**]** in cash, of a total of at least F17**[**€10,000**]** (whether in one transaction or in a series of transactions that are or appear to be linked to each other), or

(*j*) any other person of a prescribed class.

F18**[**(1A) A relevant independent legal professional shall be a designated person only as respects the carrying out of the services specified in the definition of 'relevant independent legal professional' in *section 24(1)*.**]**

(2) For the purposes of this Part, a person is to be treated as a designated person only in respect of those activities or services that render the person a designated person.

(3) A reference in this Part to a designated person does not include a reference to any of the following:

(*a*) the Minister for Finance;

(*b*) the F19**[**Central Bank of Ireland**]**;

(*c*) the National Treasury Management Agency.

(4) A person is not to be treated as a designated person for the purposes of this Part solely as a result of operating as a credit institution or financial institution, in the course of business, if—

(*a*) the annual turnover of the person's business that is attributable to operating as a credit institution or financial institution is €70,000 (or such other amount as may be prescribed) or less,

(*b*) the total of any single transaction, or a series of transactions that are or appear to be linked to each other, in respect of which the person operates as a credit institution or financial institution does not exceed €1,000 (or such other lesser amount as may be prescribed),

(*c*) the annual turnover of the person's business that is attributable to operating as a credit institution or financial institution does not exceed 5 per cent of the business's total annual turnover,

(*d*) the person's operation as a credit institution or financial institution is directly related and ancillary to the person's main business activity, and

(*e*) the person provides services when operating as a credit institution or financial institution only to persons who are customers in respect of the person's main business activity, rather than to members of the public in general.

(5) *Subsection (4)* does not apply in relation to any prescribed class of person.

(6) For the avoidance of doubt and without prejudice to the generality of *subsection (1)(a)* or *(b)*, a credit or financial institution that acts in the State in the course of business carried on by the institution in the State, by means of a branch situated in

the State, is a designated person whether or not the institution is incorporated, or the head office of the institution is situated, in a place other than in the State.

(7) The Minister may prescribe a class of persons for the purposes of *subsection (1)(j)* only if the Minister is satisfied that any of the business activities engaged in by the class—

(*a*) may be used for the purposes of—

(i) money laundering,

(ii) terrorist financing, or

(iii) an offence that corresponds or is similar to money laundering or terrorist financing under the law of a place outside the State,

or

(*b*) are of a kind likely to result in members of the class obtaining information on the basis of which they may become aware of, or suspect, the involvement of customers or others in money laundering or terrorist financing.

(8) The Minister may, in any regulations made under *subsection (7)* prescribing a class of persons, apply to the class such exemptions from, or modifications to, provisions of this Act as the Minister considers appropriate, having regard to any risk that the business activities engaged in by the class may be used for a purpose referred to in *paragraph (a)* of that subsection.

(9) The Minister may prescribe an amount for the purposes of *paragraph (a)* or *(b)* of *subsection (4)*, in relation to a person's business activities as a credit institution or financial institution, only if the Minister is satisfied that, in prescribing the amount, the purposes of that subsection will likely be fulfilled, including that—

(*a*) those activities are carried out by the person on a limited basis, and

(*b*) there is little risk that those activities may be used for a purpose referred to in *subsection (7)(a)*.

(10) The Minister may prescribe a class of persons for the purpose of *subsection (5)* only if the Minister is satisfied that the application of *subsection (4)* to the class involves an unacceptable risk that the business activities engaged in by the class may be used for a purpose referred to in *subsection (7)(a)*.

Annotations

Amendments:

F17 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 5(a)(i), (ii)(II), S.I. No. 486 of 2018.

F18 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 5(a)(ii)(I), (b), S.I. No. 486 of 2018.

F19 Substituted (1.10.2010) by *Central Bank Reform Act 2010* (23/2010), s. 15(14) and sch. 2 part 14 par. 33, S.I. No. 469 of 2010.

Editorial Notes:

E12 Power pursuant to subss. (7), (8) exercised (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Section 25) (Prescribed Class of Designated Person) Regulations 2018* (S.I. No. 487 of 2018), in effect as per reg. 1(2).

E13 Previous affecting provision: subss. (1)(d) substituted and (1A) inserted by *Criminal Justice Act 2013* (19/2013), s. 5, not commenced; substituted and inserted as per F-note above.

Beneficial owner in relation to bodies corporate.

F20**[26.** In this Part, 'beneficial owner', in relation to a body corporate, has the meaning given to it by point (6)(a) of Article 3 of the Fourth Money Laundering Directive.**]**

Annotations

Amendments:

F20 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 6, S.I. No. 486 of 2018.

Beneficial owner in relation to partnerships.

27.— In this Part, "beneficial owner", in relation to a partnership, means any individual who—

(*a*) ultimately is entitled to or controls, whether the entitlement or control is direct or indirect, more than a 25 per cent share of the capital or profits of the partnership or more than 25 per cent of the voting rights in the partnership, or

(*b*) otherwise F21**[**controls**]** the partnership.

Annotations

Amendments:

F21 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 7, S.I. No. 486 of 2018.

Beneficial owner in relation to trusts.

28.— (1) F22**[**...**]**

(2) In this Part, "beneficial owner", in relation to a trust, means any of the following:

(*a*) any individual who is entitled to a vested interest in possession, remainder or reversion, whether or not the interest is defeasible, in F22**[**...**]** the capital of the trust property;

(*b*) in the case of a trust other than one that is set up or operates entirely for the benefit of individuals referred to in *paragraph (a)*, the class of individuals in whose main interest the trust is set up or operates;

(*c*) any individual who has control over F23**[**the trust;**]**

F24**[**(*d*) the settlor;

(*e*) the trustee;

(*f*) the protector.**]**

(3) For the purposes of and without prejudice to the generality of *subsection (2)*, an individual who is the beneficial owner of a body corporate that—

(*a*) is entitled to a vested interest of the kind referred to in *subsection (2)(a)*, or

(*b*) has control over the trust,

is taken to be entitled to the vested interest or to have control over the trust (as the case may be).

(4) Except as provided by *subsection (5)*, in this section "control", in relation to a trust, means a power (whether exercisable alone, jointly with another person or with the consent of another person) under the trust instrument concerned or by law to do any of the following:

(*a*) dispose of, advance, lend, invest, pay or apply trust property;

(*b*) vary the trust;

(*c*) add or remove a person as a beneficiary or to or from a class of beneficiaries;

(*d*) appoint or remove trustees;

(*e*) direct, withhold consent to or veto the exercise of any power referred to in *paragraphs (a)* to *(d)*.

(5) For the purposes of the definition of "control" in *subsection (4)*, an individual does not have control solely as a result of the power exercisable collectively at common law to vary or extinguish a trust where the beneficiaries under the trust are at least 18 years of age, have full capacity and (taken together) are absolutely entitled to the property to which the trust applies.

Annotations

Amendments:

F22 Deleted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 8(a), (b)(i), S.I. No. 486 of 2018.

F23 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 8(b)(ii), S.I. No. 486 of 2018.

F24 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 8(b)(iii), S.I. No. 486 of 2018.

Beneficial owner in relation to estates of deceased persons.

29.— In this Part, "beneficial owner", in relation to an estate of a deceased person in the course of administration, means the executor or administrator of the estate concerned.

Other persons who are beneficial owners.

30.— (1) In this Part, "beneficial owner", in relation to a legal entity or legal arrangement, other than where *section 26, 27* or *28*, applies, means—

(*a*) if the individuals who benefit from the entity or arrangement have been determined, any individual who benefits from F25**[**...**]** the property of the entity or arrangement,

(*b*) if the individuals who benefit from the entity or arrangement have yet to be determined, the class of such individuals in whose main interest the entity or arrangement is set up or operates, and

(*c*) any individual who exercises control over F25**[**...**]** the property of the entity F26**[**or arrangement,**]**

F27**[**(*d*) any person holding a position, in relation to the legal entity or legal arrangement that is similar or equivalent to the position specified in *paragraphs (d)* to *(f)* of *section 28(2)* in relation to a trust.**]**

(2) For the purposes of and without prejudice to the generality of *subsection (1)*, any individual who is the beneficial owner of a body corporate that benefits from or exercises control over the property of the entity or arrangement is taken to benefit from or exercise control over the property of the entity or arrangement.

(3) In this Part, "beneficial owner", in relation to a case other than a case to which *section 26, 27, 28* or *29*, or *subsection (1)* of this section, applies, means any individual who ultimately owns or controls a customer or on whose behalf a transaction is conducted.

(4) F25**[**...**]**

Annotations

Amendments:

F25 Deleted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 9(a)(i), (ii)(I), (b), S.I. No. 486 of 2018.

F26 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 9(a)(ii)(II), S.I. No. 486 of 2018.

F27 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 9(a)(iii), S.I. No. 486 of 2018.

F28**[**Chapter 1A

Risk assessment by designated persons**]**

Annotations

Amendments:

F28 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 10, S.I. No. 486 of 2018.

F29**[**Business risk assessment by designated persons

30A. (1) A designated person shall carry out an assessment (in this Act referred to as a 'business risk assessment') to identify and assess the risks of money laundering and terrorist financing involved in carrying on the designated person's business activities taking into account at least the following risk factors:

(*a*) the type of customer that the designated person has;

(*b*) the products and services that the designated person provides;

(*c*) the countries or geographical areas in which the designated person operates;

(*d*) the type of transactions that the designated person carries out;

(*e*) the delivery channels that the designated person uses;

(*f*) other prescribed additional risk factors.

(2) A designated person carrying out a business risk assessment shall have regard to the following:

(*a*) any information in the national risk assessment which is of relevance to all designated persons or a particular class of designated persons of which the designated person is a member;

(*b*) any guidance on risk issued by the competent authority for the designated person;

(*c*) where the designated person is a credit institution or financial institution, any guidelines addressed to credit institutions and financial institutions issued by the European Banking Authority, the European Securities and Markets Authority or the European Insurance and Occupational Pensions Authority in accordance with the Fourth Money Laundering Directive.

(3) A business risk assessment shall be documented unless a competent authority for a designated person decides under Article 8 of the Fourth Money Laundering Directive that an individual documented risk assessment is not required and notifies the designated person.

(4) A designated person shall keep the business risk assessment, and any related documents, up to date in accordance with its internal policies, controls and procedures adopted in accordance with *section 54*.

(5) A business risk assessment shall be approved by senior management.

(6) A designated person shall make records of a business risk assessment available, on request, to the competent authority for that designated person.

(7) The Minister may prescribe additional risk factors to be taken into account in a risk assessment under *subsection (1)* only where he or she is satisfied that it is appropriate to consider such matters in order to accurately identify and assess the risks of money laundering or terrorist financing.

(8) A designated person who fails to comply with this section commits an offence and is liable—

(*a*) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment to a fine or imprisonment not exceeding 5 years (or both).**]**

Annotations

Amendments:

F29 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 10, S.I. No. 486 of 2018.

Editorial Notes:

E14 A class A fine is defined as a fine not exceeding €5,000 (4.01.2011) by *Fines Act 2010* (8/2010), s. 3, S.I. No. 662 of 2010.

F30**[**Application of risk assessment in applying customer due diligence

30B. (1) For the purposes of determining the extent of measures to be taken under *subsections (2)* and *(2A)* of *section 33* and *subsections (1)* and *(3)* of *section 35* a designated person shall identify and assess the risk of money laundering and terrorist financing in relation to the customer or transaction concerned, having regard to—

(*a*) the relevant business risk assessment,

(*b*) the matters specified in *section 30A(2)*,

(*c*) any relevant risk variables, including at least the following:

(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 of transactions or duration of the business relationship;

(iv) any additional prescribed risk variable,

(*d*) the presence of any factor specified in *Schedule 3* or prescribed under *section 34A* suggesting potentially lower risk,

(*e*) the presence of any factor specified in *Schedule 4*, and

(*f*) any additional prescribed factor suggesting potentially higher risk.

(2) A determination by a designated person under *subsection (1)* shall be documented where the competent authority for the designated person, having regard to the size and nature of the designated person and the need to accurately identify and assess the risks of money laundering or terrorist financing, so directs.

(3) For the purposes of *subsection (2)*, a State competent authority may direct a class of designated persons for whom it is the competent authority to document a determination in writing.

(4) The Minister may prescribe additional risk variables to which regard is to be had under *subsection (1)(c)(iv)* only where he or she is satisfied that it is appropriate to consider such matters in order to accurately identify and assess the risks of money laundering or terrorist financing.

(5) A designated person who fails to document a determination in accordance with a direction under *subsection (2)* commits an offence and is liable—

(*a*) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment to a fine or imprisonment not exceeding 5 years (or both).**]**

Annotations

Amendments:

F30 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 10, S.I. No. 486 of 2018.

Editorial Notes:

E15 A class A fine is defined as a fine not exceeding €5,000 (4.01.2011) by *Fines Act 2010* (8/2010), s. 3, S.I. No. 662 of 2010.

Chapter 2

Designation of places other than Member States — procedures for detecting money laundering or terrorist financing

Designation of places imposing requirements equivalent to Third Money Laundering Directive.

31.—F31**[**...**]**

Annotations

Amendments:

F31 Repealed (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 40(b), S.I. No. 486 of 2018.

Editorial Notes:

E16 Previous affecting provision: power pursuant to subs. (1) exercised (30.09.2012) by *Criminal Justice (Money Laundering and Terrorist Financing) (Section 31) Order 2012* (S.I. No. 347 of 2012), art. 4, in effect as per art. 2; enabling provision repealed as per F-note above.

E17 Previous affecting provision: power pursuant to subs. (1) exercised (15.07.2010) by *Criminal Justice (Money Laundering and Terrorist Financing) (Section 31) Order 2010* (S.I. No. 343 of 2010), in effect as per art. 2; revoked (30.09.2012) by *Criminal Justice (Money Laundering and Terrorist Financing) (Section 31) Order 2012* (S.I. No. 347 of 2012), art. 4, in effect as per art. 2.

Designation of places having inadequate procedures for detection of money laundering or terrorist financing.

32.—F32**[...]**

Annotations

Amendments:

F32 Repealed (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 40(b), S.I. No. 486 of 2018.

Chapter 3

Customer Due Diligence

Identification and verification of customers and beneficial owners.

33.— (1) A designated person shall apply the measures specified in F33**[***subsection (2)***]**, in relation to a customer of the designated person—

(*a*) prior to establishing a business relationship with the customer,

(*b*) prior to carrying out an occasional transaction with, for or on behalf of the customer or assisting the customer to carry out an occasional transaction,

F34**[**(c) prior to carrying out any service for the customer, if, having regard to the circumstances, including—

(i) the customer, or the type of customer, concerned,

(ii) the type of any business relationship which the person has with the customer,

(iii) the type of service or of any transaction or product in respect of which the service is sought,

(iv) the purpose (or the customer's explanation of the purpose) of the service or of any transaction or product in respect of which the service is sought,

(v) the value of any transaction or product in respect of which the service is sought,

(vi) the source (or the customer's explanation of the source) of funds for any such transaction or product,

the person has reasonable grounds to suspect that the customer is involved in, or the service, transaction or product sought by the customer is for the purpose of, money laundering or terrorist financing, or**]**

or

(*d*) prior to carrying out any service for the customer if—

(i) the person has reasonable grounds to doubt the veracity or adequacy of documents (whether or not in electronic form) or information that the person has previously obtained for the purpose of verifying the identity of the customer, whether obtained under this section or section 32 of the Criminal Justice Act 1994 ("the 1994 Act") prior to its repeal by this Act or under any administrative arrangements that the person may have applied before section 32 of the 1994 Act operated in relation to the person, and

(ii) the person has not obtained any other documents or information that the person has reasonable grounds to believe can be relied upon to confirm the identity of the F33**[**customer,**]**

F35**[**and

(*e*) at any time, including a situation where the relevant circumstances of a customer have changed, where the risk of money laundering and terrorist financing warrants their application.**]**

(2) The measures that shall be applied F35**[**, in accordance with *section 30B*,**]** by a designated person under *subsection (1)* are as follows:

(*a*) identifying the customer, and verifying the customer's identity on the basis of documents (whether or not in electronic form), or information, that the designated person has reasonable grounds to believe can be relied upon to confirm the identity of the customer, including—

(i) documents from a government source (whether or not a State government source), or

(ii) any prescribed class of documents, or any prescribed combination of classes of documents;

(*b*) identifying any beneficial owner connected with the customer or service concerned, and taking measures reasonably warranted by the risk of money laundering or terrorist financing—

(i) to verify the beneficial owner's identity to the extent necessary to ensure that the person has reasonable grounds to be satisfied that the person knows who the beneficial owner is, and

(ii) in the case of a legal entity or legal arrangement of a kind referred to in *section 26, 27, 28* or *30*, to understand the ownership and control structure of the entity or arrangement concerned.

F35**[**(2A) When applying the measures specified in *subsection (2)*, a designated person shall verify that any person purporting to act on behalf of the customer is so

authorised and identify and verify the identity of that person in accordance with *subsection (2)*.**]**

(3) Nothing in *subsection (2)(a)(i)* or *(ii)* limits the kinds of documents or information that a designated person may have reasonable grounds to believe can be relied upon to confirm the identity of a customer.

(4) F36**[**...**]**

(5) Notwithstanding *subsection (1)(a)*, a designated person may verify the identity of a customer or beneficial owner, in accordance with F33**[***subsection (2)***]**, during the establishment of a business relationship with the customer if the designated person has reasonable grounds to believe that—

(*a*) verifying the identity of the customer or beneficial owner (as the case may be) prior to the establishment of the relationship would interrupt the normal conduct of business, and

(*b*) there is no real risk that the customer is involved in, or the service sought by the customer is for the purpose of, money laundering or terrorist financing,

but the designated person shall take reasonable steps to verify the identity of the customer or beneficial owner, in accordance with F33**[***subsection (2)***]**, as soon as practicable.

(6) Notwithstanding *subsection (1)(a)*, F33**[**a credit institution or financial institution may allow an account, including an account that permits transactions in transferable securities, to be opened with it**]** by a customer before verifying the identity of the customer or a beneficial owner, in accordance with F33**[***subsection (2)***]**, so long as the institution ensures that transactions in connection with the account are not carried out by or on behalf of the customer or beneficial owner before carrying out that verification.

F37**[**(7) In addition to the measures required in relation to a customer and a beneficial owner under this section, credit institutions and financial institutions shall apply the measures specified in *subsections (7A)* to *(7C)* to the beneficiaries of life assurance and other investment-related assurance policies.

(7A) As soon as the beneficiaries of life assurance and other investment-related assurance policies are identified or designated, a credit institution or financial institution shall—

(*a*) take the names of beneficiaries that are identified as specifically named persons or legal arrangements, and

(*b*) in the case of beneficiaries designated by characteristics, class or other means, obtain sufficient information to satisfy the institution that it will be able to establish the identity of the beneficiary at the time of the payout.

(7B) A credit institution or financial institution shall verify the identity of a beneficiary referred to in *paragraph (a)* or *(b)* of *subsection (7A)* at the time of the payout in accordance with *subsection (2)*.

(7C) In the case of assignment, in whole or in part, of a policy of life assurance or other investment-related assurance to a third party, a credit institution or financial institution that is 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 his or her, or its, own benefit the value of the policy assigned.

(7D) In addition to the measures required in relation to a customer and a beneficial owner, in the case of beneficiaries of trusts or of similar legal arrangements that are designated by particular characteristics or class, a designated person shall obtain sufficient information concerning the beneficiary to satisfy the designated person

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.**]**

(8) F38**[**Subject to *subsection (8A)*, a designated person**]** who is unable to apply the measures specified in F38**[**subsection (2) or (4)**]** in relation to a customer, as a result of any failure on the part of the customer to provide the designated person with documents or information required under this section—

(*a*) shall not provide the service or carry out the transaction sought by that customer for so long as the failure remains unrectified, and

(*b*) shall discontinue the business relationship (if any) with the customer.

F39**[**(8A) Nothing in *subsection (8)* or *section 35(2)* shall operate to prevent a relevant independent legal professional or relevant professional adviser—

(a) ascertaining the legal position of a person, or

(b) performing the task of defending or representing a person in, or in relation to, civil or criminal proceedings, including providing advice on instituting or avoiding such proceedings.**]**

(9) F38**[**A designated person**]** who fails to comply with this section commits an offence and is liable—

(*a*) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).

(10) F36**[**...**]**

(11) The Minister may prescribe a class of documents, or a combination of classes of documents, for the purposes of *subsection (2)(a)(ii)*, only if the Minister is satisfied that the class or combination of documents would be adequate to verify the identity of customers of designated persons.

(12) For the purposes of *subsection (2)(a)(ii)*, the Minister may prescribe different classes of documents, or combinations of classes of documents, for different kinds of designated persons, customers, transactions, services or risks of money laundering or terrorist financing.

Annotations

Amendments:

F33 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 11(a), (b), (g), (h), S.I. No. 486 of 2018.

F34 Substituted (14.06.2013) by *Criminal Justice Act 2013* (19/2013), s. 6, S.I. No. 196 of 2013.

F35 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 11(c), (d), (e), S.I. No. 486 of 2018.

F36 Deleted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 11(f), (m), S.I. No. 486 of 2018.

F37 Substituted and inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 11(i), S.I. No. 486 of 2018.

F38 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 11(j), (l), S.I. No. 486 of 2018.

F39 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 11(k), S.I. No. 486 of 2018.

F40**[**Electronic money derogation

33A. (1) Subject to *section 33(1)(c)* and *(d)* and *subsection (2)*, a designated person is not required to apply the measures specified in *subsection (2)* or *(2A)* of *section 33*, or *section 35*, with respect to electronic money if—

(*a*) the payment instrument concerned—

(i) is not reloadable, or

(ii) cannot be used outside of the State and has a maximum monthly payment transactions limit not exceeding €250,

(*b*) the monetary value that may be stored electronically on the payment instrument concerned does not exceed—

(i) €250, or

(ii) where the payment instrument cannot be used outside the State, €500,

(*c*) the payment instrument concerned is used exclusively to purchase goods and services,

(*d*) the payment instrument concerned cannot be funded with anonymous electronic money,

(*e*) the issuer of the payment instrument concerned carries out sufficient monitoring of the transactions or business relationship concerned to enable the detection of unusual or suspicious transactions, and

(*f*) the transaction concerned is not a redemption in cash or cash withdrawal of the monetary value of the electronic money of an amount exceeding €100.

(2) A designated person shall not apply the exemption provided for in *subsection (1)* if—

(*a*) the customer concerned is established, or resident in, a high-risk third country, or

(*b*) the designated person is required to apply measures, in relation to the customer or beneficial owner (if any) concerned, under *section 37*.**]**

Annotations

Amendments:

F40 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 12, S.I. No. 486 of 2018.

Editorial Notes:

E18 The section heading is taken from the amending section in the absence of one included in the amendment.

Exemptions from *section 33*.

34.—F41**[**...**]**

Annotations

Amendments:

F41 Repealed (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 40(b), S.I. No. 486 of 2018.

Editorial Notes:

E19 Previous affecting provision: subs. (1) substituted (14.06.2013) by *Criminal Justice Act 2013* (19/2013), s. 7, S.I. No. 196 of 2013; section repealed as per F-note above.

F42**[**Simplified customer due diligence

34A. (1) Subject to *section 33(1)(c)* and *(d)*, a designated person may take the measures specified in *sections 33(2)* and *35* in such manner, to such extent and at such times as is reasonably warranted by the lower risk of money laundering or terrorist financing in relation to a business relationship or transaction where the designated person—

(*a*) identifies in the relevant business risk assessment, an area of lower risk into which the relationship or transaction falls, and

(*b*) considers that the relationship or transaction presents a lower degree of risk.

(2) For the purposes of identifying an area of lower risk a designated person shall have regard to—

(*a*) the matters specified in *section 30A(2)*,

(*b*) the presence of any factor specified in *Schedule 3*, and

(*c*) any additional prescribed factor suggesting potentially lower risk.

(3) Where a designated person applies simplified due diligence measures in accordance with *subsection (1)* it shall—

(*a*) keep a record of the reasons for its determination and the evidence on which it was based, and

(*b*) carry out sufficient monitoring of the transactions and business relationships to enable the designated person to detect unusual or suspicious transactions.

(4) The Minister may prescribe other factors, additional to those specified in *Schedule 3*, to which a designated person is to have regard under *subsection (2)* only if he or she is satisfied that the presence of those factors suggests a potentially lower risk of money laundering or terrorist financing.

(5) For the purposes of *subsection (1)*, a business relationship or transaction may be considered to present a lower degree of risk if a reasonable person having regard to the matters specified in *paragraphs (a)* to *(f)* of *section 30B(1)* would determine that the relationship or transaction presents a lower degree of risk of money laundering or terrorist financing.**]**

Annotations

Amendments:

F42 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 13, S.I. No. 486 of 2018.

Editorial Notes:

E20 The section heading is taken from the amending section in the absence of one included in the amendment.

Special measures applying to business relationships.

35.— (1) A designated person shall obtain information reasonably warranted by the risk of money laundering or terrorist financing on the purpose and intended nature of a business relationship with a customer prior to the establishment of the relationship.

(2) F43**[**Subject to *section 33(8A)*, a designated person**]** who is unable to obtain such information, as a result of any failure on the part of the customer, shall not provide the service sought by the customer for so long as the failure continues.

F43**[**(3) A designated person shall monitor any business relationship that it has with a customer to the extent reasonably warranted by the risk of money laundering or terrorist financing.**]**

(4) Except as provided by *section 36*, a designated person who fails to comply with this section commits an offence and is liable—

(*a*) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).

Annotations

Amendments:

F43 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 14(a), (b), S.I. No. 486 of 2018.

Exemption from *section 35(1)*.

36.—F44**[**...**]**

Annotations

Amendments:

F44 Repealed (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 40(b), S.I. No. 486 of 2018.

Editorial Notes:

E21 Previous affecting provision: subs. (1) substituted (14.06.2013) by *Criminal Justice Act 2013* (19/2013), s. 8, S.I. No. 196 of 2013; section repealed as per F-note above.

F45**[**Examination of background and purpose of certain transactions

36A. (1) A designated person shall, in accordance with policies and procedures adopted in accordance with *section 54*, examine the background and purpose of all complex or unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose.

(2) A designated person shall increase the degree and nature of monitoring of a business relationship in order to determine whether transactions referred to in *subsection (1)* appear suspicious.

(3) A designated person who fails to comply with this section commits an offence and is liable—

(*a*) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).**]**

Annotations

Amendments:

F45 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 15, S.I. No. 486 of 2018.

Editorial Notes:

E22 A class A fine is defined as a fine not exceeding €5,000 (4.01.2011) by *Fines Act 2010* (8/2010), s. 3, S.I. No. 662 of 2010.

E23 The section heading is taken from the amending section in the absence of one included in the amendment.

Enhanced customer due diligence — politically exposed persons.

37.— F46**[**(1) A designated person shall take steps to determine whether or not—

(*a*) a customer, or a beneficial owner connected with the customer or service concerned, or

(*b*) a beneficiary of a life assurance policy or other investment-related assurance policy, or a beneficial owner of the beneficiary,

is a politically exposed person or an immediate family member, or a close associate, of a politically exposed person.**]**

F46**[**(2) The designated person shall take the steps referred to in *subsection (1)*—

(*a*) in relation to a person referred to *subsection (1)(a)*, prior to—

(i) establishing a business relationship with the customer, or

(ii) carrying out an occasional transaction with, for or on behalf of the customer or assisting the customer to carry out an occasional transaction,

and

(*b*) in relation to a person mentioned in *subsection (1)(b)*—

(i) prior to the payout of the policy, or

(ii) at the time of the assignment, in whole or in part, of the policy.**]**

(3) The steps to be taken are such steps as are reasonably warranted by the risk that the customer F47**[**, or beneficiary**]** or beneficial owner (as the case may be) is involved in money laundering or terrorist financing.

F48**[**(4) If a designated person knows or has reasonable grounds to believe that a customer F49**[**...**]** is, or has become, a politically exposed person or an immediate

family member or close associate of a politically exposed person, the designated person shall—

(*a*) ensure that approval is obtained from senior management of the designated person before a business relationship is established or continued with the customer,

(*b*) determine the source of wealth and of funds for the following transactions—

(i) transactions the subject of any business relationship with the customer that are carried out with the customer or in respect of which a service is sought, or

(ii) any occasional transaction that the designated person carries out with, for or on behalf of the customer or that the designated person assists the customer to carry out,

and

F46**[**(*c*) in addition to measures to be applied in accordance with *section 35(3),* apply enhanced monitoring of the business relationship with the customer.**]]**

(5) Notwithstanding *subsections (2)(a)* and *(4)(a),* a credit institution F47**[**or financial institution**]** may allow a bank account to be opened with it by a customer before taking the steps referred to in *subsection (1)* or seeking the approval referred to in *subsection (4)(a),* so long as the institution ensures that transactions in connection with the account are not carried out by or on behalf of the customer or any beneficial owner concerned before taking the steps or seeking the approval, as the case may be.

(6) If a designated person knows or has reasonable grounds to believe that a beneficial owner F49**[**...**]** connected with a customer or with a service sought by a customer, F48**[**is, or has become, a politically exposed person**]** or an immediate family member or close associate of a politically exposed person, the designated person shall apply the measures specified in F48**[***subsection (4)(a), (b)* and *(c)***]** in relation to the customer concerned.

F47**[**(6A) If a designated person knows or has reasonable grounds to believe that a beneficiary of a life assurance or other investment-related assurance policy, or a beneficial owner of the beneficiary concerned, is a politically exposed person, or an immediate family member or a close associate of a politically exposed person, and that, having regard to section 39, there is a higher risk of money laundering or terrorist financing, it shall—

(*a*) inform senior management before payout of policy proceeds, and

(*b*) conduct enhanced scrutiny of the business relationship with the policy holder.**]**

(7) For the purposes of F46**[***subsections (4), (6)* and *(6A)***]**, a designated person is deemed to know that another person is a politically exposed person or an immediate family member or close associate of a politically exposed person if, on the basis of—

(*a*) information in the possession of the designated person (whether obtained under *subsections (1)* to *(3)* or otherwise),

(*b*) in a case where the designated person has contravened *subsection (1)* or *(2),* information that would have been in the possession of the person if the person had complied with that provision, or

(*c*) public knowledge,

there are reasonable grounds for concluding that the designated person so knows.

(8) A designated person who is unable to apply the measures specified in *subsection (1)*, *(3)*, *(4)* or *(6)* in relation to a customer, as a result of any failure on the part of the customer to provide the designated person with documents or information—

(*a*) shall discontinue the business relationship (if any) with the customer for so long as the failure continues, and

(*b*) shall not provide the service or carry out the transaction sought by the customer for so long as the failure continues.

(9) A person who fails to comply with this section commits an offence and is liable—

(*a*) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).

(10) In this section—

"close associate" of a politically exposed person includes any of the following persons:

(*a*) any individual who has joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with the politically exposed person;

(*b*) any individual who has sole beneficial ownership of a legal entity or legal arrangement set up for the actual benefit of the politically exposed person;

"immediate family member" of a politically exposed person includes any of the following persons:

(*a*) any spouse of the politically exposed person;

(*b*) any person who is considered to be equivalent to a spouse of the politically exposed person under the national or other law of the place where the person or politically exposed person resides;

(*c*) any child of the politically exposed person;

(*d*) any spouse of a child of the politically exposed person;

(*e*) any person considered to be equivalent to a spouse of a child of the politically exposed person under the national or other law of the place where the person or child resides;

(*f*) any parent of the politically exposed person;

(*g*) any other family member of the politically exposed person who is of a prescribed class;

"politically exposed person" means an individual who is, or has at any time in the preceding 12 months been, entrusted with a prominent public function, including either of the following individuals (but not including any middle ranking or more junior official):

(*a*) a specified official;

(*b*) a member of the administrative, management orsupervisory body of a state-owned enterprise;

"specified official" means any of the following officials (including any such officials in an institution of the European Communities or an international body):

(*a*) a head of state, head of government, government minister or deputy or assistant government minister;

(*b*) a member of a parliament F47**[**or of a similar legislative body**]**;

F47**[**(*bb*) a member of the governing body of a political party;**]**

(*c*) a member of a supreme court, constitutional court or other high level judicial body whose decisions, other than in exceptional circumstances, are not subject to further appeal;

(*d*) a member of a court of auditors or of the board of a central bank;

F46**[**(*e*) an ambassador, chargé d'affairs or high-ranking officer in the armed forces;**]**

F47**[**(*f*) a director, deputy director or member of the board of, or person performing the equivalent function in relation to, an international organisation.**]**

(11) The Minister may prescribe a class of family member of a politically exposed person, for the purposes of *paragraph (g)* of the definition of "immediate family member" of a politically exposed person in *subsection (10)*, only if the Minister is satisfied that it would be appropriate for the provisions of this section to be applied in relation to members of the class, having regard to any heightened risk, arising from their close family relationship with the politically exposed person, that such members may be involved in money laundering or terrorist financing.

Annotations

Amendments:

F46 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 16(a), (b), (d)(ii), (h), (i)(iii), S.I. No. 486 of 2018.

F47 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 16(c), (e), (g), (i)(i), (ii), (iii), S.I. No. 486 of 2018.

F48 Substituted (14.06.2013) by *Criminal Justice Act 2013* (19/2013), s. 9, S.I. No. 196 of 2013.

F49 Deleted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 16(d)(ii), (f), S.I. No. 486 of 2018.

Enhanced customer due diligence — correspondent banking relationships.

F50**[38.** (1) A credit institution or financial institution ('the institution') shall not enter into a correspondent relationship with another credit institution or financial institution ('the respondent institution') situated in a place other than a Member State unless, prior to commencing the relationship, the institution—

(*a*) has gathered sufficient information about the respondent institution to understand fully the nature of the business of the respondent institution,

(*b*) is satisfied on reasonable grounds, based on publicly available information, that the reputation of the respondent institution, and the quality of supervision or monitoring of the operation of the respondent institution in the place, are sound,

(*c*) is satisfied on reasonable grounds, having assessed the anti-money laundering and anti-terrorist financing controls applied by the respondent institution, that those controls are sound,

(*d*) has ensured that approval has been obtained from the senior management of the institution,

(*e*) has documented the responsibilities of each institution in applying anti-money laundering and anti-terrorist financing controls to customers in the conduct of the correspondent relationship and, in particular—

(i) the responsibilities of the institution arising under this Part, and

(ii) any responsibilities of the respondent institution arising under requirements equivalent to those specified in the Fourth Money Laundering Directive,

and

(*f*) in the case of a proposal that customers of the respondent institution have direct access to a payable-through account held with the institution in the name of the respondent institution, is satisfied on reasonable grounds that the respondent institution—

(i) has identified and verified the identity of those customers, and is able to provide to the institution, upon request, the documents (whether or not in electronic form) or information used by the institution to identify and verify the identity of those customers,

(ii) has applied measures equivalent to the measure referred to in *section 35(1)* in relation to those customers, and

(iii) is applying measures equivalent to the measure referred to in *section 35(3)* in relation to those customers.

(2) A person who fails to comply with this section commits an offence and is liable—

(*a*) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).**]**

Annotations

Amendments:

F50 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 17, S.I. No. 486 of 2018.

Editorial Notes:

E24 A class A fine is defined as a fine not exceeding €5,000 (4.01.2011) by *Fines Act 2010* (8/2010), s. 3, S.I. No. 662 of 2010.

F51**[**Enhanced customer due diligence - high-risk third countries

38A. (1) Subject to *subsection (2)*, a designated person shall apply measures, including enhanced monitoring of the business relationship, to manage and mitigate the risk of money laundering and terrorist financing, additional to those specified in this Chapter, when dealing with a customer established or residing in a high-risk third country.

(2) *Subsection (1)* shall not apply where—

(*a*) the customer is a branch or majority-owned subsidiary of a designated person and is located in a high-risk third country,

(*b*) the designated person referred to in paragraph (a) is established in a Member State, and

(*c*) the branch or majority-owned subsidiary referred to in *paragraph (a)* is in compliance with the group-wide policies and procedures of the group of which it is a member adopted in accordance with Article 45 of the Fourth Money Laundering Directive.

(3) In the circumstances specified in *subsection (2)*, the designated person shall—

(*a*) identify and assess the risk of money laundering or terrorist financing in relation to the business relationship or transaction concerned, having regard to *section 30B*, and

(*b*) apply customer due diligence measures specified in this Chapter to the extent reasonably warranted by the risk of money laundering or terrorist financing.

(4) A designated person who fails to comply with this section commits an offence and is liable—

(*a*) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).**]**

Annotations

Amendments:

F51 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 18, S.I. No. 486 of 2018.

Editorial Notes:

E25 A class A fine is defined as a fine not exceeding €5,000 (4.01.2011) by *Fines Act 2010* (8/2010), s. 3, S.I. No. 662 of 2010.

E26 The section heading is taken from the amending section in the absence of one included in the amendment.

F52**[**Enhanced due diligence in cases of heightened risk

F53**[39.** (1) Without prejudice to *sections 37*, *38* and *59*, a designated person shall apply measures to manage and mitigate the risk of money laundering or terrorist financing, additional to those specified in this Chapter, to a business relationship or transaction that presents a higher degree of risk.

(2) For the purposes of *subsection (1)* a business relationship or transaction shall be considered to present a higher degree of risk if a reasonable person having regard to the matters specified in *paragraphs (a)* to *(f)* of *section 30B(1)* would determine that the business relationship or transaction presents a higher risk of money laundering or terrorist financing.

(3) The Minister may prescribe other factors, additional to those specified in *Schedule 4*, suggesting potentially higher risk only if he or she is satisfied that the presence of those factors suggests a potentially higher risk of money laundering or terrorist financing.

(4) A designated person who fails to comply with this section commits an offence and is liable—

(*a*) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).**]]**

Annotations

Amendments:

F52 Substituted (14.06.2013) by *Criminal Justice Act 2013* (19/2013), s. 10, S.I. No. 196 of 2013.

F53 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 19, S.I. No. 486 of 2018.

Editorial Notes:

E27 A class A fine is defined as a fine not exceeding €5,000 (4.01.2011) by *Fines Act 2010* (8/2010), s. 3, S.I. No. 662 of 2010.

Reliance on other persons to carry out customer due diligence.

40.— (1) In this section, "relevant third party" means—

(*a*) a person, carrying on business as a designated person in the State—

(i) that is a credit institution,

(ii) that is a financial institution (other than an undertaking that is a financial institution solely because the undertaking provides either foreign exchange services or payment services, or both),

(iii) who is an external accountant or auditor and who is also a member of a designated accountancy body,

(iv) who is a tax adviser, and who is also a solicitor or a member of a designated accountancy body or of the Irish Taxation Institute,

(v) who is a relevant independent legal professional, or

(vi) who is a trust or company service provider, and who is also a member of a designated accountancy body, a solicitor or authorised to carry on business by the F54**[**Central Bank of Ireland**]**,

(*b*) a person carrying on business in another Member State who is supervised or monitored for compliance with the requirements specified in F55**[**the Fourth Money Laundering Directive, in accordance with Section 2 of Chapter VI of that Directive**]** and is—

(i) a credit institution authorised to operate as a credit institution under the laws of the Member State,

(ii) a financial institution (other than an undertaking that is a financial institution solely because the undertaking provides either foreign exchange services or payment services, or both) and authorised to operate as a financial institution under the laws of the Member State, or

(iii) an external accountant, auditor, tax adviser, legal professional or trust or company service provider subject to mandatory professional registration or mandatory professional supervision under the laws of the other Member State,

F56**[**...**]**

(*c*) a person who carries on business in F55**[**a place (other than a Member State) which is not a high-risk third country**]**, is supervised or monitored in the place

for compliance with requirements equivalent to those specified in F55**[**the Fourth Money Laundering Directive**]**, and is—

(i) a credit institution authorised to operate as a credit institution under the laws of the place,

(ii) a financial institution (other than an undertaking that is a financial institution solely because the undertaking provides either foreign exchange services or payment services, or both) authorised to operate as a financial institution under the laws of the place, or

(iii) an external accountant, auditor, tax adviser, legal professional or trust or company service provider subject to mandatory professional registration or mandatory professional supervision under the laws of F55**[**the place, or**]**

F57**[**(*d*) a person who carries on business in a high-risk third country, is a branch or majority-owned subsidiary of an obliged entity established in the Union, and fully complies with group-wide policies and procedures in accordance with Article 45 of the Fourth Money Laundering Directive and is—

(i) a credit institution authorised to operate as a credit institution under the laws of the place,

(ii) a financial institution (other than an undertaking that is a financial institution solely because the undertaking provides either foreign exchange services or payment services, or both) authorised to operate as a financial institution under the laws of the place, or

(iii) an external accountant, auditor, tax adviser, legal professional or trust or company service provider subject to mandatory professional registration or mandatory professional supervision under the laws of the place.**]**

F57**[**(1A) Without prejudice to the generality of *paragraphs (b)* and *(c)* of *subsection (1)*, for the purposes of those paragraphs, a person is supervised or monitored for compliance with the requirements specified in the Fourth Money Laundering Directive, in accordance with Section 2 of Chapter VI, or requirements equivalent to those requirements, where—

(*a*) the person and the designated person seeking to rely upon this section are part of the same group,

(*b*) the group applies customer due diligence and record keeping measures and policies and procedures to prevent and detect the commission of money laundering and terrorist financing in accordance with the Fourth Money Laundering Directive or requirements equivalent to those specified in the Fourth Money Laundering Directive, and

(*c*) the effective implementation of the requirements referred to in *paragraph (b)* is supervised at group level by a competent authority of the state where the parent company is incorporated.**]**

(2) A reference in *subsection (1)(b)(iii)* and *(c)(iii)* to a legal professional is a reference to a person who, by way of business, provides legal or notarial services.

(3) Subject to *subsections (4)* and *(5)*, a designated person may rely on a relevant third party to apply, in relation to a customer of the designated person, any of the measures that the designated person is required to apply, in relation to the customer, under *section 33* or *35(1)*.

(4) A designated person may rely on a relevant third party to apply a measure under *section 33* or *35(1)* only if—

(*a*) there is an arrangement between the designated person (or, in the case of a designated person who is an employee, the designated person's employer) and the relevant third party under which it has been agreed that the designated person may rely on the relevant third party to apply any such measure, and

(*b*) F55[the designated person is satisfied that the circumstances specified in *paragraphs (a)* to *(c)* of *subsection (1A)* exist, or] on the basis of the arrangement, that the relevant third party will forward to the designated person, as soon as practicable after a request from the designated person, any documents (whether or not in electronic form) or information relating to the customer that has been obtained by the relevant third party in applying the measure.

(5) A designated person who relies on a relevant third party to apply a measure under *section 33* or *35(1)* remains liable, under *section 33* or *35(1)*, for any failure to apply the measure.

(6) A reference in this section to a relevant third party on whom a designated person may rely to apply a measure under *section 33* or *35(1)* does not include a reference to a person who applies the measure as an outsourcing service provider or an agent of the designated person.

(7) Nothing in this section prevents a designated person applying a measure under *section 33* or *35(1)* by means of an outsourcing service provider or agent provided that the designated person remains liable for any failure to apply the measure.

Annotations

Amendments:

F54 Substituted (1.10.2010) by *Central Bank Reform Act 2010* (23/2010), s. 15(14) and sch. 2 part 14 par. 33, S.I. No. 469 of 2010.

F55 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 20(a)(i), (iii), (c), S.I. No. 486 of 2018.

F56 Deleted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 20(a)(ii), S.I. No. 486 of 2018.

F57 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 20(a)(iv), (b), S.I. No. 486 of 2018.

F58[Chapter 3A

Financial Intelligence Unit]

Annotations

Amendments:

F58 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 21, S.I. No. 486 of 2018. The chapter heading is taken from the chapter contents in the absence of a heading included in the amendment.

F59[State Financial Intelligence Unit

40A. (1) FIU Ireland may carry out, on behalf of the State, all the functions of an EU Financial Intelligence Unit (FIU) under the Fourth Money Laundering Directive.

(2) In this Part 'FIU Ireland' means those members of the Garda Síochána, or members of the civilian staff of the Garda Síochána, appointed by the Commissioner of the Garda Síochána in that behalf.**]**

Annotations

Amendments:

F59 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 21, S.I. No. 486 of 2018.

F60**[**Powers of FIU Ireland to receive and analyse information

40B. (1) FIU Ireland shall be responsible for receiving and analysing suspicious transaction reports and other information relevant to money laundering or terrorist financing for the purpose of preventing, detecting and investigating possible money laundering or terrorist financing.

(2) FIU Ireland's analysis function shall consist of conducting—

(*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.**]**

Annotations

Amendments:

F60 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 21, S.I. No. 486 of 2018.

F61**[**Powers of certain members of FIU Ireland to obtain information

40C. (1) A member of the Garda Síochána who is a member of FIU Ireland shall have access to the central registers established by the State for the purposes of paragraph (3) of Article 30 and paragraph (4) of Article 31 of the Fourth Money Laundering Directive.

(2) A member of the Garda Síochána who is a member of FIU Ireland may, for the purposes of preventing, detecting, investigating or combating money laundering or terrorist financing request any person to provide FIU Ireland with information held by that person under any enactment giving effect to paragraph (1) of Article 30 or paragraph (1) of Article 31 of the Fourth Money Laundering Directive.

(3) A member of the Garda Síochána who is a member of FIU Ireland may make a request in writing for any financial, administrative or law enforcement information that FIU Ireland requires in order to carry out its functions from any of the following:

(*a*) a designated person;

(*b*) a competent authority;

(*c*) the Revenue Commissioners;

(*d*) the Minister for Employment Affairs and Social Protection.

(4) A designated person who, without reasonable excuse, fails to comply with a request for information under *subsection (2)* or *(3)* commits an offence and is liable—

(*a*) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment to a fine not exceeding €500,000 or imprisonment not exceeding 3 years (or both).**]**

Annotations

Amendments:

F61 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 21, S.I. No. 486 of 2018.

Editorial Notes:

E28 A class A fine is defined as a fine not exceeding €5,000 (4.01.2011) by *Fines Act 2010* (8/2010), s. 3, S.I. No. 662 of 2010.

F62**[**Power of FIU Ireland to respond to requests for information from competent authorities

40D. (1) FIU Ireland shall respond as soon as practicable to any request for information which is based on a concern relating to money laundering or terrorist financing that it receives from—

(*a*) a competent authority,

(*b*) the Revenue Commissioners, or

(*c*) the Minister for Employment Affairs and Social Protection.

(2) FIU Ireland may provide the results of its analyses and any additional relevant information to a person mentioned in *subsection (1)* where there are grounds to suspect money laundering or terrorist financing.

(3) FIU Ireland shall be under no obligation to comply with the request for information 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.**]**

Annotations

Amendments:

F62 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 21, S.I. No. 486 of 2018.

F63**[**Power of FIU Ireland to share information

40E. (1) FIU Ireland may share information with other Financial Intelligence Units (FIUs), in accordance with subsection III of Section 3 of Chapter VI of the Fourth Money Laundering Directive.

(2) FIU Ireland may provide any information obtained by it—

(a) from a central register referred to in *section 40C(1)*, or

(b) following a request under *subsection (2)* or *(3)* of *section 40C*,

to a competent authority or to another FIU.**]**

Annotations

Amendments:

F63 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 21, S.I. No. 486 of 2018.

Chapter 4

Reporting of suspicious transactions and of transactions involving certain places

Interpretation (*Chapter 4*).

41.— In this Chapter, a reference to a designated person includes a reference to any person acting, or purporting to act, on behalf of the designated person, including any agent, employee, partner, director or other officer of, or any person engaged under a contract for services with, the designated person.

Requirement for designated persons and related persons to report suspicious transactions.

42.— (1) A designated person who knows, suspects or has reasonable grounds to suspect, on the basis of information obtained in the course of carrying on business as a designated person, that another person has been or is engaged in an offence of money laundering or terrorist financing shall report to F64**[**FIU Ireland**]** and the Revenue Commissioners that knowledge or suspicion or those reasonable grounds.

(2) The designated person shall make the report as soon as practicable after acquiring that knowledge or forming that suspicion, or acquiring those reasonable grounds to suspect, that the other person has been or is engaged in money laundering or terrorist financing.

(3) For the purposes of *subsections (1)* and *(2)*, a designated person is taken not to have reasonable grounds to know or suspect that another person commits an offence on the basis of having received information until the person has scrutinised the information in the course of reasonable business practice (including automated banking transactions).

(4) For the purposes of *subsections (1)* and *(2)*, a designated person may have reasonable grounds to suspect that another person has been or is engaged in an offence of money laundering or terrorist financing if the designated person is unable to apply any measures specified in *section 33(2)* or *(4)*, *35(1)* or *37(1)*, *(3)*, *(4)* or *(6),* in relation to a customer, as a result of any failure on the part of the customer to provide the designated person with documents or information.

(5) Nothing in *subsection (4)* limits the circumstances in which a designated person may have reasonable grounds, on the basis of information obtained in the course of carrying out business as a designated person, to suspect that another person has committed an offence of money laundering or terrorist financing.

(6) A designated person who is required to report under this section shall disclose the following information in the report:

(*a*) the information on which the designated person's knowledge, suspicion or reasonable grounds are based;

(*b*) the identity, if the designated person knows it, of the person who the designated person knows, suspects or has reasonable grounds to suspect has been or is engaged in an offence of money laundering or terrorist financing;

(*c*) the whereabouts, if the designated person knows them, of the property the subject of the money laundering, or the funds the subject of the terrorist financing, as the case may be;

(*d*) any other relevant information.

F65**[**(6A) A designated person who is required to make a report under this section shall respond to any request for additional information by FIU Ireland or the Revenue Commissioners as soon as practicable after receiving the request and shall take all reasonable steps to provide any information specified in the request.**]**

(7) A designated person who is required to make a report under this section shall not proceed with any suspicious transaction or service connected with the report, or with a transaction or service the subject of the report, prior to the sending of the report to F64**[**FIU Ireland**]** and the Revenue Commissioners unless—

(*a*) it is not practicable to delay or stop the transaction or service from proceeding, or

(*b*) the designated person is of the reasonable opinion that failure to proceed with the transaction or service may result in the other person suspecting that a report may be (or may have been) made or that an investigation may be commenced or in the course of being conducted.

(8) Nothing in *subsection (7)* authorises a designated person to proceed with a service or transaction if the person has been directed or ordered not to proceed with the service or transaction under *section 17* and the direction or order is in force.

(9) Except as provided by *section 46*, a person who fails to comply with this section commits an offence and is liable—

(*a*) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).

(10) A reference in *subsection (7)* to a suspicious transaction or service is a reference to a transaction or service that there are reasonable grounds for suspecting would, if it were to proceed—

(*a*) comprise money laundering or terrorist financing, or

(*b*) assist in money laundering or terrorist financing.

Annotations

Amendments:

F64 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 22(a), (b), S.I. No. 486 of 2018.

F65 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 22(c), S.I. No. 486 of 2018.

Requirement for designated persons to report transactions connected with places designated under *section 32*.

43.—F66**[**...**]**

Annotations

Amendments:

F66 Repealed (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 40(b), S.I. No. 486 of 2018.

Defence — internal reporting procedures.

44.— (1) Without prejudice to the way in which a report may be made under *section 42* F67**[**...**]**, such a report may be made in accordance with an internal reporting procedure established by an employer for the purpose of facilitating the operation of the section concerned.

(2) It is a defence for a person charged with an offence under *section 42* F67**[**...**]** to prove that the person was, at the time of the purported offence, an employee who made a report under that section, in accordance with such an internal reporting procedure, to another person.

Annotations

Amendments:

F67 Deleted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 23, S.I. No. 486 of 2018.

Use of reported and other information in investigations.

45.— (1) Information included in a report under this Chapter may be used in an investigation into money laundering or terrorist financing or any other offence.

(2) Nothing in this section limits the information that may be used in an investigation into any offence.

Disclosure not required in certain circumstances.

46.— (1) Nothing in this Chapter requires the disclosure of information that is subject to legal privilege.

(2) Nothing in this Chapter requires a relevant professional adviser to disclose information that he or she has received from or obtained in relation to a client in the course of ascertaining the legal position of the client.

(3) *Subsection (2)* does not apply to information received from or obtained in relation to a client with the intention of furthering a criminal purpose.

Disclosure not to be treated as breach.

47.— The disclosure of information by a person in accordance with this Chapter shall not be treated, for any purpose, as a breach of any restriction imposed by any other enactment or rule of law on disclosure by the person or any other person on whose behalf the disclosure is made.

Chapter 5

Tipping off by designated persons

Interpretation (*Chapter 5*).

48.— In this Chapter, "legal adviser" means a barrister or solicitor.

Tipping off.

49.— (1) A designated person who knows or suspects, on the basis of information obtained in the course of carrying on business as a designated person, that a report

has been, or is required to be, made under *Chapter 4* shall not make any disclosure that is likely to prejudice an investigation that may be conducted following the making of the report under that Chapter.

(2) A designated person who knows or suspects, on the basis of information obtained by the person in the course of carrying on business as a designated person, that an investigation is being contemplated or is being carried out into whether an offence of money laundering or terrorist financing has been committed, shall not make any disclosure that is likely to prejudice the investigation.

(3) A person who fails to comply with this section commits an offence and is liable—

(*a*) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).

(4) In this section, a reference to a designated person includes a reference to any person acting, or purporting to act, on behalf of the designated person, including any agent, employee, partner, director or other officer of, or any person engaged under a contract for services with, the designated person.

Defence — disclosure to customer in case of direction or order to suspend service or transaction.

50.— It is a defence in any proceedings against a person ("the defendant") for an offence under *section 49*, in relation to a disclosure, for the defendant to prove that—

(*a*) the disclosure was to a person who, at the time of the disclosure, was a customer of the defendant or of a designated person on whose behalf the defendant made the disclosure,

(*b*) the defendant, or the designated person on whose behalf the defendant made the disclosure, was directed or ordered under *section 17* not to carry out any specified service or transaction in respect of the customer, and

(*c*) the disclosure was solely to the effect that the defendant, or a designated person on whose behalf the defendant made the disclosure, had been directed by a member of the Garda Síochána, or ordered by a judge of the District Court, under *section 17* not to carry out the service or transaction for the period specified in the direction or order.

Defences — disclosures within undertaking or group.

51.— (1) It is a defence in any proceedings against an individual for an offence under *section 49*, in relation to a disclosure, for the individual to prove that, at the time of the disclosure—

(*a*) he or she was an agent, employee, partner, director or other officer of, or was engaged under a contract for services by, an undertaking, and

(*b*) he or she made the disclosure to an agent, employee, partner, director or other officer of, or a person engaged under a contract for services by, the same undertaking.

F68**[**(2) It is a defence in any proceedings against a person for an offence under section 49, in relation to a disclosure, for the person to prove that, at the time of the disclosure—

(*a*) the person was a credit institution or financial institution or a majority-owned subsidiary, or a branch, of a credit institution or financial institution, or made the disclosure on behalf of a credit institution or a financial institution or a majority-owned subsidiary, or a branch, of a credit institution or financial institution,

(*b*) the disclosure was to a credit institution or a financial institution or a majority-owned subsidiary, or a branch, of a credit institution or financial institution,

(*c*) the institution to which the disclosure was made was situated in a Member State or a country other than a high-risk third country,

(*d*) both the institution making the disclosure, or on whose behalf the disclosure was made, and the institution to which it was made belonged to the same group, and

(*e*) both the institutions referred to in *paragraph (d)* were in compliance with group-wide policies and procedures adopted in accordance with *section 54* or, as the case may be, Article 45 of the Fourth Money Laundering Directive.**]**

(3) It is a defence in any proceedings against a person for an offence under *section 49*, in relation to a disclosure, for the person to prove that, at the time of the disclosure—

(*a*) the person was a legal adviser or relevant professional adviser,

(*b*) both the person making the disclosure and the person to whom it was made carried on business in a Member State F68**[**or in a country other than a high-risk third country**]**, and

(*c*) those persons performed their professional activities within different undertakings that shared common ownership, management or control.

Annotations

Amendments:

F68 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 24(a), (b), S.I. No. 486 of 2018.

Defences — other disclosures between institutions or professionals.

52.— (1) This section applies to a disclosure—

(*a*) by or on behalf of a credit institution to another credit institution,

(*b*) by or on behalf of a financial institution to another financial institution,

(*c*) by or on behalf of a legal adviser to another legal adviser, or

(*d*) by or on behalf of a relevant professional adviser of a particular kind to another relevant professional adviser of the same kind.

(2) It is a defence in any proceedings against a person for an offence under *section 49*, in relation to a disclosure to which this section applies, for the person to prove that, at the time of the disclosure—

(*a*) the disclosure related to—

(i) a customer or former customer of the person (or an institution or adviser on whose behalf the person made the disclosure) and the institution or adviser to which or whom it was made, or

(ii) a transaction, or the provision of a service, involving both the person (or an institution or adviser on whose behalf the person made the disclosure) and the institution or adviser to which or whom it was made,

(*b*) the disclosure was only for the purpose of preventing money laundering or terrorist financing,

(*c*) the institution or adviser to which or whom the disclosure was made was situated in a Member State or in F69**[**a country other than a high-risk third country**]**, and

(*d*) the institution or adviser making the disclosure, or on whose behalf the disclosure was made, and the institution or adviser to which or whom it was made were subject to equivalent duties of professional confidentiality and the protection of personal data F70**[**...**]**.

(3) A reference in this section to a customer of an adviser includes, in the case of an adviser who is a barrister, a reference to a person who is a client of a solicitor who has sought advice from the barrister for or on behalf of the client.

Annotations

Amendments:

F69 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 25, S.I. No. 486 of 2018.

F70 Deleted (25.05.2018) by *Data Protection Act 2018* (7/2018), s. 213(b), S.I. No. 174 of 2018.

Defences — other disclosures.

53.— (1) It is a defence in any proceedings against a person for an offence under *section 49*, in relation to a disclosure, for the person to prove that—

(*a*) the disclosure was to the authority that, at the time of the disclosure, was the competent authority responsible for monitoring that person, or for monitoring the person on whose behalf the disclosure was made, under this Part,

(*b*) the disclosure was for the purpose of the detection, investigation or prosecution of an offence (whether or not in the State), or

(*c*) the person did not know or suspect, at the time of the disclosure, that the disclosure was likely to have the effect of prejudicing an investigation into whether an offence of money laundering or terrorist financing had been committed.

(2) It is a defence in any proceedings against a person for an offence under *section 49*, in relation to a disclosure, for the person to prove that—

(*a*) at the time of the disclosure, the person was a legal adviser or relevant professional adviser,

(*b*) the disclosure was to the person's client and solely to the effect that the person would no longer provide the particular service concerned to the client,

(*c*) the person no longer provided the particular service after so informing the client, and

(*d*) the person made any report required in relation to the client in accordance with *Chapter 4*.

Chapter 6

Internal policies and procedures, training and record keeping

Internal policies and procedures and training.

F71**[54.** (1) A designated person shall adopt internal policies, controls and procedures in relation to the designated person's business to prevent and detect the commission of money laundering and terrorist financing.

(2) In particular, a designated person shall adopt internal policies, controls and procedures to be followed by any persons involved in carrying out the obligations of the designated person under this Part.

(3) The internal policies, controls and procedures referred to in *subsection (1)* shall include policies, controls and procedures dealing with—

(*a*) the identification, assessment, mitigation and management of risk factors relating to money laundering or terrorist financing,

(*b*) customer due diligence measures,

(*c*) monitoring transactions and business relationships,

(*d*) the identification and scrutiny of complex or large transactions, unusual patterns of transactions that have no apparent economic or visible lawful purpose and any other activity that the designated person has reasonable grounds to regard as particularly likely, by its nature to be related to money laundering or terrorist financing,

(*e*) measures to be taken to prevent the use for money laundering or terrorist financing of transactions or products that could favour or facilitate anonymity,

(*f*) measures to be taken to prevent the risk of money laundering or terrorist financing which may arise from technological developments including the use of new products and new practices and the manner in which services relating to such developments are delivered,

(*g*) reporting (including the reporting of suspicious transactions),

(*h*) record keeping,

(*i*) measures to be taken to keep documents and information relating to the customers of that designated person up to date,

(*j*) measures to be taken to keep documents and information relating to risk assessments by that designated person up to date,

(*k*) internal systems and controls to identify emerging risks and keep business-wide risk assessments up to date, and

(*l*) monitoring and managing compliance with, and the internal communication of, these policies, controls and procedures.

(4) A designated person shall ensure that policies, controls and procedures adopted in accordance with this section are approved by senior management and shall keep such policies, controls and procedures under review, in particular when there are changes to the business profile or risk profile of the designated person.

(5) In preparing internal policies, controls and procedures under this section, the designated person shall have regard to any guidelines on preparing, implementing and reviewing such policies and procedures that are issued by the competent authority for that designated person.

(6) A designated person shall ensure that persons involved in the conduct of the designated person's business are—

(*a*) instructed on the law relating to money laundering and terrorist financing, and

(*b*) provided with ongoing training on identifying a transaction or other activity that may be related to money laundering or terrorist financing, and on how to proceed once such a transaction or activity is identified.

(7) A designated person shall appoint an individual at management level, (to be called a 'compliance officer') to monitor and manage compliance with, and the internal communication of, internal policies, controls and procedures adopted by the designated person under this section if directed in writing to do so by the competent authority for that designated person.

(8) A designated person shall appoint a member of senior management with primary responsibility for the implementation and management of anti-money laundering measures in accordance with this Part if directed in writing to do so by the competent authority for that designated person.

(9) A designated person shall undertake an independent, external audit to test the effectiveness of the internal policies, controls and procedures outlined in this section if directed in writing to do so by the competent authority for that designated person.

(10) A reference in this section to persons involved in carrying out the obligations of the designated person under this Part includes a reference to directors and other officers, and employees, of the designated person.

(11) The obligations imposed on a designated person under this section do not apply to a designated person who is an employee of another designated person.

(12) *Subsections (6)*, *(7)*, *(8)*, and *(9)* do not apply to a designated person who is an individual and carries on business alone as a designated person.

(13) A competent authority shall not issue a direction for the purposes of *subsection (7)*, *(8)* or *(9)* unless it is satisfied that, having regard to the size and nature of the designated person, it is appropriate to do so.

(14) A competent authority may make a direction to a class of designated persons for whom it is the competent authority for the purposes of *subsection (7)*, *(8)* or *(9)*.

(15) A designated person who fails to comply with this section commits an offence and is liable—

(*a*) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).**]**

Annotations

Amendments:

F71 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 26, S.I. No. 486 of 2018.

Editorial Notes:

E29 A class A fine is defined as a fine not exceeding €5,000 (4.01.2011) by *Fines Act 2010* (8/2010), s. 3, S.I. No. 662 of 2010.

E30 Previous affecting provision: section amended (14.06.2013) by *Criminal Justice Act 2013* (19/2013), s. 11(a), (b), (c), S.I. 196 of 2013; section substituted as per F-note above.

Keeping of records by designated persons.

55.— (1) A designated person shall keep records evidencing the procedures applied, and information obtained, by the designated person under *Chapter 3* in relation to—

(*a*) each customer, and

(*b*) in the case of a designated person to whom *section 38* applies, each F72**[**correspondent relationship**]**.

(2) Without prejudice to the generality of *subsection (1)*, a designated person shall take the original or a copy of all documents used by the designated person for the purposes of *Chapter 3*, including all documents used to verify the identity of customers or beneficial owners in accordance with *section 33*.

(3) A designated person shall keep records evidencing the history of services and transactions carried out in relation to each customer of the designated person.

(4) F72**[**Subject to *subsections (4A)*, *(4B)* and *(4C)*, the documents and other records**]** referred to in *subsections (1)* to *(3)* F73**[**shall be retained by the designated person**]** for a period of not less than 5 years after—

(*a*) in the case of a record referred to in *subsection (1)(a)*, the date on which the designated person ceases to provide any service to the customer concerned or the date of the last transaction (if any) with the customer, whichever is the later,

(*b*) in the case of a record referred to in *subsection (1) (b)*, the date on which the F72**[**correspondent relationship**]** concerned ends,

(*c*) in the case of a record referred to in *subsection (3)* evidencing the carrying out of a particular transaction by the designated person with, for or on behalf of the customer (other than a record to which *paragraph (d)* applies), the date on which the particular transaction is completed or discontinued,

(*d*) in the case of a record referred to in *subsection (3)* evidencing the carrying out of a particular occasional transaction comprised of a series of transactions, with, for or on behalf of a customer, the date on which the series of transactions is completed or discontinued, or

(*e*) in the case of a record referred to in *subsection (3)* evidencing the carrying out of a particular service for or on behalf of the customer (other than a record to which *paragraph (c)* or *(d)* applies), the date on which the particular service is completed or discontinued.

F74**[**(4A) Where a member of the Garda Síochána not below the rank of Sergeant having carried out a thorough assessment of the necessity and proportionality of further retention is satisfied—

(*a*) that certain documents or records, or documents or records relating to a certain business relationship or occasional transaction, are required for the purposes of an investigation related to money laundering or terrorist financing, or

(*b*) notwithstanding the fact that a decision to institute proceedings against a person may not have been taken, that the documents or records are likely to be required for the prosecution of an offence of money laundering or terrorist financing,

the member may give a direction in writing to a designated person to retain the documents and other records for a period, up to a maximum of 5 years, additional to the period referred to in *subsection (4)*.

(4B) Where a direction has been given to a designated person in accordance with *subsection (4A)* and neither *paragraph (a)* nor *(b)* of that subsection continue to apply a member of the Garda Síochána shall, as soon as practicable, notify the designated person to whom the direction was given of that fact and the direction shall expire on the date of that notification.

(4C) A designated person who is given a direction under *subsection (4A)* shall retain the documents or records specified in the direction until the earlier of—

(*a*) the expiration of the additional period specified in the direction, and

(*b*) the expiration of the direction.**]**

(5) *Subsection (4)(a)* extends to any record that was required to be retained under section 32(9)(*a*) of the Act of 1994 immediately before the repeal of that provision by this Act.

(6) *Subsection (4)(c)* to *(e)* extends to any record that was required to be retained under section 32(9)(*b*) of the Criminal Justice Act 1994 immediately before the repeal of that provision by this Act and for that purpose—

(*a*) a reference in *subsection (4)(c)* to *(e)* to a record referred to in *subsection (3)* includes a reference to such a record, and

(*b*) a reference in *subsection (4)(d)* to an occasional transaction comprised of a series of transactions includes a reference to a series of transactions referred to in section 32(3)(*b*) of the Criminal Justice Act 1994.

(7) A designated person may keep the records referred to in *subsections (1)* to *(6)* wholly or partly in an electronic, mechanical or other non-written form only if they are capable of being reproduced in a written form.

F75**[**(7A) The records required to be kept by a designated person under this section may be kept outside the State provided that the designated person ensures that those records are produced in the State to—

(a) a member of the Garda Síochána,

(b) an authorised officer appointed under section 72,

(c) a relevant authorised officer within the meaning of section 103, or

(d) a person to whom the designated person is required to produce such records in relation to his or her business, trade or profession,

as soon as practicable after the records concerned are requested, or where the obligation to produce the records arises under an order of a court made under section 63 of the Criminal Justice Act 1994, within the period which applies to such production under the court order concerned.**]**

F74**[**(7B) Upon the expiry of the retention periods referred to in this section a designated person shall ensure that any personal data contained in any document or other record retained solely for the purposes of this section is deleted.**]**

(8) The requirements imposed by this section are in addition to, and not in substitution for, any other requirements imposed by any other enactment or rule of law with respect to the keeping and retention of records by a designated person.

(9) The obligations that are imposed on a designated person under this section continue to apply to a person who has been a designated person, but has ceased to carry on business as a designated person.

(10) A requirement for a designated person that is a body corporate to retain any record under this section extends to any body corporate that is a successor to, or a continuation of, the body corporate.

(11) The Minister may make regulations prescribing requirements relating to the retention of records referred to in this section of a body corporate that is wound up or a partnership that is dissolved.

(12) A designated person who fails to comply with this section commits an offence and is liable—

(*a*) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).

Annotations

Amendments:

F72 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 27(a), (b), (c), S.I. No. 486 of 2018.

F73 Substituted (14.06.2013) by *Criminal Justice Act 2013* (19/2013), s. 12(a), S.I. No. 196 of 2013.

F74 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 27(d), (e), S.I. No. 486 of 2018.

F75 Inserted (14.06.2013) by *Criminal Justice Act 2013* (19/2013), s. 12(b), S.I. No. 196 of 2013.

Chapter 7

Special provisions applying to credit and financial institutions

Measures for retrieval of information relating to business relationships.

56.—(1) A F76**[**...**]** designated person shall have systems in place to enable it to respond fully and promptly to enquiries from the Garda Síochána—

(*a*) as to whether or not it has, or has had, a business relationship, within the previous F77**[**5 years**]**, with a person specified by the Garda Síochána, and

(*b*) the nature of any such relationship with that person.

(2) F77**[**A designated person who**]** fails to comply with this section commits an offence and is liable—

(*a*) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).

Annotations

Amendments:

F76 Deleted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 28(a), S.I. No. 486 of 2018.

F77 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 28(b), (c), S.I. No. 486 of 2018.

F78**[**Group-wide policies and procedures

57. (1) A designated person that is part of a group shall implement group-wide policies and procedures, including data protection policies and policies and procedures for sharing information within the group, for the purposes of carrying out customer due diligence and preventing and detecting the commission of money laundering and terrorist financing.

(2) A designated person incorporated in the State that operates a branch, majority-owned subsidiary or establishment in a place other than the State shall ensure that the branch, majority-owned subsidiary or establishment adopts and applies group-wide policies and procedures referred to in *subsection (1)*.

(3) Where a place referred to in *subsection (2)*, other than a Member State, is a place that does not permit the implementation of the policies and procedures required under *subsection (1)* the designated person shall—

(*a*) ensure that each of its branches and majority-owned subsidiaries in that place applies additional measures to effectively handle the risk of money laundering or terrorist financing, and

(*b*) notify the competent authority for that designated person of the additional measures applied under *paragraph (a)*.

(4) A designated person incorporated in the State that operates a branch, majority-owned subsidiary or establishment in another Member State shall ensure that the branch, majority-owned subsidiary or establishment complies with the requirements of the Fourth Money Laundering Directive as they apply in that Member State.

(5) A designated person incorporated in the State that has a branch or majority-owned subsidiary located in a place, other than a Member State, in which the minimum requirements relating to the prevention and detection of money laundering and terrorist financing are less strict than those of the State shall ensure that the branch or majority-owned subsidiary implement the requirements of the State, including requirements relating to data protection, to the extent that the third country's law so allows.

(6) Subject to *section 49*, a designated person that is part of a group that makes a report under *section 42* shall share that report within the group for the purposes of preventing and detecting the commission of money laundering and terrorist financing unless otherwise instructed by FIU Ireland.

(7) A designated person that fails to comply with this section commits an offence and is liable—

(*a*) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).**]**

Annotations

Amendments:

F78 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 29, S.I. No. 486 of 2018.

Editorial Notes:

E31 A class A fine is defined as a fine not exceeding €5,000 (4.01.2011) by *Fines Act 2010* (8/2010), s. 3, S.I. No. 662 of 2010.

F79**[**Additional measures where implementation of policies and procedures is not possible

57A. (1) Where a competent authority receives a notification under *section 57(3)(b)* and is not satisfied that the additional measures applied in accordance with that subsection are sufficient for the purposes of carrying out customer due diligence and preventing and detecting the commission of money laundering and terrorist financing it shall exercise additional supervisory actions, where necessary requesting a group to close down its operations in the third country and may, by notice in writing, direct

the designated person to take such additional actions as the competent authority considers necessary to mitigate the risk of money laundering or terrorist financing.

(2) A notice under *subsection (1)*—

(*a*) may direct the group—

(i) not to establish a business relationship,

(ii) to terminate a business relationship, or

(iii) not to undertake a transaction,

and

(*b*) shall specify the matters which, in the opinion of the competent authority, give rise to the risk of money laundering or terrorist financing and in respect of which the additional measures taken are insufficient.

(3) A notice under *subsection (1)* shall take effect—

(*a*) where the notice so declares, immediately the notice is received by the person on whom it is served,

(*b*) in any other case—

(i) where no appeal is taken against the notice, on the expiration of the period during which such an appeal may be taken or the day specified in the notice as the day on which it is to come into effect, whichever is the later, or

(ii) in case such an appeal is taken, on the day next following the day on which the notice is confirmed on appeal or the appeal is withdrawn or the day specified in the notice as that on which it is to come into effect, whichever is the later.

(4) A designated person that is aggrieved by a notice may, within the period of 30 days beginning on the day on which the notice is served, appeal against the notice to the High Court and in determining the appeal the court may—

(*a*) if the court is satisfied that in the circumstances of the case it is reasonable to do so, confirm the notice, with or without modification, or

(*b*) cancel the notice.

(5) The bringing of an appeal against a notice which is to take effect in accordance with *subsection (3)(a)* shall not have the effect of suspending the operation of the notice, but the appellant may apply to the court to have the operation of the notice suspended until the appeal is disposed of and, on such application, the court may, if it thinks proper to do so, direct that the operation of the notice be suspended until the appeal is disposed of.

(6) Where on the hearing of an appeal under this section a notice is confirmed the High Court may, on the application of the appellant, suspend the operation of the notice for such period as in the circumstances of the case the High Court considers appropriate.

(7) A person who appeals under *subsection (4)* against a notice or who applies for a direction suspending the application of the notice under *subsection (6)* shall at the same time notify the competent authority concerned of the appeal or the application and the grounds for the appeal or the application and the competent authority shall be entitled to appear, be heard and adduce evidence on the hearing of the appeal or the application.

(8) A designated person that fails to comply with a direction made by the competent authority for that designated person under *subsection (1)* commits an offence and is liable—

(*a*) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).

(9) A competent authority may, by notice in writing to the designated person concerned, vary or revoke a notice under *subsection (1)*.**]**

Annotations

Amendments:

F79 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 30, S.I. No. 486 of 2018.

Editorial Notes:

E32 A class A fine is defined as a fine not exceeding €5,000 (4.01.2011) by *Fines Act 2010* (8/2010), s. 3, S.I. No. 662 of 2010.

E33 The section heading is taken from the amending section in the absence of one included in the amendment.

Anonymous accounts.

58.— (1) A credit institution or financial institution shall not set up an anonymous account for, or provide an anonymous passbook to, any customer.

(2) A credit institution or financial institution shall not keep any anonymous account, or anonymous passbook, that was in existence immediately before the commencement of this section for any customer.

(3) A credit institution or financial institution that fails to comply with this section commits an offence and is liable—

(*a*) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).

Relationships between credit institutions and shell banks.

F80**[59.** (1) A credit institution or financial institution shall not enter into a correspondent relationship with a shell bank.

(2) A credit institution or financial institution that has entered into a correspondent relationship with a shell bank before the commencement of this section shall not continue that relationship.

(3) A credit institution or financial institution shall not engage in or continue a correspondent relationship with a bank that the institution knows permits its accounts to be used by a shell bank.

(4) A credit institution or financial institution shall apply appropriate measures to ensure that it does not enter into or continue a correspondent relationship that permits its accounts to be used by a shell bank.

(5) A credit institution or financial institution that fails to comply with this section commits an offence and is liable—

(*a*) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).

(6) In this section, 'shell bank' means a credit institution or financial institution (or a body corporate that is engaged in activities equivalent to those of a credit institution or financial institution) that—

(*a*) does not have a physical presence, involving meaningful decision-making and management, in the jurisdiction in which it is incorporated,

(*b*) is not authorised to operate, and is not subject to supervision, as a credit institution, or as a financial institution, (or equivalent) in the jurisdiction in which it is incorporated, and

(*c*) is not affiliated with another body corporate that—

(i) has a physical presence, involving meaningful decision-making and management, in the jurisdiction in which it is incorporated, and

(ii) is authorised to operate, and is subject to supervision, as a credit institution, a financial institution or an insurance undertaking, in the jurisdiction in which it is incorporated.**]**

Annotations

Amendments:

F80 Substituted Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 31, S.I. No. 486 of 2018.

Editorial Notes:

E34 A class A fine is defined as a fine not exceeding €5,000 (4.01.2011) by *Fines Act 2010* (8/2010), s. 3, S.I. No. 662 of 2010.

Chapter 8

Monitoring of designated persons

Meaning of "competent authority".

60.— (1) Subject to *section 61*, a reference in this Part to the competent authority for a designated person is a reference to the competent authority prescribed for the class of designated persons to which the designated person belongs.

(2) If no such competent authority is prescribed, a reference in this Part to the competent authority is a reference to the following:

(*a*) in the case of a designated person that is a credit institution or a financial institution, the F81**[**Central Bank of Ireland**]**;

(*b*) in the case of a designated person who is an auditor, external accountant, tax adviser or trust or company service provider—

(i) if the person is a member of a designated accountancy body, the designated accountancy body, or

(ii) if the person is not a member of a designated accountancy body and is a body corporate, or a body of unincorporated persons, carrying out its

functions under this Part F82**[**through officers and members**]** of it who are members of a designated accountancy body, the designated accountancy body;

(*c*) in the case of a designated person who is a solicitor, the Law Society of Ireland;

(*d*) in the case of a designated person who is a barrister, the General Council of the Bar of Ireland;

(*e*) in the case of any designated person other than a designated person referred to in *paragraph (a)*, *(b)*, *(c)* or *(d)*, the Minister.

(3) The Minister may prescribe a competent authority for a class of designated persons, for the purpose of *subsection (1)*, only if the Minister is satisfied that the competent authority is more appropriate than the competent authority specified in *subsection (2)* for the class of designated persons, having regard to the nature of the business activities engaged in by that class.

Annotations

Amendments:

F81 Substituted (1.10.2010) by *Central Bank Reform Act 2010* (23/2010), s. 15(14) and sch. 2 part 14 par. 33, S.I. No. 469 of 2010.

F82 Substituted (14.06.2013) by *Criminal Justice Act 2013* (19/2013), s. 13, S.I. No. 196 of 2013.

F83 Inserted by *Legal Services Regulation Act 2015* (65/2015), s. 214, not commenced as of date of revision.

Modifications (not altering text):

C5 Prospective affecting provision: para. (d) amended and para. (da) inserted by *Legal Services Regulation Act 2015* (65/2015), s. 214, not commenced as of date of revision.

(*d*) in the case of a designated person who is a barrister F83**[**who is a member of the Law Library**]**, the General Council of the Bar of Ireland;

F83**[**(*da*) in the case of a designated person who is a barrister who is not a member of the Law Library, the Legal Services Regulatory Authority;**]**

Editorial Notes:

E35 Power pursuant to subs. (3) exercised (1.09.2016) by *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Competent Authority and State Competent Authority) Regulations 2016* (S.I. No. 453 of 2016), in effect as per reg. 2.

E36 Powers pursuant to subs. (3) exercised (3.03.2014) by *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Competent Authority) Regulations 2014* (S.I. No. 79 of 2014), in effect as per reg. 2.

Agreements between competent authorities where more than one applicable.

61.— (1) Where there is more than one competent authority for a designated person under *section 60*, those competent authorities may agree that one of them will act as the competent authority for that person, and references in this Part to a competent authority are to be construed accordingly.

(2) An agreement under this section, in relation to a designated person, takes effect when the competent authority who has agreed to act as the competent authority for the designated person gives notice, in writing, to that person.

(3) An agreement under this section, in relation to a designated person, ceases to have effect when—

(*a*) any of the parties to the agreement gives notice, in writing, to the other parties of the termination of the agreement,

(*b*) the agreement expires, or

(*c*) as a result of the operation of *section 60(1)*, the competent authority who has agreed to act as the competent authority is no longer a competent authority of the person under *section 60*,

whichever is the earliest.

Meaning of "State competent authority".

62.— (1) In this Part, a reference to a State competent authority is a reference to one of the following competent authorities:

(*a*) the F84**[**Central Bank of Ireland**]**;

(*b*) the Minister;

(*c*) such other competent authority as is prescribed.

(2) The Minister may prescribe a competent authority as a State competent authority for the purposes of *subsection (1) (c)* only if—

(*a*) the Minister is satisfied that the competent authority is appropriate, having regard to the functions of State competent authorities under this Part, and

(*b*) the competent authority is a Minister of the Government or an officer of a particular class or description of a Department of State or is a body (not being a company) by or under an enactment.

Annotations

Amendments:

F84 Substituted (1.10.2010) by *Central Bank Reform Act 2010* (23/2010), s. 15(14) and sch. 2 part 14 par. 33, S.I. No. 469 of 2010.

F85 Inserted by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 32, not commenced as of date of revision.

Modifications (not altering text):

C6 Prospective affecting provision: subs. (1)(aa) inserted by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 32, not commenced as of date of revision.

F85**[**(*aa*) the Legal Services Regulatory Authority;**]**

Editorial Notes:

E37 Power pursuant to subs. (2) exercised (1.09.2016) by *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Competent Authority and State Competent Authority) Regulations 2016* (S.I. No. 453 of 2016), in effect as per reg. 2.

General functions of competent authorities.

63.— (1) A competent authority shall effectively monitor the designated persons for whom it is a competent authority and take measures that are reasonably necessary for the purpose of securing compliance by those designated persons with the requirements specified in this Part.

(2) The measures that are reasonably necessary include reporting to the Garda Síochána and Revenue Commissioners any knowledge or suspicion that the competent

authority has that a designated person has been or is engaged in money laundering or terrorist financing.

(3) In determining, in any particular case, whether a designated person has complied with any of the requirements specified in this Part, a competent authority shall consider whether the person is able to demonstrate to the competent authority that the requirements have been met.

(4) A competent authority that, in the course of monitoring a designated person under this section, acquires any knowledge or forms any suspicion that another person has been or is engaged in money laundering or terrorist financing shall report that knowledge or suspicion to the Garda Síochána and Revenue Commissioners.

Application of other enactments.

64.— Nothing in this Part limits any functions that a competent authority (including a State competent authority) has under any other enactment or rule of law.

Annual reporting.

65.— A competent authority shall include, in each annual report published by the authority, an account of the activities that it has carried out in performing its functions under this Act during the year to which the annual report relates.

Request to bodies to provide names, addresses and other information relating to designated persons.

66.— (1) In this section, a reference to relevant information, in relation to a person, that is held by a body is a reference to any of the following information that is held by the body:

(*a*) the name, address or other contact details of the person;

(*b*) any other prescribed information relating to the person.

(2) A State competent authority may, by notice in writing, request any public body, or any body that represents, regulates or licenses, registers or otherwise authorises persons carrying on any trade, profession, business or employment, to provide the authority with any relevant information, in relation to—

(*a*) any designated persons for whom the authority is a competent authority, or

(*b*) any persons whom the body reasonably considers may be such designated persons.

(3) A State competent authority may make a request under this section only in relation to information that is reasonably required by the authority to assist the authority in carrying out its functions under this Part.

(4) Notwithstanding any other enactment or rule of law, a body that receives a request under this section shall disclose the relevant information concerned.

(5) The Minister may prescribe information, for the purposes of *subsection (1)(b)*, that a State competent authority may request under this section only if the Minister is satisfied that the information is appropriate, having regard to the functions of the State competent authority under this Part.

Direction to furnish information or documents.

67.— (1) A State competent authority may, by notice in writing, direct a designated person for whom the authority is a competent authority to provide such information or documents (or both) relating to the designated person specified in the notice.

(2) A person who, without reasonable excuse, fails to comply with a direction under this section commits an offence and is liable, on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both).

(3) In giving a direction under this section, a State competent authority shall specify the manner in which any document or information is required to be furnished and a reasonable time by which the document or information is required to be furnished.

(4) A person is required to furnish documents in accordance with this section only if the documents are in the person's possession or within the person's power to obtain lawfully.

(5) If a person knows the whereabouts of documents to which the direction applies, the person shall furnish to the State competent authority who gave the direction a statement, verified by a statutory declaration, identifying the whereabouts of the documents. The person shall furnish the statement no later than the time by which the direction specifies that the documents are required to be furnished.

(6) A person who, without reasonable excuse, fails to comply with *subsection (5)* commits an offence and is liable, on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both).

(7) If any document required to be furnished under this section is in electronic, mechanical or other form, the document shall be furnished in written form, unless the direction specifies otherwise.

(8) A State competent authority may take copies of, or extracts from, any document furnished to the authority under this section.

Direction to provide explanation of documents.

68.— (1) A State competent authority may, by notice in writing, direct a designated person for whom the authority is a competent authority to furnish to the authority an explanation of any documents relating to the designated person that—

(*a*) the person has furnished to the authority in complying with a direction under *section 67*, or

(*b*) an authorised officer has lawfully removed from premises under *section 77* (including as applied by *section 78*).

(2) In giving a direction under this section, a State competent authority shall specify the manner in which any explanation of a document is required to be furnished and a reasonable time by which the explanation is required to be furnished.

(3) A person who, without reasonable excuse, fails to comply with a direction under this section commits an offence and is liable, on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both).

Purpose of direction under *section 67* or *68*.

69.— A State competent authority may give a direction under *section 67* or *68* only in relation to information or documents reasonably required by the authority to assist the authority to perform its functions under this Part.

Self-incrimination (*sections 67* and *68*).

70.— Nothing in *section 67* or *68* requires a person to comply with a direction under the section concerned to furnish any information if to do so might tend to incriminate the person.

F86[Directions to comply with obligations under this Part.

71.— (1) A State competent authority may, by notice in writing, direct a designated person or a class of designated persons in respect of whom the authority is the competent authority to—

(a) discontinue, or refrain from engaging in, specified conduct that in the opinion of the authority concerned constitutes, or, if engaged in, would constitute, a breach of any specified provision of this Part, or

(b) take specific actions or to establish specific processes or procedures that in the opinion of the authority are reasonably necessary for the purposes of complying with any specified provision of this Part.

(2) The State competent authority shall specify in any such direction a reasonable period of time within which the person to whom it is given is required to comply with the direction.

(3) If a designated person to whom a direction has been issued under subsection (1) fails to comply with the direction and is subsequently found guilty of an offence—

(a) which consists of the conduct specified in the direction given under subsection (1)(a), or

(b) which would not have been committed if the direction under subsection (1)(b) had been complied with,

the court may take the failure to comply with the direction into account as an aggravating factor in determining any sentence to be imposed on the person for the offence.**]**

Annotations

Amendments:

F86 Substituted (14.06.2013) by *Criminal Justice Act 2013* (19/2013), s. 14, S.I. No. 196 of 2013.

Appointment of authorised officers.

72.— (1) A State competent authority may appoint employees of the authority or other persons who, in the opinion of the authority, are suitably qualified or experienced, to be authorised officers for the purpose of this Chapter.

(2) A State competent authority may revoke any appointment made by the authority under *subsection (1)*.

(3) An appointment or revocation under this section shall be in writing.

(4) A person's appointment by a State competent authority as an authorised officer ceases—

(*a*) on the revocation by the authority of the appointment,

(*b*) in a case where the appointment is for a specified period, on the expiration of the period,

(*c*) on the person's resignation from the appointment, or

(*d*) in a case where the person is an employee of the authority—

(i) on the resignation of the person as an employee of the authority, or

(ii) on the termination of the person's employment with the authority for any other reason.

Warrant of appointment.

73.— (1) Every authorised officer appointed by a State competent authority shall be furnished with a warrant of appointment as an authorised officer by the State competent authority.

(2) In the course of performing the functions of an authorised officer under this Chapter, the officer shall, if requested to do so by any person affected, produce the officer's warrant of appointment for inspection.

Powers may only be exercised for assisting State competent authority.

74.— An authorised officer may exercise powers as an authorised officer under this Chapter only for the purpose of assisting the State competent authority that appointed the authorised officer in the performance of the authority's functions under this Part.

General power of authorised officers to enter premises.

75.— (1) An authorised officer may enter any premises at which the authorised officer reasonably believes that the business of a designated person has been or is carried on.

(2) An authorised officer may enter any premises at which the authorised officer reasonably believes records or other documents relating to the business of a designated person are located.

(3) An authorised officer may enter premises under *subsection (1)* or *(2)*—

(*a*) in a case where the authorised officer reasonably believes that the business of a designated person is carried on at the premises (as referred to in *subsection (1)*), at any time during which the authorised officer reasonably believes that the business is being carried on there, or

(*b*) in any other case, at any reasonable time.

Entry into residential premises only with permission or warrant.

76.— Nothing in this Chapter shall be construed as empowering an authorised officer to enter any dwelling without the permission of the occupier or the authority of a warrant under *section 78*.

Power of authorised officers to do things at premises.

77.— (1) An authorised officer may, at any premises lawfully entered by the officer, do any of the following:

(*a*) inspect the premises;

(*b*) request any person on the premises who apparently has control of, or access to, records or other documents that relate to the business of a designated person (being a designated person whose competent authority is the State competent authority who appointed the authorised officer)—

(i) to produce the documents for inspection, and

(ii) if any of those documents are in an electronic, mechanical or other form, to reproduce the document in a written form;

(*c*) inspect documents produced or reproduced in accordance with such a request or found in the course of inspecting the premises;

(*d*) take copies of those documents or of any part of them (including, in the case of a document in an electronic, mechanical or other form, a copy of the document in a written form);

(*e*) request any person at the premises who appears to the authorised person to have information relating to the documents, or to the business of the designated person, to answer questions with respect to the documents or that business;

(*f*) remove and retain the documents (including in the case of a document in an electronic, mechanical or other form, a copy of the information in a written form) for the period reasonably required for further examination;

(*g*) request a person who has charge of, operates or is concerned in the operation of data equipment, including any person who has operated that equipment, to give the officer all reasonable assistance in relation to the operation of the equipment or access to the data stored within it;

(*h*) secure, for later inspection, the premises or part of the premises at which the authorised officer reasonably believes records or other documents relating to the business of the designated person are located.

(2) A person to whom a request is made in accordance with *subsection (1)* shall—

(*a*) comply with the request so far as it is possible to do so, and

(*b*) give such other assistance and information to the authorised officer with respect to the business of the designated person concerned as is reasonable in the circumstances.

(3) A reference in this section to data equipment includes a reference to any associated apparatus.

(4) A reference in this section to a person who operates or has operated data equipment includes a reference to a person on whose behalf data equipment is operated or has been operated.

Entry to premises and doing of things under warrant.

78.— (1) A judge of the District Court may issue a warrant under this section if satisfied, by information on oath of an authorised officer, that there are reasonable grounds for believing that—

(*a*) documents relating to the business of a designated person that are required for the purpose of assisting the State competent authority that appointed the authorised officer under this Chapter in the performance of the authority's functions under this Part are contained on premises, and

(*b*) the premises comprise a dwelling or an authorised officer has been obstructed or otherwise prevented from entering the premises under *section 75*.

(2) A warrant under this section authorises an authorised officer, at any time or times within one month of the issue of the warrant—

(*a*) to enter the premises specified in the warrant, and

(*b*) to exercise the powers conferred on authorised officers by this Chapter or any of those powers that are specified in the warrant.

(3) Entry to premises the subject of a warrant may be effected with the use of reasonable force.

Authorised officer may be accompanied by others.

79.— An authorised officer may be accompanied, and assisted in the exercise of the officer's powers (including under a warrant issued under *section 78*), by such other authorised officers, members of the Garda Síochána or other persons as the authorised officer reasonably considers appropriate.

Offence to obstruct, interfere or fail to comply with request.

80.— (1) A person commits an offence if the person, without reasonable excuse—

(*a*) obstructs or interferes with an authorised officer in the exercise of the officer's powers under this Chapter, or

(*b*) fails to comply with a requirement, or request made by an authorised officer, under *section 77* (including as applied by *section 78*).

(2) A person who commits an offence under this section is liable, on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both).

(3) A reference in this section to an authorised officer includes a member of the Garda Síochána or other person who is accompanying and assisting the officer in accordance with *section 79*.

Self-incrimination — questions of authorised officers.

81.— Nothing in this Chapter requires a person to answer questions if to do so might tend to incriminate the person.

Production of documents or information not required in certain circumstances.

82.— Nothing in this Chapter requires the production of any document or information subject to legal privilege.

Disclosure or production not to be treated as breach or to affect lien.

83.— (1) The disclosure or production of any information or document by a person in accordance with this Chapter shall not be treated as a breach of any restriction under any enactment or rule of law on disclosure or production by the person or any other person on whose behalf the information or document is disclosed or produced.

(2) The production referred to in *subsection (1)* of any item forming part of the documents relating to the business of a designated person shall not prejudice any lien that the designated person or any other person claims over that item.

Chapter 9

Authorisation of Trust or Company Service Providers

Annotations

Modifications (not altering text):

C7 Application of Chapter extended (15.07.2010) by *European Communities (Trust or Company Service Providers) (Temporary Authorisation) Regulations 2010* (S.I. No. 347 of 2010), regs. 5 and 9, in effect as per reg. 2.

5. A person to whom these Regulations apply who makes an application for an authorisation under section 88 of the Act of 2010 shall, subject to the provisions of these Regulations, be deemed to be the holder of an authorisation under Chapter 9 of Part 4 of the Act of 2010 and any such authorisation deemed to have been so granted is in these Regulations referred to as a "temporary authorisation".

...

9. The holder of a temporary authorisation shall be subject to and comply with the provisions of Chapter 9 of Part 4 of the Act of 2010 as if such authorisation had been granted under that Chapter and without prejudice to the generality of the foregoing—

(a) a temporary authorisation may be amended under section 93 of the Act of 2010,

(b) a temporary authorisation may be revoked in accordance with sections 96 and 97 of the Act of 2010,

(c) the Minister may as respects the holder of a temporary authorisation give a direction under section 98 of the Act of 2010.

...

Interpretation (*Chapter 9*).

84.— F87**[**(1)**]** In this Chapter—

"Appeal Tribunal" means an Appeal Tribunal established under *section 101*;

"authorisation" means an authorisation to carry on business as a trust or company service provider granted under this Chapter and, if such an authorisation is renewed or amended under this Chapter, means, unless the context otherwise requires, the authorisation as renewed or amended (as the case may be);

"principal officer" means—

(*a*) in relation to a body corporate, any person who is a director, manager, secretary or other similar officer of the body corporate or any person purporting to act in such a capacity, or

(*b*) in relation to a partnership—

(i) any person who is a partner in, or a manager or other similar officer of, the partnership or any person purporting to act in such a capacity, and

(ii) in a case where a partner of the partnership is a body corporate, any person who is a director, manager, secretary or other similar officer of such a partner or any person purporting to act in such a capacity;

F87**[**'subsidiary' has the meaning assigned to it by section 155 of the Companies Act 1963**]**

"trust or company service provider" does not include any of the following:

(*a*) a member of a designated accountancy body;

(*b*) a barrister or solicitor;

(*c*) a credit institution or financial institution.

F87**[**(2) (a) Subject to paragraph (b), in this Chapter a reference to the Minister shall, in a case where the applicant for or the holder of an authorisation is a subsidiary of a credit or financial institution, be construed as a reference to the Central Bank of Ireland.

(b) Paragraph (a) does not apply to—

(i) section 88(5),

(ii) sections 89(5)(b)(ii), 90(3)(b)(ii), 93(6)(b)(ii), 97(6)(b)(ii), 98(2)(b)(ii) and 100(2) in so far as those provisions relate to the specifying of a form by the Minister,

(iii) section 94(3),

(iv) section 101,

(v) section 104(8),

(vi) section 106(7).**]**

Annotations

Amendments:

F87 Inserted (3.03.2014) by *Criminal Justice Act 2013* (19/2013), s. 15(a), (b), (c), S.I. No. 80 of 2014.

Meaning of "fit and proper person".

85.— For the purposes of this Chapter, a person is not a fit and proper person if any of the following apply:

(*a*) the person has been convicted of any of the following offences:

(i) money laundering;

(ii) terrorist financing;

(iii) an offence involving fraud, dishonesty or breach of trust;

(iv) an offence in respect of conduct in a place other than the State that would constitute an offence of a kind referred to in *subparagraph (i)*, *(ii)* or *(iii)* if the conduct occurred in the State;

(*b*) in a case where the person is an individual, the person is under 18 years of age;

(*c*) the person—

(i) has suspended payments due to the person's creditors,

(ii) is unable to meet other obligations to the person's creditors, or

(iii) is an individual who is an undischarged bankrupt;

(*d*) the person is otherwise not a fit and proper person.

Authorisations held by partnerships.

86.— (1) A reference in a relevant document to the holder or proposed holder of an authorisation includes, in a case where the holder or proposed holder is a partnership, a reference to each partner of the partnership unless otherwise specified.

(2) A reference in *subsection (1)* to a relevant document is a reference to any of the following:

(*a*) this Chapter;

(*b*) a regulation made for the purposes of this Chapter;

(*c*) an authorisation or condition of an authorisation;

(*d*) any notice or direction given under this Chapter;

(*e*) any determination under this Chapter.

(3) Without prejudice to the generality of *subsection (1)* or *section 111*, where any requirement is imposed by or under this Chapter on the holder of an authorisation and failure to comply with the requirement is an offence, each partner of a partnership (being a partnership that is the holder of an authorisation) who contravenes the requirement is liable for the offence.

Prohibition on carrying on business of trust or company service provider without authorisation.

87.— (1) A person commits an offence if the person carries on business as a trust or company service provider without being the holder of an authorisation issued by the Minister under this Chapter.

(2) A person who commits an offence under *subsection (1)* is liable—

(*a*) on summary conviction, to a fine not exceeding €5,000, or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment not exceeding 5 years (or both).

Application for authorisation.

88.— (1) An individual, body corporate or partnership may apply to the Minister for an authorisation to carry on business as a trust or company service provider.

(2) The application shall—

(*a*) be in a form provided or specified by the Minister,

(*b*) specify the name of—

(i) the proposed holder of the authorisation,

(ii) in a case where the proposed holder of the authorisation is a body corporate or partnership or an individual who proposes to carry on business as a trust or company service provider as a partner in a partnership, any principal officer of the body corporate or partnership (as the case may be), and

(iii) any person who is, or is proposed to be, a beneficial owner of the business,

(*c*) be accompanied by any consent, in the form provided or specified by the Minister, that is required to enable access to personal data F88**[**...**]** held by other persons or bodies and that is required to assist the Minister in determining, for the purposes of *section 89* (including as applied by *section 92*) whether or not the proposed holder and other persons referred to in *paragraph (b)* are fit and proper persons,

(*d*) contain such other information, and be accompanied by such documents, as the Minister requests,

(*e*) be accompanied by the prescribed fee (if any).

(3) The Minister may, by written notice given to an applicant, require the applicant to provide, within the period of not less than 14 days specified in the notice, such additional information and documents as are reasonably necessary to enable the Minister to determine the application.

(4) As soon as practicable after an applicant becomes aware that any information or document provided to the Minister under this section contains a material inaccuracy or has changed in any material particular, including information or a document provided in relation to an application that has been granted, but not including information or a document provided in relation to an application that has been refused, the applicant shall give notice in writing to the Minister of the error or change in circumstances, as the case may be.

(5) For the purposes of *subsection (2)(e)* (including as applied by *section 92*), the Minister may prescribe different fees, to accompany applications for authorisations under this Chapter, for different classes of proposed holders of those authorisations and in prescribing such fees may differentiate between the fee to accompany such an application for an authorisation (not being an application for the renewal of such an authorisation) and the fee to accompany an application for the renewal of such an authorisation.

Annotations

Amendments:

F88 Deleted (25.05.2018) by *Data Protection Act 2018* (7/2018), s. 213(c), S.I. No. 174 of 2018.

Editorial Notes:

E38 Fee prescribed in respect of application for authorisation made under section (15.07.2010) by *Trust or Company Service Provider (Authorisation) (Fees) Regulations 2010* (S.I. No. 348 of 2010), in effect as per reg. 1(2).

E39 Procedure for and conditions pertaining to temporary authorisation in relation to a person who is a trust or company service provider prescribed (15.07.2010) by *European Communities (Trust or Company Service Providers) (Temporary Authorisation) Regulations 2010* (S.I No. 347 of 2010), in effect as per reg. 2.

Grant and refusal of applications for authorisation.

89.— (1) The Minister may refuse an application under *section 88* only if—

(*a*) the application does not comply with the requirements of *section 88*,

(*b*) the applicant does not provide any additional documents or information in accordance with a notice given under *section 88 (3)*,

(*c*) the Minister has reasonable grounds to be satisfied that information given to the Minister by the applicant in connection with the application is false or misleading in any material particular,

(*d*) the Minister has reasonable grounds to be satisfied that any of the following persons is not a fit and proper person:

(i) the proposed holder of the authorisation;

(ii) in a case where the proposed holder of the authorisation is a body corporate or partnership or an individual who proposes to carry on business as a trust or company service provider as a partner in a partnership, any principal officer of the body corporate or partnership (as the case may be);

(iii) any person who is, or is proposed to be, a beneficial owner of the business concerned,

(*e*) the applicant has failed to satisfy the Minister that the proposed holder of the authorisation will comply with the obligations imposed on trust or company service providers, as designated persons, under this Part,

(*f*) the applicant has failed to satisfy the Minister that the proposed holder of the authorisation will comply with each of the following:

(i) any conditions that the Minister would have imposed on the authorisation concerned if the Minister had granted the application;

(ii) any prescribed requirements referred to in *section 94*;

(iii) *section 95*;

(iv) *section 98*;

(v) *section 106*,

(*g*) the proposed holder of the authorisation is so structured, or the business of the proposed holder is so organised, that the proposed holder is not capable of being regulated under this Chapter, or as a designated person under this Part, to the satisfaction of the Minister,

(*h*) in a case where the proposed holder of the authorisation is a body corporate, the body corporate is being wound up,

(*i*) in a case where the proposed holder of the authorisation is a partnership, the partnership is dissolved by the death or bankruptcy of a partner or because of the operation of a provision of the Partnership Act 1890 or otherwise,

(*j*) in a case where any person referred to in *paragraph (d)* has been authorised to carry on business as a trust or company service provider in another Member State, an authority of the other Member State that performs functions similar to those of the Minister under this Chapter has terminated the authority of the person to carry on business as a trust or company service provider in the other Member State, or

(*k*) in a case where the proposed holder of the authorisation is a subsidiary of a body corporate that is authorised to carry on business as a trust or company service provider in another Member State, an authority of the other Member

State that performs functions similar to those of the Minister under this Chapter has terminated the authority of the body corporate to carry on business as a trust or company service provider in the other Member State.

(2) If the Minister proposes to refuse an application, the Minister shall serve on the applicant a notice in writing—

(*a*) specifying the grounds on which the Minister proposes to refuse the application, and

(*b*) informing the applicant that the applicant may, within 21 days after the serving of the notice, make written representations to the Minister showing why the Minister should grant the application.

(3) Not later than 21 days after a notice is served on an applicant under *subsection (2)*, the applicant may make written representations to the Minister showing why the Minister should grant the application.

(4) The Minister may refuse an application only after having considered any representations made by the applicant in accordance with *subsection (3)*.

(5) As soon as practicable after refusing an application, the Minister shall serve a written notice of the refusal on the applicant. The notice shall include a statement—

(*a*) setting out the grounds on which the Minister has refused the application, and

(*b*) informing the applicant that—

(i) the applicant may appeal to an Appeal Tribunal against the refusal, and

(ii) if the applicant proposes to appeal to an Appeal Tribunal against the refusal, the applicant may, within one month after being served with the notice of refusal, serve a notice of intention to appeal on the Minister, in the form provided or specified by the Minister.

(6) If the Minister does not refuse the application, he or she shall grant it and, on granting the application, the Minister shall—

(*a*) record the appropriate particulars of the holder of the authorisation in the register of persons authorised to carry on business as a trust or company service provider, and

(*b*) issue the applicant with an authorisation that authorises the holder of the authorisation to carry on business as a trust or company service provider.

Minister may impose conditions when granting an application for an authorisation.

90.— (1) In granting an application for an authorisation under this Chapter, the Minister may impose on the holder of the authorisation any conditions that the Minister considers necessary for the proper and orderly regulation of the holder's business as a trust or company service provider and, in particular, for preventing the business from being used to carry out money laundering or terrorist financing.

(2) The Minister shall specify any such conditions in the authorisation granted to the holder or in one or more documents annexed to that authorisation.

(3) If, under this section, the Minister imposes any conditions on an authorisation, the Minister shall serve on the holder of the authorisation, together with the authorisation, a written notice of the imposition of the conditions that includes a statement—

(*a*) setting out the grounds on which the Minister has imposed the conditions, and

(*b*) informing the holder that—

(i) the holder may appeal to an Appeal Tribunal against the imposition of any of the conditions, and

(ii) if the holder proposes to appeal to an Appeal Tribunal against the imposition of any of the conditions, the holder may, within one month after being served with the notice of the imposition of conditions, serve a notice of intention to appeal on the Minister, in the form provided or specified by the Minister.

Terms of authorisation.

91.— (1) An authorisation comes into force on the day on which the authorisation is granted, or, if a later date is specified in the authorisation, on that later date, whether or not an appeal against any conditions of the authorisation is made under *section 100*.

(2) An authorisation remains in force, unless sooner revoked under this Chapter, for a period of 3 years from the date on which it comes into force.

(3) A reference in this section to an authorisation does not include a reference to an authorisation that is renewed under *section 92*.

Renewal of authorisation.

92.— (1) The Minister may renew an authorisation on the application of the holder of the authorisation unless the authorisation has been revoked under this Chapter.

(2) *Sections 88* to *90* apply, with any necessary modifications, in relation to an application for the renewal of an authorisation.

(3) An application for the renewal of an authorisation shall be made not less than 10 weeks before the end of the period for which it was granted.

(4) In addition to the grounds specified in *section 89* (as applied by *subsection (2)*), the Minister may refuse to grant a renewed authorisation on the grounds that the application for renewal has been made less than 10 weeks before the end of the period for which the authorisation was granted.

(5) If an application for the renewal of an authorisation is made within the time provided for in *subsection (3)* and is not determined by the Minister before the end of the period for which the authorisation was granted, the authorisation remains in force until the date on which the application is determined.

(6) A renewed authorisation comes into force on—

(*a*) in a case where *subsection (5)* applies, the date on which the application is determined, or

(*b*) in any other case, the day immediately following the end of the period for which the authorisation that it renews was granted or last renewed, as the case may be.

(7) A renewed authorisation, unless sooner revoked under this Chapter, remains in force for a period of 3 years from the date on which it comes into force under *subsection (6)*.

(8) *Subsections (6)* and *(7)* have effect whether or not an appeal against any conditions of the authorisation is made under *section 100*.

Annotations

Editorial Notes:

E40 Fee prescribed in respect of application for renewal of authorisation made under section (15.07.2010) by *Trust or Company Service Provider (Authorisation) (Fees) Regulations 2010* (S.I. No. 348 of 2010), in effect as per reg. 1(2).

Minister may amend authorisation.

93.— (1) The Minister may amend an authorisation granted under this Chapter by varying, replacing or revoking any conditions or by adding a new condition if the Minister considers that the variation, replacement, revocation or addition is necessary for the proper and orderly regulation of the business of the holder of the authorisation as a trust or company service provider and, in particular, for preventing the business from being used to carry out money laundering or terrorist financing.

(2) If the Minister proposes to amend an authorisation under this section, the Minister shall serve on the holder of the authorisation a notice in writing informing the holder of the Minister's intention to amend the authorisation.

(3) The notice shall—

(*a*) specify the proposed amendment, and

(*b*) inform the holder that the holder may, within 21 days after service of the notice, make written representations to the Minister showing why the Minister should not make that amendment.

(4) Not later than 21 days after a notice is served under *subsection (2)* on the holder of an authorisation, the holder may make written representations to the Minister showing why the Minister should not amend the authorisation.

(5) The Minister may amend an authorisation only after having considered any representations to the Minister made in accordance with *subsection (4)* showing why the Minister should not amend the authorisation.

(6) The Minister shall serve written notice of any amendment of an authorisation on the holder of the authorisation. The notice shall include a statement—

(*a*) setting out the grounds on which the Minister has amended the authorisation, and

(*b*) informing the holder that—

(i) the holder may appeal to an Appeal Tribunal against the amendment, and

(ii) if the holder proposes to appeal to an Appeal Tribunal against the amendment, the holder may, within one month after being served with the notice of amendment, serve a notice of intention to appeal on the Minister, in the form provided or specified by the Minister.

(7) The amendment of an authorisation under this section takes effect from the date of the notice of amendment or, if a later date is specified in the notice, from that date, whether or not an appeal against the amendment is made under *section 100*.

Offence to fail to comply with conditions or prescribed requirements.

94.— (1) The holder of an authorisation commits an offence if the holder fails to comply with—

(*a*) any condition of the authorisation, or

(*b*) any prescribed requirements.

(2) A person who commits an offence under this section is liable—

(*a*) on summary conviction, to a fine not exceeding €2,000, or

(*b*) on conviction on indictment, to a fine not exceeding €100,000.

(3) The Minister may prescribe requirements for the purposes of *subsection (1)(b)* only if the Minister is satisfied that it is necessary to do so for the proper and orderly regulation of the business of trust or company service providers and, in particular, for preventing such businesses from being used to carry out money laundering orterrorist financing.

Annotations

Modifications (not altering text):

C8 Application extended (15.07.2010) by *European Communities (Trust or Company Service Providers) (Temporary Authorisation) Regulations 2010* (S.I No. 347 of 2010), reg. 10, in effect as per reg. 2.

10. A temporary authorisation shall be subject to any prescribed requirements referred to in section 94 of the Act of 2010.

Holder of authorisation to ensure that principal officers and beneficial owners are fit and proper persons.

95.— (1) The holder of an authorisation shall take reasonable steps to ensure that the following persons are fit and proper persons:

(*a*) in a case where the holder of the authorisation is a body corporate, a partnership or an individual carrying on business as a trust or company service provider as a partner in a partnership, any principal officer of the body corporate or partnership (as the case may be);

(*b*) any person who is a beneficial owner of the business concerned.

(2) A person who commits an offence under this section is liable—

(*a*) on summary conviction, to a fine not exceeding €2,000, or

(*b*) on conviction on indictment, to a fine not exceeding €100,000.

Revocation of authorisation by Minister on application of holder.

96.— The Minister shall revoke an authorisation on the application of the holder of the authorisation, but only if satisfied that the holder of the authorisation has fully complied with each of the following:

(*a*) any conditions of the authorisation;

(*b*) any prescribed requirements referred to in *section 94*;

(*c*) *section 95*;

(*d*) *section 98*;

(*e*) *section 106*.

Revocation of authorisation other than on application of holder.

97.— (1) The Minister may revoke an authorisation only if the Minister has reasonable grounds to be satisfied of any of the following:

(*a*) the holder of the authorisation has not commenced to carry on business as a trust or company service provider within 12 months after the date on which the authorisation was granted;

(*b*) the holder of the authorisation has not carried on such a business within the immediately preceding 6 months;

(*c*) the authorisation was obtained by means of a false or misleading representation;

(*d*) any of the following persons is not a fit and proper person:

(i) the holder of the authorisation;

(ii) in a case where the holder of the authorisation is a body corporate, a partnership or an individual carrying on business as a trust or company service provider as a partner in a partnership, any principal officer of the body corporate or partnership (as the case may be);

(iii) any person who is a beneficial owner of the business concerned;

(*e*) the holder of the authorisation has contravened or is contravening the obligations imposed on trust or company service providers, as designated persons, under this Part;

(*f*) the holder of the authorisation has contravened or is contravening any of the following:

(i) a condition of the authorisation;

(ii) a prescribed requirement referred to in *section 94*;

(iii) *section 95*;

(iv) *section 98*;

(v) *section 106*;

(*g*) the holder of the authorisation is so structured, or the business of the holder is so organised, that the holder is not capable of being regulated under this Chapter or as a designated person under this Part;

(*h*) in a case where the holder of the authorisation is a body corporate, the body corporate is being wound up;

(*i*) in a case where the holder of the authorisation is a partnership, the partnership is dissolved by the death or bankruptcy of a partner or because of the operation of a provision of the Partnership Act 1890 or otherwise;

(*j*) in a case where any person referred to in *paragraph (d)* has been authorised to carry on business as a trust or company service provider in another Member State, an authority of the other Member State that performs functions similar to those of the Minister under this Chapter has terminated the authority of the person to carry on business as a trust or company service provider in the other Member State;

(*k*) in a case where the holder of the authorisation is a subsidiary of a body corporate that is authorised to carry on business as a trust or company service provider in another Member State, an authority of the other Member State that performs functions similar to those of the Minister under this Chapter has terminated the authority of the body corporate to carry on business as a trust or company service provider in the other Member State.

(2) If the Minister proposes to revoke an authorisation under this section, the Minister shall serve on the holder of the authorisation a notice in writing informing the holder of the Minister's intention to revoke the authorisation.

(3) The notice shall—

(*a*) specify the grounds on which the Minister proposes to revoke the authorisation, and

(*b*) inform the holder that the holder may, within 21 days after service of the notice, make written representations to the Minister showing why the Minister should not revoke the authorisation.

(4) Not later than 21 days after a notice is served under *subsection (2)* on the holder of an authorisation, the holder may make written representations to the Minister showing why the Minister should not revoke the authorisation.

(5) The Minister may revoke the authorisation only after having considered any representations made by the holder of the authorisation in accordance with *subsection (4)*.

(6) As soon as practicable after revoking an authorisation under this section, the Minister shall serve written notice of the revocation on the person who was the holder of the authorisation. The notice shall include a statement—

(*a*) setting out the reasons for revoking the authorisation, and

(*b*) informing the holder that—

(i) the holder may appeal to an Appeal Tribunal against the revocation, and

(ii) if the holder proposes to appeal to an Appeal Tribunal against the revocation, the holder may, within one month after being served with the notice of revocation, serve a notice of intention to appeal on the Minister in the form provided or specified by the Minister.

(7) The revocation of an authorisation under this section takes effect from the date of the notice of revocation or, if a later date is specified in the notice, from that date, whether or not an appeal against the revocation is made under *section 100*.

Direction not to carry out business other than as directed.

98.— (1) If the Minister reasonably believes that there may be grounds for revoking an authorisation under *section 97*, the Minister may serve on the holder of the authorisation a direction in writing prohibiting the holder from carrying on business as a trust or company service provider other than in accordance with conditions specified by the Minister.

(2) The Minister shall include in a direction under this section a statement—

(*a*) setting out F89**[**the reasons**]** for giving the direction,

(*b*) informing the holder of the authorisation concerned that—

(i) the holder may appeal to an Appeal Tribunal against the direction, and

(ii) if the holder proposes to appeal to an Appeal Tribunal against the direction, the holder may, within one month after being served with the direction, serve a notice of intention to appeal on the Minister in the form provided or specified by the Minister,

and

(*c*) specifying the conditions with which the holder of the authorisation is required to comply.

(3) The Minister may, by notice in writing served on the holder of the authorisation concerned, amend or revoke a direction given under this section.

(4) Without prejudice to the generality of *subsection (3)*, the Minister may, by notice in writing given to the holder of the authorisation concerned, extend the period during which a direction remains in force by a further period or periods not exceeding 6 months.

(5) A direction under this section takes effect from the date on which it is given or, if a later date is specified in the direction, from that date, whether or not an appeal against the direction is made under *section 100*.

(6) A direction under this section ceases to have effect—

(*a*) at the end of the period, not exceeding 6 months, specified in the direction, or if the period is extended under *subsection (4)*, at the end of the extended period, or

(*b*) on the revocation of the holder's authorisation under this Chapter,

whichever occurs first.

(7) A person who contravenes a direction given under this section, or fails to comply with a condition contained in the direction, commits an offence.

(8) A person who commits an offence under this section is liable—

(*a*) on summary conviction, to a fine not exceeding €5,000, or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).

Annotations

Amendments:

F89 Substituted (3.03.2014) by *Criminal Justice Act 2013* (19/2013), s. 16(a), S.I. No. 80 of 2014.

Minister to publish notice of revocation or direction.

99.— As soon as practicable after revoking an authorisation under *section 96* or *97*, or giving a direction under *section 98*, the Minister shall publish in *Iris Oifigiúil* a notice giving particulars of the revocation or direction.

Appeals against decisions of Minister.

100.— (1) In this section, "appealable decision" means a decision of the Minister under—

(*a*) *section 89* to refuse an application for an authorisation,

(*b*) *section 89*, as applied by *section 92*, to refuse an application for the renewal of an authorisation,

(*c*) *section 90* to impose conditions on an authorisation,

(*d*) *section 90*, as applied by *section 92*, to impose conditions on an authorisation that is renewed,

(*e*) *section 93* to amend an authorisation,

(*f*) *section 97* to revoke an authorisation, or

(*g*) *section 98*to serve a direction on the holder of an authorisation.

(2) A person aggrieved by an appealable decision may, within one month after being served with notice of the decision, serve a notice of the person's intention to appeal against the decision on the Minister in the form provided or specified by the Minister.

(3) On receipt of the notification, the Minister shall refer the matter to an Appeal Tribunal established under *section 101*.

(4) The Appeal Tribunal may invite the person and the Minister to make written submissions to it in relation to the appeal.

(5) The Appeal Tribunal shall notify the person, in writing, of the following matters:

(*a*) the date and time of the hearing of the appeal;

(*b*) that the person may attend the hearing;

(*c*) that the person may be represented at the hearing by a barrister, solicitor or agent.

(6) An Appeal Tribunal may refuse to hear, or continue to hear, an appeal under this section if it is of the opinion that the appeal is vexatious, frivolous, an abuse of process or without substance or foundation.

(7) The Appeal Tribunal shall (unless the appeal is withdrawn, or discontinued or dismissed under *subsection (6)*) determine the appeal by—

(*a*) affirming the decision of the Minister to which the appeal relates, or

(*b*) substituting its determination for that decision.

(8) The Appeal Tribunal shall notify its determination in writing to the Minister and the person appealing.

(9) Within 3 months after the date on which an appeal is determined by an Appeal Tribunal, the Minister or person who appealed may appeal to the High Court on any question of law arising from the determination.

Annotations

Modifications (not altering text):

C9 Appeal tribunal established for period commencing on 22nd day of May 2013 and ending on 21st day of May 2018 to adjudicate on appeals under section (16.05.2013) by *Trust or Company Service Provider Authorisation (Appeal Tribunal) (Establishment) Order 2013* (S.I. No. 167 of 2013), reg. 3.

Appeal Tribunals.

101.— (1) The Minister may, by order, establish, for a specified period, an Appeal Tribunal or more than one Appeal Tribunal to adjudicate on appeals under *section 100*.

(2) An Appeal Tribunal shall be independent in the performance of its functions.

(3) The Minister may appoint a person who is a practising barrister or solicitor of not less than 7 years' standing to be a member of and constitute an Appeal Tribunal.

(4) The appointment shall be subject to such terms and conditions, including remuneration, as the Minister may determine with the consent of the Minister for Finance.

(5) A person constituting an Appeal Tribunal may at any time resign by a letter sent to the Minister, and the resignation shall take effect on the date on which the Minister receives the letter.

(6) The Minister may, at any time, revoke an appointment of a person under this section for stated misbehaviour or if, in the opinion of the Minister, the person has become incapable through ill health or otherwise of effectively performing the functions of an Appeal Tribunal.

(7) An Appeal Tribunal may determine its own procedure, subject to *section 101* and to any general directions given to Appeal Tribunals by the Minister in the interests of securing consistency of procedures in relation to appeals under this Chapter.

Annotations

Editorial Notes:

E41 Power pursuant to subs. (1) exercised (19.11.2018 to 18.11.2023) by *Trust or Company Service Provider Authorisation (Appeal Tribunal) (Establishment) Order 2018* (S.I. N. 475 of 2018). The establishment of two appeal tribunals in identical terms is explained in the explanatory memorandum.

E42 Power pursuant to subs. (1) exercised (19.11.2018 to 18.11.2023) by *Trust or Company Service Provider Authorisation (Appeal Tribunal) (Establishment) Order 2018* (S.I. N. 474 of 2018). The establishment of two appeal tribunals in identical terms is explained in the explanatory memorandum.

E43 Power pursuant to subs. (1) exercised (22.05.2013 to 21.05.2018) by *Trust or Company Service Provider Authorisation (Appeal Tribunal) (Establishment) Order 2013* (S.I. No. 167 of 2013).

Provision of information by Garda Síochána as to whether or not person is fit and proper person.

102.— (1) The Minister may request the Commissioner of the Garda Síochána to provide any information that is required to assist the Minister in determining, for the purposes of this Chapter, whether or not any of the following persons is a fit and proper person:

(*a*) the holder or proposed holder of an authorisation;

(*b*) in a case where the holder or proposed holder of the authorisation is a body corporate, a partnership or an individual carrying on, or proposing to carry on, business as a trust or company service provider as a partner in a partnership, any principal officer of the body corporate or partnership (as the case may be);

(*c*) any person who is a beneficial owner of the business of the holder or proposed holder of the authorisation concerned.

(2) Notwithstanding any other enactment or rule of law, the Commissioner of the Garda Síochána shall provide the Minister with information in accordance with a request of the Minister under this section.

Extension of powers under *Chapter 8* for purposes related to this Chapter.

103.— (1) The functions of a State competent authority, in relation to designated persons, under *Chapter 8*, may be performed by the Minister F90**[**to assist in carrying out**]** functions in relation to trust or company service providers under this Chapter.

(2) For that purpose, *sections 66* to *83* apply with any necessary modifications, including the following:

(*a*) a relevant authorised officer has, in respect of trust or company service providers within the meaning of this Chapter, all of the functions that an authorised officer appointed by a State competent authority under *section 72* has in respect of designated persons;

(*b*) a judge of the District Court, in the case of an application under *section 78* by a relevant authorised officer in respect of a trust or company service provider, has all of the functions that such a judge has, in the case of a similar application under that section by an authorised officer appointed by a State competent authority under *section 72*, in respect of a designated person;

(*c*) *section 79* applies so as to enable a relevant authorised officer to be accompanied and assisted in the exercise of the officer's powers as referred to in that section;

(*d*) *section 80* applies to a person who engages in conduct, referred to in that section, in relation to—

(i) a relevant authorised officer, and

(ii) any person accompanying and assisting the officer in accordance with *section 79* as applied by *paragraph (c)*.

(3) This section has effect whether or not the Minister is the State competent authority for any class of trust or company service providers.

(4) In this section "relevant authorised officer" means an authorised officer appointed by the Minister under *section 72*, as applied by this section.

Annotations

Amendments:

F90 Substituted (3.03.2014) by *Criminal Justice Act 2013* (19/2013), s. 16(b), S.I. No. 80 of 2014.

Register of persons holding authorisations.

104.— (1) The Minister shall establish and maintain a register of persons authorised under this Chapter to carry on business as a trust or company service provider containing—

(*a*) the name and the address of the principal place of business of each person authorised to carry on business as a trust or company service provider, and

(*b*) such other information as may be prescribed.

(2) The register may be in book form, electronic form or such other form as the Minister may determine. The register may be maintained in an electronic, mechanical or other non-written form only if it is capable of being reproduced in a written form.

(3) The Minister shall maintain the register F91**[**at an office in the State**]**.

(4) Members of the public are entitled, without charge, to inspect the register F91**[**during ordinary business hours**]**.

F92**[**(5) The Minister may publish a register in written, electronic or other form and a member of the public is entitled to obtain a copy of a register or of an entry in a register on payment of such reasonable copying charges as may be prescribed (if any).**]**

(6) The holder of an authorisation to whom an entry in the Register relates shall, as soon as practicable after the holder becomes aware of any error in the entry, or any change in circumstances that is likely to have a bearing on the accuracy of the entry, give notice in writing to the Minister of the error or change in circumstances, as the case may be.

(7) In any legal proceedings, a certificate purporting to be signed by the Minister and stating that a person—

(*a*) is recorded in the Register as the holder of an authorisation,

(*b*) is not recorded in the Register as the holder of an authorisation,

(*c*) was recorded in the Register as being, at a specified date or during a specified period, the holder of an authorisation, or

(*d*) was not recorded in the Register as being, at a specified date or during a specified period, the holder of an authorisation,

is evidence of the matter referred to in *paragraph (a)*, *(b)*, *(c)* or *(d)* (as the case may be), and is taken to have been signed by the person purporting to have signed it, unless the contrary is shown.

(8) The Minister may prescribe particulars for the purposes of *subsection (1) (b)* or *section 105* only if satisfied that those particulars reasonably relate to the business of trust or company service providers or to the regulation of the business of trust or company service providers under this Part.

Annotations

Amendments:

F91 Substituted (3.03.2014) by *Criminal Justice Act 2013* (19/2013), s. 16(c), S.I. No. 80 of 2014.

F92 Substituted (14.06.2013) by *Criminal Justice Act 2013* (19/2013), s. 17, S.I. No. 196 of 2013.

Minister to publish list of persons holding authorisations.

105.— The Minister shall, not less frequently than once during every period of 12 months after the commencement of this section, publish in *Iris Oifigiúil* a list of persons holding authorisations, together with other prescribed particulars (if any).

Holders of authorisations to retain certain records.

106.— (1) The holder of an authorisation shall—

(*a*) retain at an office or other premises in the State such records as may be specified by the Minister, and

(*b*) notify the Minister in writing of the address of any office or other premises where those records are retained.

(2) The requirement imposed by *subsection (1)* is in addition to, and not in substitution for, any other requirements imposed under any other enactment or rule of law with respect to the retention of records by the holder of an authorisation, including the requirements specified in *section 55*.

(3) The holder of an authorisation shall retain the records referred to in *subsection (1)* for a period of not less than 6 years after—

(*a*) in the case of a record made in relation to a customer of the holder, the last dealing with the customer, or

(*b*) in any other case, the record is made.

(4) The holder of an authorisation may keep the records referred to in *subsection (1)* wholly or partly in an electronic, mechanical or other non-written form only if they are capable of being reproduced in a written form.

(5) The obligations that are imposed on a holder of an authorisation under this section continue to apply to a person who has been the holder of an authorisation, but has ceased to hold an authorisation or to carry on business as a trust or company service provider.

(6) A requirement for the holder of an authorisation that is a body corporate to retain any record under this section applies to any body corporate that is a successor to, or a continuation of, the body corporate.

(7) The Minister may make regulations prescribing requirements relating to the retention of records referred to in this section of a body corporate that is wound up or a partnership that is dissolved.

(8) A person who fails to comply with this section commits an offence and is liable—

(*a*) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).

Chapter 10

Other

Guidelines.

107.—F93**[**...**]**

Annotations

Amendments:

F93 Repealed (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 40(b), S.I. No. 486 of 2018.

F94**[**Defence

107A. It shall be a defence in proceedings for an offence under this Part for the person charged with the offence to prove that the person took all reasonable steps to avoid the commission of the offence.**]**

Annotations

Amendments:

F94 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 33, S.I. No. 486 of 2018.

Editorial Notes:

E44 The section heading is taken from the amending section in the absence of one included in the amendment.

Minister may delegate certain functions under this Part.

108.— (1) The Minister may, by instrument in writing, delegate any of the Minister's functions under *Chapter 8* or *9*, or under *section 109*, to a named officer or an officer of a particular class or description.

(2) A delegation under this section may be made subject to such conditions or limitations as to the performance of any of the functions delegated, or as to time or circumstance, as may be specified in the instrument of delegation.

(3) The Minister may, by instrument in writing, revoke a delegation under this section.

(4) A function delegated under this section may, while the delegation remains unrevoked, be performed by the delegate in accordance with the terms of the delegation.

(5) The Minister may continue to perform any functions delegated under this section.

(6) Nothing in this section shall be construed as affecting the application to this Act of the general law concerning the imputing of acts of an officer of a Minister of the Government to the Minister of the Government.

(7) In this section, "officer" means an officer of the Minister who is an established civil servant for the purposes of the Civil Service Regulation Act 1956.

F95[Obligation for certain designated persons to register with Central Bank of Ireland

108A. (1) Subject to *subsection (2)*, a person who is a designated person pursuant to paragraph (a) of the definition of 'financial institution' in *section 24(1)* and *section 25(1)(b)*, or who carries on the business of a cheque cashing office, shall register with the Bank.

(2) *Subsection (1)* shall not apply to a designated person that is authorised or licensed to carry on its activities by, or is registered with, the Bank under—

(*a*) an Act of the Oireachtas (other than this Act),

(*b*) a statute that was in force in Saorstát Éireann immediately before the date of the coming into operation of the Constitution and that continues in force by virtue of Article 50 of the Constitution, or

(*c*) an instrument made under an Act of the Oireachtas or a statute referred to in *paragraph (b)*.

(3) A designated person who is required to register under this section commits an offence if the person fails to do so and is liable—

(*a*) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment to a fine or imprisonment for a term not exceeding 5 years (or both).

(4) The Bank shall establish and maintain a register of persons that register under this section (referred to in this section as 'the Register').

(5) The following particulars shall be entered into the Register in respect of each designated person registered:

(*a*) the name of the designated person;

(*b*) the address of the head office and registered office of the designated person;

(*c*) the activities that the designated person carries out that are contained within the meaning of *paragraph (a)* of the definition of financial institution in *section 24(1)*.

(6) The following particulars shall be entered into the Register in respect of each person registered who carries on the business of a cheque cashing office:

(*a*) the name of the person;

(*b*) the address of the registered office of the person;

(*c*) the addresses at which the business of a cheque cashing office is carried on.

(7) The Bank may specify a procedure for registering under this section.

(8) The Register may be in book form, electronic form or such other form as the Bank may determine. The Register may be maintained in an electronic, mechanical or other non-written form only if it is capable of being reproduced in a written form.

(9) The particulars entered in the Register pursuant to this section relating to a person who is a designated person pursuant to *section 25(1)(b)* and *paragraph (a)* of the definition of financial institution in *section 24(1)* may be removed from the Register where that person ceases to be a designated person pursuant to those provisions or is authorised or licensed to carry on its activities by, or is registered with, the Bank under an enactment specified in *paragraph (a)*, *(b)* or *(c)* of *subsection (2)*.

(10) The particulars entered in the Register pursuant to this section relating to a person who carries on the business of a cheque cashing office may be removed from

the Register where that person ceases to carry on the business of a cheque cashing office or is authorised or licensed to carry on its activities by, or is registered with, the Bank under an enactment specified in *paragraph (a)*, *(b)* or *(c)* of *subsection (2)*.

(11) In this section 'Bank' means the Central Bank of Ireland.**]**

Annotations

Amendments:

F95 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 34, S.I. No. 486 of 2018.

Editorial Notes:

E45 A class A fine is defined as a fine not exceeding €5,000 (4.01.2011) by *Fines Act 2010* (8/2010), s. 3, S.I. No. 662 of 2010.

E46 The section heading is taken from the amending section in the absence of one included in the amendment.

Registration of persons directing private members' clubs.

109.— (1) A person who is a designated person pursuant to *section 25(1)(h)* shall register with the Minister in accordance with suchprocedures as may be prescribed or otherwise imposed by the Minister.

(2) A person who is required to register under this section commits an offence if the person fails to do so and is liable—

(*a*) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both), or

(*b*) on conviction on indictment to a fine or imprisonment for a term not exceeding 5 years (or both).

(3) The following particulars shall be entered into a register established and maintained by the Minister for the purposes of this section:

(*a*) the name of each designated person who registers under this section;

(*b*) the name and address of the premises of the private members' club in relation to which the person is a designated person;

(*c*) any prescribed information as may be reasonably required by the Minister for the purposes of this Act.

(4) The register may be in book form, electronic form or such other form as the Minister may determine. The register may be maintained in an electronic, mechanical or other non-written form only if it is capable of being reproduced in a written form.

(5) The Minister shall maintain the register at an office of the Department.

(6) The Minister may prescribe particulars for the purposes of *subsection (3)(c)* only if satisfied that those particulars reasonably relate to the business or regulation of persons directing members' clubs as designated persons.

F96**[**(7) The Minister may publish the register in written, electronic or other form and a member of the public is entitled to obtain a copy of the register or of an entry in the register on payment of such reasonable copying charges as may be prescribed (if any).

(8) The particulars entered in the register pursuant to this section relating to a person who is a designated person pursuant to section 25(1)(h) may be removed from

the register where that person ceases to be a designated person pursuant to that provision.**]**

Annotations

Amendments:

F96 Inserted (14.06.2013) by *Criminal Justice Act 2013* (19/2013), s. 18, S.I. No. 196 of 2013.

F97**[**Managers and beneficial owners of private members' clubs to hold certificates of fitness

109A. (1) An individual who—

(*a*) effectively directs a private members' club at which gambling activities are carried on, or

(*b*) is a beneficial owner of a private members' club at which gambling activities are carried on,

shall hold a certificate of fitness and probity (referred to in this section and *sections 109B*, *109C*, *109D* and *109E* as a 'certificate of fitness') granted by a Superintendent of the Garda Síochána or, as the case may be, by the Minister.

(2) An individual who fails to comply with *subsection (1)* commits an offence and is liable—

(a) on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months, or both, or

(b) on conviction on indictment to a fine or imprisonment for a term not exceeding 5 years, or both.

(3) Where on the date that is 6 months from the coming into force of this section an individual has applied for a certificate of fitness, this section shall not apply to that individual until such time as the application, and any appeal in relation to the application, has been finally determined.**]**

Annotations

Amendments:

F97 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 35, S.I. No. 486 of 2018.

F98**[**Application for certificate of fitness

109B. (1) Upon compliance with *subsection (2)*, an individual shall make an application for a certificate of fitness—

(*a*) where the individual ordinarily resides in the State—

(i) to the Superintendent of the Garda Síochána for the district in which he or she ordinarily resides, or

(ii) to the Superintendent of the Garda Síochána for the district in which the private members' club concerned is located or is proposed to be located,

or

(*b*) where the individual ordinarily resides outside the State, to the Minister.

(2) An individual intending to apply for a certificate of fitness under this section shall, not later than 14 days and not earlier than one month before making the

application, publish in two daily newspapers circulating in the State, a notice in such form as may be prescribed, of his or her intention to make the application.

(3) An application for a certificate of fitness under this section shall be in such form as may be prescribed.

(4) The applicant for a certificate of fitness shall provide the Superintendent of the Garda Síochána, or as the case may be, the Minister to whom the application concerned is made with all such information as he or she may reasonably require for the purposes of determining whether a relevant consideration referred to in *section 109C* exists.

(5) A Superintendent of the Garda Síochána, or as the case may be, the Minister to whom an application for a certificate of fitness is duly made under this section shall, not later than 56 days after receiving the application, either—

(*a*) grant the application and issue a certificate of fitness to the applicant, or

(*b*) refuse the application.

(6) A certificate of fitness under this section shall be in such form as may be prescribed.

(7) An individual who, in applying for a certificate of fitness under this section, makes a statement or provides information to a Superintendent of the Garda Síochána or, as the case may be, to the Minister, that he or she knows, or ought reasonably to know, is false or misleading in a material respect commits an offence and is liable—

(*a*) on summary conviction to a class A fine or imprisonment for a term not exceeding 6 months, or both, or

(*b*) on conviction on indictment to a fine not exceeding €50,000 or imprisonment for a term not exceeding 2 years, or both.

(8) A Superintendent of the Garda Síochána shall, as soon as may be after making a decision in relation to an application for a certificate of fitness, notify the Minister in writing of that decision.**]**

Annotations

Amendments:

F98 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 35, S.I. No. 486 of 2018.

Editorial Notes:

E47 A class A fine is defined as a fine not exceeding €5,000 (4.01.2011) by *Fines Act 2010* (8/2010), s. 3, S.I. No. 662 of 2010.

E48 The section heading is taken from the amending section in the absence of one included in the amendment.

F99**[**Grounds of refusal to grant certificate of fitness

109C. (1) A Superintendent of the Garda Síochána or, as the case may be, the Minister shall not refuse an application for a certificate of fitness made in accordance with *section 109B* unless—

(*a*) a relevant consideration exists, or

(*b*) he or she is not satisfied that the applicant has provided such information as he or she reasonably requires for the purposes of determining whether a relevant consideration exists.

(2) For the purposes of *subsection (1)*, a relevant consideration exists if—

(*a*) the applicant stands convicted of an offence under—

(i) an enactment relating to excise duty on betting,

(ii) the Gaming and Lotteries Acts 1956 to 2013,

(iii) section 1078 of the Taxes Consolidation Act 1997,

(iv) the Criminal Justice (Theft and Fraud Offences) Act 2001, or

(v) this Act,

(*b*) the applicant stands convicted of an offence under the law of a place (other than the State)—

(i) consisting of an act or omission that, if committed in the State, would constitute an offence referred to in *paragraph (a)*, or

(ii) relating to the conduct of gambling,

or

(*c*) the applicant was previously refused a certificate of fitness and either—

(i) the applicant did not appeal the refusal, or

(ii) on appeal to the District Court, the refusal was affirmed.

(3) In this section, 'enactment' means—

(*a*) an Act of the Oireachtas,

(*b*) a statute that was in force in Saorstát Éireann immediately before the date of the coming into operation of the Constitution and that continues in force by virtue of Article 50 of the Constitution,

(*c*) an instrument made under—

(i) an Act of the Oireachtas, or

(ii) a statute referred to in *paragraph (b)*.**]**

Annotations

Amendments:

F99 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 35, S.I. No. 486 of 2018.

Editorial Notes:

E49 The section heading is taken from the amending section in the absence of one included in the amendment.

F100[Duration of certificate of fitness

109D. (1) A certificate of fitness shall remain in force until the expiration of 3 years after the date on which the certificate was issued.

(2) If, before the expiration of a certificate of fitness, the individual to whom it was issued makes an application for a new certificate of fitness, the first-mentioned certificate of fitness shall remain in force—

(*a*) until the issue of the new certificate of fitness,

(*b*) in circumstances where the application is refused by the Superintendent of the Garda Síochána concerned or by the Minister and the individual does not make a request referred to in *section 109E(1)*, until the expiration of the period within which the request may be made,

(*c*) in circumstances where the application is refused by the Superintendent of the Garda Síochána concerned or by the Minister and the individual makes a request referred to in section *109E(1)* but does not bring an appeal under that section, until the expiration of the period specified in *subsection (3)* of that section, or

(*d*) in circumstances where the application is refused by the Superintendent of the Garda Síochána concerned or the Minister and the individual appeals the refusal in accordance with *section 109E*, until—

(i) the District Court affirms the refusal in accordance with that section, or

(ii) the issue of a new certificate of fitness pursuant to a direction of the District Court under *subsection (4)(b)* of that section.**]**

Annotations

Amendments:

F100 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 35, S.I. No. 486 of 2018.

Editorial Notes:

E50 The section heading is taken from the amending section in the absence of one included in the amendment.

F101[Appeal where application for certificate of fitness is refused

109E. (1) If a Superintendent of the Garda Síochána, or as the case may be, the Minister refuses an application for a certificate of fitness, he or she shall, on the request in writing of the applicant made not later than 14 days after the refusal, give the applicant a statement in writing of the reasons for the refusal.

(2) A person to whom a certificate of fitness has been refused may, not later than 14 days after receiving a statement in writing under *subsection (1)*, appeal the refusal to the District Court.

(3) A person who brings an appeal under this section shall, in such manner and within such period as may be prescribed give notice of the appeal to the Superintendent of the Garda Síochána concerned or, as the case may be, the Minister.

(4) The District Court may, upon an appeal under this section, either—

(*a*) affirm the refusal, or

(*b*) grant the appeal and direct the Superintendent of the Garda Síochána concerned, or as the case may be, the Minister to issue a certificate of fitness to the appellant.

(5) The Superintendent of the Garda Síochána concerned or, as the case may be, the Minister shall comply with a direction of the District Court under this section not later than 3 days after the giving of the direction.

(6) The respondent in an appeal under this section shall not be entitled to advance as a reason for opposing an appeal under this section a reason not specified in a statement of the reasons for a refusal given to the appellant pursuant to a request under *subsection (1)*.

(7) If the District Court affirms a refusal under *subsection (4)(a)*, it may also make an order requiring the appellant to pay the costs incurred by the respondent in defending the appeal and may determine the amount of such costs.

(8) There shall be no appeal to the Circuit Court from a decision of the District Court under this section.

(9) An appeal under this section by a person ordinarily resident in the State shall be brought before a judge of the District Court assigned to the District Court district—

(*a*) in which he or she ordinarily resides, or

(*b*) in which the private members' club concerned is located or is proposed to be located.

(10) An appeal under this section by a person not ordinarily resident in the State shall be brought before a judge of the District Court assigned to the Dublin Metropolitan District.**]**

Annotations

Amendments:

F101 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 35, S.I. No. 486 of 2018.

Editorial Notes:

E51 The section heading is taken from the amending section in the absence of one included in the amendment.

PART 5

Miscellaneous

Service of documents.

110.— (1) A notice or other document that is required or permitted, under this Act, to be served on or given to a person shall be addressed to the person by name and may be served or given to the person in one of the following ways:

(*a*) by delivering it to the person;

(*b*) by leaving it at the address at which the person ordinarily resides or carries on business;

(*c*) by sending it by post in a pre-paid registered letter to the address at which the person ordinarily resides or carries on business;

(*d*) if an address for service has been furnished, by leaving it at, or sending it by post in a pre-paid registered letter to, that address;

(*e*) in the case of a direction to an individual or body (whether incorporated or unincorporated) under *Part 3* not to carry out any specified service or transaction at a branch or place of business of the body or individual, by leaving it at, or by sending it by post in a pre-paid registered letter to, the address of the branch or place of business (as the case may be);

(*f*) if the person giving notice considers that notice should be given immediately and a fax machine is located at an address referred to in *paragraph (b)*, *(c)*, *(d)* or *(e)*, by sending it by fax to that machine, but only if the sender's fax machine generates a message confirming successful transmission of the total number of pages of the notice.

(2) For the purposes of this section—

(*a*) a company registered under the Companies Acts is taken to be ordinarily resident at its registered office, and

(*b*) any body corporate other than a company registered under the Companies Acts or any unincorporated body is taken to be ordinarily resident at its principal office or place of business in the State.

(3) Nothing in *subsection (1)(e)* prevents the serving or giving of a direction or other document for the purposes of *Part 3* under any other provision of this section.

(4) This section is without prejudice to any mode of service or of giving a notice or any other document provided for under any other enactment or rule of law.

(5) This section does not apply in relation to the service of a notice on the Minister referred to in *section 100 (2)*.

Offences — directors and others of bodies corporate and unincorporated bodies.

111.— Where an offence under this Act is committed by a body corporate or by a person purporting to act on behalf of a body corporate or on behalf of an unincorporated body of persons, and is proved to have been committed with the consent or connivance, or to be attributable to any wilful neglect, of a person who, when the offence is committed, is—

(*a*) a director, manager, secretary or other officer of the body, or a person purporting to act in that capacity, or

(*b*) a member of the committee of management or other controlling authority of the body, or a person purporting to act in that capacity,

that person is taken to have also committed the offence and may be proceeded against and punished accordingly.

Disclosure of information in good faith.

112.— (1) This section applies to the disclosure in good faith, to a member of the Garda Síochána or to any person who is concerned in the investigation or prosecution of an offence of money laundering or terrorist financing, of—

(*a*) a suspicion that any property has been obtained in connection with any such offence, or derives from property so obtained, or

(*b*) any matter on which such a suspicion is based.

(2) A disclosure to which this section applies shall not be treated, for any purpose, as a breach of any restriction on the disclosure of information imposed by any other enactment or rule of law.

Amendment of Bail Act 1997.

113.— The Schedule to the Bail Act 1997 is amended by inserting the following paragraph after paragraph 34 (inserted by section 48 of the Criminal Justice (Miscellaneous Provisions) Act 2009):

"*Money Laundering.*

35. Any offence under *Part 2* of the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010*.".

Amendment of Central Bank Act 1942.

114.— (1) In this section, "Act of 1942" means the Central Bank Act 1942.

(2) Section 33AK(5) (inserted by section 26 of the Central Bank and Financial Services Authority of Ireland Act 2003) of the Act of 1942 is amended by deleting paragraph (*n*).

(3) The Act of 1942 is amended by inserting the following after section 33AN (inserted by section 10 of the Central Bank and Financial Services Authority of Ireland Act 2004):

"Application of Part to credit unions.

33ANA.— (1) This Part applies in relation to—

(*a*) the commission or suspected commission by a credit union of a contravention of—

(i) a provision of *Part 4* of the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010*,

(ii) any direction given to the credit union under a provision of *Part 4* of that Act,

(iii) any condition or requirement imposed on the credit union under a provision of *Part 4* of that Act or under any direction given to the credit union under a provision of that Part, or

(iv) any obligation imposed on the credit union by this Part or imposed by the Regulatory Authority pursuant to a power exercised under this Part,

and

(*b*) participation, by a person concerned in the management of a credit union, in the commission by the credit union of such a contravention.

(2) For those purposes—

(*a*) a reference in this Part to a regulated financial service provider includes a reference to a credit union,

(*b*) a reference in this Part to a prescribed contravention includes a reference to a contravention, by a credit union, of a provision, direction, condition, requirement or obligation referred to in subsection (1), and

(*c*) a reference in this Part to a person concerned in the management of a regulated financial service provider includes a reference to a person concerned in the management of a credit union.

(3) Nothing in this section limits the application of this Part in relation to matters other than those referred to in subsection (1).

(4) This section has effect notwithstanding anything to the contrary in section 184 of the Credit Union Act 1997.".

(4) Schedule 2 (substituted by section 31 of the Central Bank and Financial Services Authority of Ireland Act 2003) to the Act of 1942 is amended in Part 1 by inserting the following at the end of the Part:

"

No. __ of 2010	*Criminal Justice (Money Laundering and Terrorist Financing) Act 2010*	*Part 4*

".

F102[Prescribed amounts under section 33AQ of Central Bank Act 1942 in respect of certain contraventions

114A. (1) In this section 'Act of 1942' means the Central Bank Act 1942 and 'designated person' means a designated person within the meaning of Part 4.

(2) Notwithstanding subsection (4) of section 33AQ of the Act of 1942, in the case of a contravention of *Chapter 3*, *4* or *6* of *Part 4*, or *section 30B*, *57*, *57A*, *58* or *59*, by a designated person, the prescribed amount for the purpose of subsection (3)(c) of section 33AQ is—

(a) if the designated person is a body corporate or an unincorporated body, the greatest of—

(i) €10,000,000,

(ii) twice the amount of any benefit derived by the person from the contravention (where that benefit can be determined), and

(iii) an amount equal to 10 per cent of the turnover of the body for its last complete financial year before the finding is made,

(b) if the designated person is a natural person—

(i) where the designated person is not a credit institution or financial institution, the greater of—

(I) €1,000,000, and

(II) twice the amount of any benefit derived by the person from the contravention (where that benefit can be determined),

(ii) where the designated person is a credit institution or financial institution, the greater of—

(I) €5,000,000, and

(II) twice the amount of any benefit derived by the person from the contravention (where that benefit can be determined).

(3) Notwithstanding subsection (6) of section 33AQ of the Act of 1942, in the case of a contravention of *Chapter 3*, *4* or *6* of *Part 4*, or *section 30B*, *57*, *57A*, *58* or *59*, by a designated person, the prescribed amount for the purpose of subsection (5)(b) of section 33AQ is—

(a) where the designated person is not a credit institution or financial institution, the greater of—

(i) €1,000,000, and

(ii) twice the amount of any benefit derived by the person from the contravention (where that benefit can be determined),

(b) where the designated person is a credit institution or financial institution, the greater of—

(i) €5,000,000, and

(ii) twice the amount of any benefit derived by the person from the contravention (where that benefit can be determined).

(4) For the purposes of *subsection (2)(a)(iii)*, 'turnover of the body' means total annual turnover of the designated person according to the latest available accounts approved by the management body of the designated person or, where the designated person 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[12], 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.**]**

Annotations

Amendments:

F102 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 36, S.I. No. 486 of 2018.

Editorial Notes:

E52 The section heading is taken from the amending section in the absence of one included in the amendment.

Amendment of Courts (Supplemental Provisions) Act 1961.

115.— Section 32A(1) of the Courts (Supplemental Provisions) Act 1961 (inserted by section 180 of the Criminal Justice Act 2006) is amended as follows:

(*a*) in paragraph (*d*) (inserted by section 18 of the Criminal Justice (Surveillance) Act 2009) by substituting "Criminal Justice (Surveillance) Act 2009;" for "Criminal Justice (Surveillance) Act 2009.";

(*b*) by inserting the following paragraph after paragraph (*d*):

"(*e*) any of the following powers under *Part 3* of the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010*:

(i) the power to order a person not to carry out any service or transaction;

(ii) the power to revoke an order referred to in subparagraph (i);

(iii) the power to make an order in relation to property if considered essential to do so for the purpose of enabling—

(I) the person who applies for the order to discharge the reasonable living and other necessary expenses incurred or to be incurred in respect of the person or the person's dependants, or

(II) the person who applies for the order to carry on a business, trade, profession or other occupation to which any of the property relates.".

Consequential amendment of Central Bank Act 1997.

116.— Section 28 (substituted by section 27 of the Central Bank and Financial Services Authority of Ireland Act 2004) of the Central Bank Act 1997 is amended, in the definitions of "bureau de change business" and "money transmission service", by substituting the following for paragraphs (*a*) and (*b*) of those definitions:

"(*a*) by a person or body that is required to be licensed, registered or otherwise authorised by the Bank under a designated enactment (other than under this Part) or designated statutory instrument, or".

[12] OJ No. L 182, 29.6.2013, p. 19

Consequential amendment of Criminal Justice Act 1994.

117.— (1) In this section, "Act of 1994" means the Criminal Justice Act 1994.

(2) Section 3(1) of the Act of 1994 is amended in the definition of "drug trafficking" by substituting the following for paragraph (*d*):

"(*d*) engaging in any conduct (whether or not in the State) in relation to property obtained, whether directly or indirectly, from anything done in relation to a controlled drug, being conduct that—

(i) is an offence under *Part 2* of the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010* ("*Part 2* of the *Act of 2010*") or would have been an offence under that Part if the Part had been in operation at the time when the conduct was engaged in, or

(ii) in the case of conduct in a place outside of the State, other than conduct referred to in subparagraph (i)—

(I) would be an offence under *Part 2* of the *Act of 2010* if done in corresponding circumstances in the State, or

(II) would have been an offence under that Part if done in corresponding circumstances in the State and if the Part had been in operation at the time when the conduct was engaged in, or".

(3) Section 3(1) of the Act of 1994 is amended in the definition of "drug trafficking offence" by substituting the following for paragraph (*e*):

"(*e*) an offence under *Part 2* of the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010*, or under section 31 of this Act (as in force before the commencement of that Part), in relation to the proceeds of drug trafficking,".

Consequential amendment of Criminal Justice (Mutual Assistance) Act 2008.

118.— Section 94(3) of the Criminal Justice (Mutual Assistance) Act 2008 is amended by substituting "*Part 2* of the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010*" for "section 31 of the Criminal Justice Act 1994, as substituted by section 21 of the Criminal Justice (Theft and Fraud Offences) Act 2001".

Consequential amendment of Criminal Justice (Theft and Fraud Offences) Act 2001.

119.— Section 40(1) of the Criminal Justice (Theft and Fraud Offences) Act 2001 is amended by substituting the following for the definition of "money laundering":

"'money laundering' means an offence under *Part 2* of the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010*;".

Consequential amendment of Investor Compensation Act 1998.

120.— (1) In this section, "Act of 1998" means the Investor Compensation Act 1998.

(2) Section 30(1) of the Act of 1998 is amended in the definition of "net loss" by substituting the following for subparagraph (iii):

"(iii) money or investment instruments arising out of transactions in respect of which an offence has been committed under the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010* (" Act of 2010 "),

(iv) money or investment instruments arising out of transactions in respect of which an offence has been committed under a provision of Part IV of the Criminal Justice Act 1994 prior to the repeal of that provision by the *Act of 2010*,

(v) money or investment instruments arising out of transactions in respect of which an offence has been committed under a provision of section 57 or 58 of the Criminal Justice Act 1994 prior to the repeal of that provision by the *Act of 2010*, or

(vi) money or investment instruments arising out of transactions in respect of which there has been a criminal conviction, at any time, for money laundering, within the meaning of 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 [12].".

(3) Section 35 of the Act of 1998 is amended by substituting the following for subsection (3):

"(3) Notwithstanding the time limits provided for in subsections (1) and (2), the competent authority may direct the Company or a compensation scheme approved under section 25, as appropriate, to suspend any payment to an eligible investor, where the investor has been charged with any of the following offences, pending the judgment of a court in respect of the charge:

(*a*) an offence under the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010* (" Act of 2010");

(*b*) an offence committed, prior to the repeal by the *Act of 2010* of any of the following provisions of the Criminal Justice Act 1994, under that provision:

(i) a provision of Part IV;

(ii) section 57;

(iii) section 58;

(*c*) an offence otherwise arising out of, or relating to, money laundering, within the meaning of 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 [13].".

Consequential amendment of Taxes Consolidation Act 1997.

121.— (1) In this section, "Act of 1997" means the Taxes Consolidation Act 1997.

(2) Section 898F (substituted by section 90 of, and Schedule 4 to, the Finance Act 2004) of the Act of 1997 is amended as follows:

(*a*) in subsection (3) by substituting "which is acceptable for the purposes of *Chapter 3* of *Part 4* of the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010*" for "it acquires by virtue of section 32 of the Criminal Justice Act 1994";

(*b*) in subsection (4) by substituting "which is acceptable for the purposes of *Chapter 3* of *Part 4* of the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010*" for "it acquires by virtue of section 32 of the Criminal Justice Act 1994";

(*c*) in subsection (5)(*a*) (substituted by section 124(1)(*a*) of the Finance Act 2006) by inserting "(or has done so, before the relevant commencement date, in accordance with this section as in force before that date)" after "in accordance with this section";

(*d*) by inserting the following paragraph after subsection (6)(*a*):

"(*aa*) A paying agent who—

[12] OJ L 309, 25.11.2005, p.15

[13] OJ L 309, 25.11.2005, p.15

(i) before the relevant commencement date, established the identity and residence of an individual under this section as in force before that date, and

(ii) was required, immediately before the relevant commencement date and as a result of paragraph (*a*), to continue to treat that individual as so identified and so resident,

shall continue to treat that individual as so identified and so resident until such time as the paying agent is in possession, or aware, of information which can reasonably be taken to indicate that the individual has been incorrectly identified or is not so resident or has changed his or her residence.";

(*e*) in subsection (6)(*b*) by inserting "or (*aa*)" after "paragraph (*a*)";

(*f*) in subsection (7) by inserting "(or as established, before the relevant commencement date, in accordance with this section as in force before that date)" after "this section";

(*g*) by inserting the following subsection after subsection (7):

"(8) In this section, 'relevant commencement date' means the date on which *section 121(2)* of the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010* comes into operation.".

(3) Section 898G (substituted by section 90 of, and Schedule 4 to, the Finance Act 2004) of the Act of 1997 is amended as follows:

(*a*) in subsection (2) by substituting "*Chapter 3* of *Part 4* of the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010*" for "section 32 of the Criminal Justice Act 1994";

(*b*) in subsection (4)(*b*) by substituting "*Chapter 3* of *Part 4* of the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010*" for "section 32 of the Criminal Justice Act 1994";

(*c*) in subsection (5)(*b*)(iii) by substituting "*Chapter 3* of *Part 4* of the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010*" for "section 32 of the Criminal Justice Act 1994";

(*d*) in subsection (6)(*a*) (substituted by section 124(1)(*b*) of the Finance Act 2006) by inserting "(or has done so, before the relevant commencement date, in accordance with this section as in force before that date)" after "in accordance with this section";

(*e*) by inserting the following paragraph after subsection (8)(*a*):

"(*aa*) A paying agent who—

(i) before the relevant commencement date, established the identity and residence of an individual under this section as in force before that date, and

(ii) was required, immediately before the relevant commencement date and as a result of paragraph (*a*), to continue to treat that individual as so identified and so resident,

shall continue to treat that individual as so identified and so resident until such time as the paying agent is in possession, or aware, of information which can reasonably be taken to indicate that the individual has been incorrectly identified or is not so resident or has changed his or her residence.";

(*f*) in subsection (8)(*b*) by inserting "or (*aa*)" after "paragraph (*a*)";

(*g*) in subsection (9) by inserting "(or as established, before the relevant commencement date, in accordance with this section as in force before that date)" after "this section";

(*h*) by inserting the following subsection after subsection (9):

"(10) In this section, ' relevant commencement date' means the date on which *section 121 (3)* of the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010* comes into operation.".

Consequential amendment of Taxi Regulation Act 2003.

122.— Section 36(1)(*f*) of the Taxi Regulation Act 2003 is amended by substituting "*Part 2* of the *Criminal Justice (Money Laundering and Terrorist Financing) Act 2010*" for "Part IV of the Criminal Justice Act 1994".

Section 4.

SCHEDULE 1

REVOCATIONS OF STATUTORY INSTRUMENTS

Title of Instrument (1)	Number and Year (2)	Extent of Revocation (3)
Criminal Justice Act 1994 (Section 32(10)(*a*)) Regulations 1995	S.I. No. 104 of 1995	The whole Regulations.
Criminal Justice Act 1994 (Section 32(10)(*b*)) Regulations 1995	S.I. No. 105 of 1995	The whole Regulations.
Criminal Justice Act 1994 (Section 32(10)(*d*)) Regulations 1995	S.I. No. 106 of 1995	The whole Regulations.
Criminal Justice Act 1994 (Section 32(10)(*b*)) (No. 2) Regulations 1995	S.I. No. 324 of 1995	The whole Regulations.
Criminal Justice Act 1994 (Section 32(10)(*a*)) Regulations 2003	S.I. No. 216 of 2003	The whole Regulations.
Criminal Justice Act 1994 (Section 32) Regulations 2003	S.I. No. 242 of 2003	The whole Regulations.
Criminal Justice Act 1994 (Section 32) (Amendment) Regulations 2003	S.I. No. 416 of 2003	The whole Regulations.
Criminal Justice Act 1994 (Section 32) (Prescribed States or Countries) Regulations 2003	S.I. No. 618 of 2003	The whole Regulations.
Criminal Justice Act 1994 (Section 32) (Prescribed Activities) Regulations 2004	S.I. No. 3 of 2004	The whole Regulations.
Criminal Justice Act 1994 (Section 32) (Prescribed States or Countries) Regulations 2004	S.I. No. 569 of 2004	The whole Regulations.

Section 24.

F103[SCHEDULE 2

ANNEX I TO DIRECTIVE 2013/36/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 26 JUNE 2013[13] 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

LIST OF ACTIVITIES SUBJECT TO MUTUAL RECOGNITION

[13] OJ No. L 176, 27.6.2013, p. 338

1. Taking deposits and other repayable funds.

2. Lending including *inter alia*: consumer credit, credit agreements relating to immovable property, factoring, with or without recourse, financing of commercial transactions (including forfeiting).

3. Financial leasing.

4. Payment services as defined in Article 4(3) of Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007[14] 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.

5. Issuing and administering other means of payment (e.g. travellers' cheques and bankers' drafts) insofar as such activity is not covered by point 4.

6. Guarantees and commitments.

7. Trading for own account or for account of customers in any of the following:

(*a*) money market instruments (cheques, bills, certificates of deposit, etc.);

(*b*) foreign exchange;

(*c*) financial futures and options;

(*d*) exchange and interest-rate instruments;

(*e*) transferable securities.

8. Participation in securities issues and the provision of services relating to such issues.

9. Advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertakings.

10. Money broking.

11. Portfolio management and advice.

12. Safekeeping and administration of securities.

13. Credit reference services.

14. Safe custody services.

15. Issuing electronic money.

The services and activities provided for in Sections A and B of Annex I to Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004[15] on markets in financial instruments, when referring to the financial instruments provided for in Section C of Annex I of that Directive, are subject to mutual recognition in accordance with Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013[16].**]**

[14] OJ No. L 319, 5.12.2007, p. 1
[15] OJ No. L 145, 30.4.2004, p. 1
[16] OJ No. L 176, 27.6.2013, p. 338

Annotations

Amendments:

F103 Substituted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 37, S.I. No. 486 of 2018.

Section 34A

F104[SCHEDULE 3

NON-EXHAUSTIVE LIST OF FACTORS SUGGESTING POTENTIALLY LOWER RISK

(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 *subparagraph (3)*.

(2) Product, service, transaction or delivery channel risk factors:

(*a*) life assurance 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 anti-money laundering (AML) or combating financing of terrorism (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 Financial Action Task Force (FATF) recommendations and effectively implement these requirements.**]**

Annotations

Amendments:

F104 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 38, S.I. No. 486 of 2018.

Section 39

F105**[**SCHEDULE 4

NON-EXHAUSTIVE LIST OF FACTORS SUGGESTING POTENTIALLY HIGHER RISK

(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 *subparagraph (3)*;

(*c*) non-resident customers;

(*d*) legal persons or arrangements that are personal asset-holding vehicles;

(*e*) companies that have nominee shareholders or shares in bearer form;

(*f*) businesses that are cash intensive;

(*g*) 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;

(*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*) 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 organisations such as, for example, the European Union or the United Nations;

(*d*) countries (or geographical areas) providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.**]**

Annotations

Amendments:

F105 Inserted (26.11.2018) by *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018* (26/2018), s. 39, S.I. No. 486 of 2018.

Disclaimer Note: the suggested responses supplied in this sample "Firm Business Risk Assessment" is just that, suggestions and is not intended to be taken as a response to all firms and their circumstances. In all cases the firm responses should be tailored to the specifics of their firm.

Firm Business Risk Assessment – OMNIPRO Accountants & Co

The MLRO should engage with the staff and partners of the firm to ensure risk factors appropriate to the clients of the firm are considered. Also the MLRO should consider factors identified in the risk assessment undertaken by the firm's Institute for AML regulation purposes and also the National Risk Assessment.

Firm Name	OMNIPRO Accountants & Co
Firm Type	Sole partnership firm
No of Clients of Firm	400 Approximately
Risk Review Date	XX MM YYYY

		Y/N	Risk Consideration	Action Comment
The Firm				
1.	Has the firm introduced AML procedures?	Y	Low Risk	The firm has had previous AML procedures in place since 2013 and now has updated to reflect the requirements of the 2018 revisions to the Criminal Justice Act of 2010 (CJA 2010 (revised))
		Y	Medium Risk	The firm has only adopted AML procedure during 2019 following the implementation of the 2018 revisions to the Criminal Justice Act of 2010
2.	Has the firm appointed a MLRO?	Y	Low Risk	The firm has appointed XXXXXX as the MLRO
		Y	Low Risk	No the firm has not appointed an MLRO as the firm requirements under CJA 2010 (revised) has been split between XXXXX being a person of Senior Management who is responsible for the implementation of AML within the Firm and XXXXX as the Compliance Officer of the firm being a management person of the firm.
3.	Does the Firm or its Partners provide any specialised services or focused industry specialism's?	N	Low risk	The Firm only provides standard bookkeeping, accountancy, tax advisory and audit services to clients
		Y	Medium Risk	The firm provides

Disclaimer Note: the suggested responses supplied in this sample "Firm Business Risk Assessment" is just that, suggestions and is not intended to be taken as a response to all firms and their circumstances. In all cases the firm responses should be tailored to the specifics of their firm.

			High Risk	The firm provides the following specialised services for some clients which other than the standard service results in a higher risk to AML compliance of the firm (specify the service XXXX)
4.	Has all staff received initial training?	Y	Low Risk	All staff trained annually. Staff training completed in 2019 on roll out in relation to new procedures
		Y	Medium Risk	Staff have been provided training in previous years but have not been provided with up to date training on the requirements of CJA 2010(revised); **OR** The staff training has been training provided on XX DATE however the new staff entered into the firm since this date have not been provided training in relation to the firms obligations under CJA 2010 (revised)
		N	High Risk	The firm has not yet provided training to staff in relation to its money laundering and terrorist financing obligations which will facilitate the ongoing monitoring of the client relationship and identification of suspicious transactions
5.	Do new staff receive training on commencement of employment with the firm?	Y	Low risk	No new staff joined the firm **OR** New staff having entered the firm have been provided training, **OR** the new staff having entered the firm are not engaged in liaising or providing services to the clients of the firm therefore they do not need to be provided training
		N	Medium Risk	New staff having entered into the firm have not been provided on entry into the firm but will be provided

Disclaimer Note: the suggested responses supplied in this sample "Firm Business Risk Assessment" is just that, suggestions and is not intended to be taken as a response to all firms and their circumstances. In all cases the firm responses should be tailored to the specifics of their firm.

				training on the next round of annual training to staff
6.	Is there evidence of training?	Y	Low Risk	The firm maintains a training log of AML training provided which is maintained at Appendix 9
		N	Medium Risk	The firm does not maintain a record of the training provided but this will be addressed by maintaining an attendance log at the next annual training provided
The Customers / Clients				
1.	Are all clients known to the firm or if new has there ever been a history of difficulty in verifying identification?	Y	Low risk	All clients are known to the firm, have been met in person and ID's obtained.
		N	Medium Risk	The firm has not met all clients as some are referred to them from existing overseas clients through the firm's Networking Group and Organisation and the firm has relied on third party verification by the Network firm of that clients location
2.	Are the beneficial owners know in all cases?	Y	Low risk	Beneficial owners are known for all clients
		N	Medium Risk	The firm has been able to identify all beneficial owners in all cases with the exception of one client which information and responses are currently requested from the client on.
		N	High Risk	The firm has been unable to identify the beneficial owners for a number of clients for the following reasons [State reasons]
3.	Do the clients maintain proper books and records?	Y	Low risk	For all clients of the firm, basic books and records are maintained
		N	Low Risk	In general most clients of the firm maintain basic books and records,

Disclaimer Note: the suggested responses supplied in this sample "Firm Business Risk Assessment" is just that, suggestions and is not intended to be taken as a response to all firms and their circumstances. In all cases the firm responses should be tailored to the specifics of their firm.

				however some clients have become late filing and or have resulted in strike off due to poor record maintenance accordingly the client has been reported to the ODCE but the risk to AML is low as the reasons for poor records is known
4.	Are any of the clients of the firm politically exposed individuals?	N Y	Low risk High Risk	No clients of the firm are identified as PEPs[1] The firm has a PEP in the form of a [TD / High court Judge] and accordingly for that specific client enhanced due diligence will be performed by the firm and ongoing monitoring of the client relationship

[1] A PEP is an individual who is or, has been entrusted with prominent public functions, or an immediate family member, or a known close associate of such a person. The definition includes persons holding a prominent position in European Union and international bodies such as the UN, World Bank or IMF. Examples of PEPs include:

- Heads of state, heads of government, ministers and deputy or assistant ministers;
- Members of parliaments or head of governing body of a political body;
- Members of supreme courts, of constitutional courts or of other high level judicial bodies;
- Members of courts of auditors or of the boards of Central Banks;
- Ambassadors, charges d'affaires and high-ranking officers in the armed forces, and
- Members of the administrative, management or supervisory boards of State-owned enterprises.

Disclaimer Note: the suggested responses supplied in this sample "Firm Business Risk Assessment" is just that, suggestions and is not intended to be taken as a response to all firms and their circumstances. In all cases the firm responses should be tailored to the specifics of their firm.

5.	Do any clients demonstrate;			
	- frequent changes in accountants, auditors or other financial advisors;	N	Low Risk	All clients are long standing clients of the firm or have come to the firm through referrals while some have come from previous accountants professional clearance has been sought and provided by the previous accountant
		Y	Medium Risk	While the majority of clients are long standing clients of the firm some have come from previous accountants professional clearance has been sought and some cases provided by the previous accountant. In small number of clients professional clearance while sought no response has been provided by the previous accountant and accordingly the firm will ensure the business relationship is more frequently reviewed until such time as the firm is satisfied the relationship if low risk
	- a focus attention on anonymity and secrecy	N	Low risk	All clients are known to the firm
		Y	Medium Risk	While all clients are known to the firm, one client has been referred through the firms network group and the client has not been met in person but is a high profile public individual who wishes to ensure anonymity of their activities. Due to this the firm will ensure ongoing monitoring of the relationship and staff will be made aware of identifying suspicious activities, while the individual may wish to ensure their business dealing are secret the firm shall ensure it knows the nature and purpose of transactions

Disclaimer Note: the suggested responses supplied in this sample "Firm Business Risk Assessment" is just that, suggestions and is not intended to be taken as a response to all firms and their circumstances. In all cases the firm responses should be tailored to the specifics of their firm.

	- frequent unexplained foreign travel to higher risk countries or frequent expensive foreign travel with no explanation of purpose	N	Low risk	To the firms knowledge and from discussions with client, there are no trips to higher risk weak AML countries and all travel is explained and accounted for accordingly as family holidays, recreational or supported business trips
		Y	Medium Risk	One client acquires products and resources from a country of heightened AML Risk as a result transactions and travel happens to this location, while this is as part of the business, the firm will review these transactions in the course of the clients work in more detail to understand their business purpose with sufficient support to ensure there is no higher risk to AML
	- Unusual business activity that is not supported (i.e. high turnover for the size of business) -	N	Low risk	There is no identifiable unexplained high turnover of the clients or whose business activity is not understood by the firm
	- Operate in significant levels of cash	N	Low risk	There is no business/ client which works in un supported cash transactions of a significant volume. Those which handle cash have basic level controls are the handling of cash
		Y	Medium Risk	Due to the nature of some clients business (such as takeaway's, supermarkets, publicans, taxi's), larger levels of cash is held or transacted accordingly the Firm in the course of the clients work in more detail to understand their business purpose with sufficient support to ensure there is no higher risk to AML

Disclaimer Note: the suggested responses supplied in this sample "Firm Business Risk Assessment" is just that, suggestions and is not intended to be taken as a response to all firms and their circumstances. In all cases the firm responses should be tailored to the specifics of their firm.

	- An above normal focus on avoiding tax or reducing payments of tax	N Y	Low risk Medium Risk	No single client can be said to be any more focused than usual on their reduction of tax One client has been previous the subject of a revenue investigation in which they were found incorrectly applying VAT and supplying supporting evidence for VAT claims, the client is proactively trying to reduce tax payments, accordingly the firm will monitor the ongoing relationship and the nature of transactions with the client for the susceptibility of heighted AML Risk, other than this client all other clients can be said to be no more focused than usual on their reduction of tax
6.	Does the firm act for Offshore trusts and/or companies	N Y Y	Low risk Low risk Medium Risk	The firm has no offshore clients While the firm does act for Offshore trusts and/or companies, the beneficial owners and intended purpose of the Trust/Company is known The firm does act for Offshore trusts and/or companies and due to nature of the transactions and the structure types the firm will monitor the relationship and transactions in more detail in the performance of the work with client
The Products and Services				
1.	Does the firm provide any higher risk services that exposes the firm through the provision of that service to a higher susceptibility to criminal activity by extension of the	N	Low risk	No higher risk services provided

Disclaimer Note: the suggested responses supplied in this sample "Firm Business Risk Assessment" is just that, suggestions and is not intended to be taken as a response to all firms and their circumstances. In all cases the firm responses should be tailored to the specifics of their firm.

	information provided by the client and its by the firm (i.e. Personal Insolvency, holding of client moneys, acting as a trustee).			
2.	Do any clients require transactions be reported in a particular way for the purposes of facilitating tax arrangements?	N Y	Low risk Medium Risk	No clients require transactions be treated in a particular manner **OR** the majority of clients do not require transactions be treated in a particular manner however one or two do, but the rational and intended business purpose for this treatment is known to the firm The firm has a specific client which requires particular type of transactions be reported in a particular way which is not in the understanding of how these types of transactions should be treated, the client has been made aware of this but continues to request they be recorded in this manner, accordingly the firm will continue to monitor the relationship and transactions for suspicious activity other than this client no other clients require transactions be treated in a particular manner
Geographic Location				
1.	Are any clients or there beneficial owners located in a higher risk jurisdiction with non-compatible AML compliance requirements?	N Y	Low risk High Risk	There are no identified clients or beneficial owners of clients located in higher risk jurisdictions. The firm has identified one client/Beneficial owner which is located in XXXX which has been determined as higher AML risk jurisdiction, the firm has reviewed the EU Sanctions list and ensured the client is not on it, however by the

Disclaimer Note: the suggested responses supplied in this sample "Firm Business Risk Assessment" is just that, suggestions and is not intended to be taken as a response to all firms and their circumstances. In all cases the firm responses should be tailored to the specifics of their firm.

				nature of the location the firm will continue to apply enhanced due diligence to that specific client
2.	Do any clients:			
	- Transaction in jurisdictions which are higher risk locations or on the EU Sanctions List - Receive large amounts from overseas which are matched by payments out to other overseas countries that the client could be perceived as a facilitator	N Y	Low risk High Risk	While some clients are in receipt of income from abroad it is done in the normal course of business and is not from a location of higher risk or from the EU Sanctions list The firm has identified one client acquires products and resources from a sister company located in a country of heightened AML Risk as a result transactions and travel happens to this location, while this is as part of the business, the firm will review these transactions in the course of the clients work given the significant level of transactions in more detail to understand their business purpose with sufficient support to ensure there is no higher risk to AML
3.	Is the firm reliant on any third party verifier (agent) for Customer Due Diligence not based in the EU or location with similar AML compliance requirements.	N Y	Low risk High Risk	The firm has verified all customers and is not reliant on any third party verifications The firm has identified one client/Beneficial owner which the firm is reliant on third party verification from XXXX which has been determined as higher AML risk jurisdiction, the firm has reviewed the EU Sanctions list and ensured the client is not on it, however by the nature of the location of the client and third party verifier the firm will continue to apply enhanced due diligence to that specific client
Delivery Channels				

Disclaimer Note: the suggested responses supplied in this sample "Firm Business Risk Assessment" is just that, suggestions and is not intended to be taken as a response to all firms and their circumstances. In all cases the firm responses should be tailored to the specifics of their firm.

1.	Have any client not been met face to face?	Y N	Low risk Medium Risk	All clients are known to the firm, have been met in person and ID's obtained. The firm has not met all clients as some are referred to them from existing overseas clients through the firm's Networking Group and Organisation and the firm has relied on third party verification by the Network firm of that clients location **OR** The firm maintains an online portal via its website that it does not need to meet clients, while ID's are obtained and due diligence procedures applied the firm will perform a more frequent review of the business relationship and transactions for these clients
2.	Where services and client interaction is done using online or electronic methods is the client at least met once per year in person?	Y N	Low risk Medium Risk	Clients may supply responses and supporting information by email but are met at lease once a year by a representative of the firm The firm maintains an online portal via its website that it does not need to meet clients, while ID's are obtained and due diligence procedures applied the firm will perform a more frequent review of the business relationship and transactions for these clients
3.	Does any client travel significant distances to use the firm's services without commercial justification	N	Low risk	All clients are within the ROI and are no more than half a days travel to the firm **OR** The firm has overseas clients which is referred to it from its network group and or existing clients and this is the basis of long distance, and the firm is

Disclaimer Note: the suggested responses supplied in this sample "Firm Business Risk Assessment" is just that, suggestions and is not intended to be taken as a response to all firms and their circumstances. In all cases the firm responses should be tailored to the specifics of their firm.

				knowledgeable in the reason for the business relationship with the client and services being provided
Office Transactions				
1.	Is the firm income from local or national clients?	Y N	Low risk Low Risk	The firms income is from local and Irish registered businesses The has a foreign parent of a newly established company for which it is providing services and in receipt of money for the services being provided from that foreign parent
2.	Is the money received for the settlement of fees paid from Irish based bank accounts or from another EU based institution where the clients, parent or beneficial owner transacts from?	Y	Low risk	All clients of the firm only make payments from their ROI bank accounts to the firm **OR** Some clients of the firm maintain overseas bank accounts for the business activities in that location and other than making payments due to the cashflow, the money received by the firm is from the ROI accounts. For all other clients money is received from ROI accounts
3.	Do any clients of the firm try to pay for services using cash, prepaid cards virtual currencies or other alternative means?	N	Low risk	The firm does not receive cash or virtual cash in lieu of services provided and clients are made aware of this.
Client Money Account Transactions		N/a		The firm does not operate a client monies account
1.	Does the firm operate client monies bank accounts?	N	Low risk	
2.	In operating client money bank accounts does the client: - Want to use the firm's client account in instead of a bank account in their or their business's name - Have significant funds for investment for which	N	Low risk	

Disclaimer Note: the suggested responses supplied in this sample "Firm Business Risk Assessment" is just that, suggestions and is not intended to be taken as a response to all firms and their circumstances. In all cases the firm responses should be tailored to the specifics of their firm.

	there is no clear source of those funds or is willing to accept higher risk and lower return than the industry sector norms when investing			
3.	Were any clients introduced by a third party and want the firm to hold large sums of money	N	Low risk	
Any Other Factors				

Accountant's Resource Center

AML Guidance Manual

OMNIPRO
Let Your Expertise Benefit From Ours

OmniPro – Anti Money Laundering Guidance

DISCLAIMER

THE FOLLOWING GUIDANCE MATERIAL IS BASED ON THE CRIMINAL JUSTICE (MONEY LAUNDERING AND TERRORIST FINANCING) ACT 2010[1] AS REVISED AND UPDATED ON THE 14 NOVEMBER 2018 AND IS OMNIPRO'S INTERPRETATION OF THAT LEGISLATION, IN CONJUNCTION WITH THE REQUIREMENTS OF YOUR SUPERVISORY BODY. IT DOES NOT PURPORT TO GIVE DEFINITIVE PROFESSIONAL ADVICE IN ANY FORM. IT SHOULD, ACCORDINGLY, NOT BE RELIED UPON AS SUCH.

DESPITE TAKING EVERY CARE IN THE PREPARATION OF THIS DOCUMENT OMNIPRO DOES NOT GUARANTEE THE ACCURACY OR VERACITY OF ANY INFORMATION OR OPINION, OR THE APPROPRIATENESS, SUITABILITY OR APPLICABILITY OF ANY PRACTICE OR PROCEDURE CONTAINED THEREIN. THIS GUIDANCE SHOULD BE READ IN CONJUNCTION WITH, AND NOT AS A SUBSTITUTE FOR, THE LEGISLATION.

OMNIPRO DOES NOT TAKE ANY LEGAL RESPONSIBILITY FOR THE CONTENTS OF THIS MANUAL AND THE CONSEQUENCES THAT MAY ARISE DUE TO ANY ERRORS OR OMISSIONS. OMNIPRO SHALL THEREFORE NOT BE LIABLE FOR ANY DAMAGE OR ECONOMIC LOSS OCCASIONED TO ANY PERSON ACTING ON, OR REFRAINING FROM ANY ACTION, AS A RESULT OF OR BASED ON THE MATERIAL CONTAINED IN THIS PUBLICATION.

IF YOU ARE IN DOUBT OF YOUR RESPONSIBILITIES IN RELATION TO REPORTING SUSPICIONS TO THE GARDA SÍOCHÁNA OR THE REVENUE COMMISSIONERS IT IS SUGGESTED THAT YOU OBTAIN INDEPENDENT LEGAL ADVICE.

Copyright & Licensing

Financial Intelligence Unit
This document contains links to information, produced by the Financial Intelligence Unit of Ireland and An Garda Síochána and the Copyright of this information reproduced in whole or part has been done so courtesy of the Financial Intelligence Unit.

Re-Use of Public Sector Information – Regulations 2005 (S.I. 279 of 2005)
This site contains legislation being reproduced under the Re-Use of Public Sector Information – Regulations 2005 (S.I. 279 of 2005).

OmniPro complies with regulations on the Re-Use of Public Sector Information under PSI General Licence No. : 2005/08/01. The regulations are available on http://www.psi.gov.ie.

[1] The Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018 (26/2018) that came into effect on the 14 November 2018 states that it may be citied as the Criminal Justice (Money Laundering and Terrorist Financing) Acts 2010 to 2018.

Similar to Companies Ac 2014 any amendments made are by "Deletion" and "Insertion" to specific sections of the existing Criminal Justice (Money Laundering and Terrorist Financing) Acts 2010, therefore the principle title of the relevant legislation as primary reference continues to be the Criminal Justice (Money Laundering and Terrorist Financing) Acts 2010 and for the purpose of reference within this guidance document the revised legislation will be referred to as the "2010 Act"

OmniPro – Anti Money Laundering Guidance

Contents

OmniPro – Anti Money Laundering Guidance

OmniPro – Anti Money Laundering Guidance

Definitions

2010 Act	Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, updated the 26 November 2018 for the 2018 revisions overlaid into the 2010 Act is available at. http://revisedacts.lawreform.ie/eli/2010/act/6/revised/en/html
Accountancy Services	*Accountancy services* include any service provided under a contract for services (i.e. not a contract of employment) which pertains to the recording, review, analysis, calculation or reporting of financial information.
Accounting Firm or Firm	An *Accounting firm* being a sole practitioner, company, partnership or other organisation undertaking defined services. This includes accountancy practices, whether structured as partnerships, sole practitioners or corporate practices.
Business relationship	A business, professional or commercial relationship between an *accounting firm* and a *client*, which is expected by the accounting firm, at the time when the contact is established, to have an element of duration.
CCAB-I	Consultative Committee of Accountancy Bodies in Ireland - the committee represents the Institute of Chartered Accountants in Ireland; the Association of Chartered Certified Accountants; the Chartered Institute of Management Accountants; and the Institute of Certified Public Accountants in Ireland.
Client	A person in a *business relationship*, or carrying out an occasional *transaction*, with an *accounting firm*.
Criminal Conduct	Conduct that constitutes an offence in Ireland as well as conduct occurring elsewhere that constitutes an offence under the law of that place and would have been an offence if it had taken place in Ireland.
Customer due diligence	The process by which Know Your Client information is gathered and the identity of a *client* is established and verified, for both new and existing *clients*.
Defined services	Activities carried on, in the course of business carried on by *accounting firms* or *individuals* as an auditor, *external accountant*, insolvency practitioner or *tax adviser* or as trust and company service providers. It also includes persons providing financial services under the Investment Business Regulations under the oversight of their professional body.
EEA	European Economic Area countries, which are the European Union member states plus EFTA

OmniPro – Anti Money Laundering Guidance

	(European Free Trade Association) member states.
Enhanced due diligence	Additional due diligence steps that must be applied in situations where there is a higher risk of *money laundering* or *terrorist financing* in specific situations as described per sections 37, 38 and 59 of the 2010 Act or where the designated person has identified the relationship presents a higher risk
External accountant	Means a person (an accounting firm or sole practitioner) who by way of business provides accountancy services (other than when providing such services to the employer of the person) whether or not the person holds accountancy qualifications or is a member of a designated accountancy body.
External report	A Suspicious Transaction Report (STR) made under the 2010 Act to the Garda Síochána (FIU Ireland) via goAML and the Revenue Commissioners.
FIU Ireland	The Irish State Financial Intelligence Unit who carries out all the functions of an EU Financial Intelligence Unit (FIU) under the Irish Money Laundering legislation and who comprises of members of the Garda Síochána.
Individuals	Includes the partners, directors, subcontractors, consultants and employees of accounting firms.
Internal Report	A Suspicious Transaction Report (STR) made internally by an individual in accordance with procedures established by the accounting firm.
Money laundering offences	As defined in the 2010 Act, as where a person commits a money laundering offence by: • concealing or disguising the true nature, source, location, disposition, movement or ownership of criminal property, or any rights relating to the property; • converting, transferring, handling, acquiring, possessing or using the criminal property; or • removing the criminal property from, or bringing the property into, the State. Other offences involve money laundering outside the State in certain circumstances, attempts outside the State to commit offences in the State and aiding, abetting, counselling or procuring outside the State commission of offence in the State.
Politically exposed persons (PEPs)	Politically exposed persons, as defined in Section 37 of the 2010 Act.

OmniPro – Anti Money Laundering Guidance

Prejudicing an investigation	It involves the making of any disclosure that is likely to prejudice an investigation.
Proceeds of criminal conduct	Any property that is derived from or obtained through criminal conduct, whether directly or indirectly, or in whole or in part.
Professional privilege reporting exemption	An exemption from reporting suspicions formed on the basis of information received under legal privilege while ascertaining the legal position of the client but the exemption is not available where the information is used for furthering a criminal purpose.
Professional Service Provider	Defined in Section 24 of the 2010 Act as an auditor, external accountant, tax adviser, relevant independent legal professional or trust or company service provider.
Required disclosure	The requirement to disclose: • information on which the knowledge, suspicion or reasonable grounds are based; • the identity, if known, of the person known or suspected to be or have been engaged in an offence of money laundering or terrorist financing; • the whereabouts, if known, of the criminal property; and • any other relevant information.
Senior Management	Defined in Section 24 of the 2010 Act as an officer or employee with sufficient knowledge of the firms 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.
Simplified due diligence	The phrase used to refer to reduced customer due diligence measures provided for certain categories of clients whom the designated person has identified the relationship as low risk.
Tax adviser	Means a person who by way of business provides advice about the tax affairs of other persons.
Terrorist financing	Means an offence under Section 13 of the *2005 Act*, which states: "a person is guilty of an offence if, in or outside the State, the person by any means, directly or indirectly, unlawfully and wilfully provides, collects or receives funds intending that they be used or knowing that they will be used, in whole or in part in order to carry out: a) An act constitutes an offence under the law of the State and within the scope of, and as defined in, any treaty that it is listed in the annex to the Terrorist Financing Convention, or

OmniPro – Anti Money Laundering Guidance

b) An act (other than one referred to in paragraph (a):
   1) That is intended to cause death or serious bodily injury to a civilian or to any other person not taking an active part in the hostilities in a situation of armed conflict, and
   2) The purpose of which is, by its nature or context, to intimidate a population or to compel a government or an international organisation to do, or abstain from doing, any act.

The offence also encompasses providing, collecting or receiving funds whilst knowing or intending that they will be used for the benefit or purposes of a terrorist group or to carry out other *terrorist offences* under Section 6 of the *2005 Act*. Attempting to commit the above offences is also an offence.

Terrorist offences

Section 6 of the *2005 Act* defines *terrorist offences*, incorporating:
terrorist activity (defined as the intention to (i) seriously intimidate a population; (ii) unduly compel a government or an international organisation to perform or abstain from performing an act; or (iii) seriously destabilise or destroy the fundamental political, constitutional, economic or social structures of a state or an international organisation); and
terrorist-linked activity (defined as an act which is committed with a view to engaging in a terrorist activity)

Tipping off

Has the meaning as described in Section 49 of the Act See "*prejudicing an investigation" for a basic principle of the term*.

Fourth money laundering directive

References in this *Guidance* to the "*Fourth Money Laundering Directive*" are to 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* and *terrorist financing*. It is available from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2015_141_R_0003&from=ES

OmniPro – Anti Money Laundering Guidance

1. What is Money Laundering in Ireland?

A summary of Offences under the Act

The primary money laundering offences are defined by *The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (the "2010 Act")*, as amended by *The Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018*.

In summary terms it states an individual commits a money laundering offence, inside or outside the State, if they engage in any of the following acts in relation to property that is the proceeds of criminal conduct:

- concealing or disguising the true nature, source, location, disposition, movement or ownership of criminal property, or any rights relating to the property;
- converting, transferring, handling, acquiring, possessing or using the criminal property; or
- removing the criminal property from, or bringing the property into, the State; and
- that person knows or believes (or is reckless as to whether or not) the property is the proceeds of criminal conduct.

Other offences involve money laundering outside Ireland in certain circumstances, attempts outside Ireland to commit offences in Ireland and aiding, abetting, counselling or procuring outside Ireland commission of offence in Ireland (i.e. There is no need for the proceeds to pass through Ireland).

In simple terms there are three broad groups of offences related to money laundering that firms need to avoid committing. These are:

- knowingly assisting (in a number of specified ways) in concealing, or entering into arrangements for the acquisition, use, and/or possession of, criminal property;
- failing to report knowledge, suspicion, or where there are reasonable grounds for knowing or suspecting, that another person is engaged in money laundering; and
- tipping off, or prejudicing an investigation.

Any of these offences is punishable by up to 14 years' imprisonment and/or a fine not exceeding €5,000.

It is also a separate offence under the 2010 Act not to establish adequate and appropriate policies and procedures in place to forestall and prevent money laundering (regardless of whether or not money laundering actually takes place) which can be punishable by up to 5 years and/or a fine.

What is the Proceeds of Crime and Money Laundering Activity

Criminal property by extension of the interpretation of "proceeds of criminal conduct" may take (but not exclusively) all real or personal property such as the following forms:

- Money or Money's worth;
- Securities, legal documents or instruments in any form including electronic or digital; and
- Tangible or intangible property.

OmniPro – Anti Money Laundering Guidance

1. What is Money Laundering in Ireland? *(continued)*

Money laundering can involve the proceeds of offending in Ireland but also of conduct overseas that would have been an offence had it taken place in the Ireland. For the purposes of this guidance money laundering also includes terrorist financing. There are no materiality or de minimis exceptions to money laundering or terrorist financing offences.

Money laundering activity can include:

- A single act (for example, possessing the proceeds of one's own crime);
- Complex and sophisticated schemes involving multiple parties;
- Multiple methods of handling and transferring criminal property; or
- Concealing criminal property or entering into arrangements to assist others to conceal criminal property.

A summary of the requirements of an Accountancy Firm

The 2010 Act imposes criminal liability on certain individuals in firms subject to the money laundering regulations. Where the firm is a body corporate, an officer of that body corporate (i.e. a director, manager, secretary, chief executive, member of the committee of management, or a person purporting to act in such a capacity), who consents or connives in the commission of an offence by the firm, or where that offence (by the firm) is attributable to the lack of supervision or control on his part, himself commits a criminal offence and may be prosecuted. Similarly, where the firm is a partnership, a partner who consents to or connives in the commission of offences under the money laundering regulations, or where the commission of any such offence is attributable to any neglect on his part, will be individually liable to be prosecuted for the offence. A similar rule applies to officers of unincorporated associations.

Accountancy firms need to be alert in the work they do the risks posed by:

- Clients;
- Suppliers;
- Employees; and
- The customers, suppliers, employees and associates of clients.

Neither the business nor its client needs to have been party to money laundering for a reporting obligation to arise (see Section five of this guidance).

For the purposes of 2010 Act an Offence is not deemed to have been committed if:

- The persons involved did not know or suspect that they were dealing with the proceeds of crime; or
- A report of the suspicious money laundering activity is made promptly to:
    - A Money Laundering Reporting Officer (MLRO) (i.e. an internal Suspicious Transaction Report (STR)); or
    - An Garda Síochána as the FIU Ireland via goAML under the provisions of Section 42 of the 2010 Act (as an external STR) and the STR is made before the offence takes place so that the necessary consent to proceed (referred to as a defence against money laundering by the 2010 Act) is obtained beforehand; or
- There is a reasonable excuse for not reporting the suspicious money laundering activity because there is a risk to the personal safety or security of the persons of the designated person obligated to report.

OmniPro – Anti Money Laundering Guidance

2. Responsibility and Oversight within a Professional Service Provider for Money Laundering

What are the responsibilities of Designated Persons?

Professional service providers as defined by the act can be an auditor, external accountant, tax adviser, relevant independent legal professional[2] or trust or company service provider and all fall within the meaning of "Designated Person" as detailed in Section 25 of the 2010 Act.

Under the amended 2010 Act designated persons are required to have:

- Systems and controls capable of:
    - assessing the risk associated with a client;
    - performing Customer Due Diligence;
    - monitoring existing clients;
    - keeping appropriate records; and
    - enabling staff to make an internal Suspicious Transaction Report (STR) (i.e. to their MLRO).
- Ongoing training of all principals, directors and staff so that they understand both their own personal AML obligations and the business-wide systems and controls developed for the identification of money laundering and terrorist financing and related activities (section 54(6)(b)).
- Effective internal risk management systems and controls must be established and the relevant *senior management* responsibilities clearly defined.

Section 54(7) of the 2010 Act stipulates a designated person shall appoint an individual at management level to be a "Compliance Officer" for the purpose of monitoring and managing compliance of the internal policies, controls and procedures adopted by the business. Likewise, Section 54(8) states a member of senior management is appointed primary responsibility for implementation and management of the 2010 Act requirements.

Depending on the size, complexity and structure of a business, these two roles may be combined in a single individual provided that person has sufficient seniority, authority, governance responsibility, time, capacity and resources to do both roles properly. This guidance primarily describes the situation in which one individual fulfils the combined role, referred to in this guidance as the Money Laundering Reporting Officer (MLRO). The role of the MLRO is not defined in legislation but has traditionally included responsibility for internal controls and risk management around money laundering and terrorist financing, in accordance with sectoral guidance. Businesses with an MLRO should periodically review the MLRO's brief to ensure that:

- it reflects current law, regulation, guidance, best practice and the experience of the business in relation to the effective management of money laundering and terrorist financing risk; and
- the MLRO has the seniority, authority, governance responsibility, time, capacity and resources to fulfil the brief.

[2] A relevant independent legal professional, includes, in the case of the provision of services by a barrister, a person who is a client of a solicitor seeking advice from the barrister for or on behalf of the client and does not, in that case, include the solicitor,

OmniPro – Anti Money Laundering Guidance

2. Responsibility and Oversight within a Professional Service Provider for Money Laundering *(continued)*

Where the MLRO role as described above is split to meet the individual obligations of Section 54(7) and 54(8) of the 2010 Act into two or more individuals, the allocation of the duties should be clear to the individuals assigned the duties and those in governance of the organisation with ultimate responsibility for compliance with anti-money laundering legislation. Depending on the size, complexity and structure of the firm, management may use this as the basis of how to assign duties between the two or more individuals, however persons allocated responsibility should have appropriate knowledge understanding and expertise around money laundering requirements.

If a designated person fails to meet its obligations under the 2010 Act, civil penalties or criminal sanctions can be imposed on the designated persons and any individuals deemed responsible. This could include anyone in a senior position who neglected their own responsibilities or agreed to something that resulted in the compliance failure.

How should sole practitioners implement these requirements?

As it would not be appropriate to the size and nature of the business, a sole practitioner who has no relevant employees as directed by Section 54(12) of the 2010 Act need not:

- appoint a board member to be responsible for the business' compliance with the Irish anti-money laundering regime, as the sole practitioner will be held responsible;
- appoint a nominated officer because the sole practitioner will be responsible for submitting external reports to An Garda Siochana via the goAML platform;
- establish an independent audit function for AML policies, controls and procedures.

What are the responsibilities of Senior Management/MLRO?

The 2010 Act defines *senior management* as: an officer or employee (and need not, in all cases, be a member of the board of directors) with sufficient knowledge of the business's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure.

Whilst the legislation does not state that a firm must appoint a Money Laundering Reporting Officer (MLRO) it is probably easier that it does so, this will allow one person to have ownership of the area.

This person should be a senior member of staff (hence the legislation reference to senior management) and it is suggested that this is either a partner or senior manager, however it may be a staff member with sufficient knowledge and understanding of the money laundering obligations under the legislation Section 54(10). This person must be fully supported by the partners within the firm, for example relevant resources must be provided to ensure that the MLRO is in a position to ensure that appropriate procedures are implemented within the firm, including training.

The 2010 Act stipulates that the approval of *Senior Management / MLRO* must be obtained:

- For a business risk assessment (Section 30A(5))
- For the policies, controls and procedures adopted by the business (Section 54(4));
- Before entering into or continuing a business relationship with a Politically Exposed Person (PEP), a family member of a PEP or a known close associate of a PEP (Section 37(4)(a)).

OmniPro – Anti Money Laundering Guidance

2. Responsibility and Oversight within a Professional Service Provider for Money Laundering *(continued)*

As directed by section 54(6)(b) of the legislation designated persons are required to ensure staff are provided with ongoing training in relation to AML however for the *Senior Management / MLRO* must receive regular CPD appropriate to their role to thereby be able to fulfil the obligations set by the designated persons in ensuring compliance be the firm for AML.

The obligations of the Senior management/MLRO of the firm in addition to (b) above include:

a. Responsibility to ensure that the firm's policies, controls and procedures are appropriately designed and implemented, and are effectively operated to reduce the risk of the firm being used in connection with money laundering or terrorist financing and ensure compliance. Section 54(3) states those policies, controls and procedures shall include:
    i. The identification, assessment, mitigation and management of risk factors relating to money laundering or terrorist financing,
    ii. Customer due diligence (CDD) measures,
    iii. Monitoring transactions and business relationships,
    iv. The identification and scrutiny of complex or large transactions, (unusual patterns of transactions or other activity that may be related to money laundering or terrorist financing,
    v. Measures to be taken to prevent the use for money laundering or terrorist financing of transactions or products that could favour or facilitate anonymity,
    vi. Measures to be taken to prevent the risk of money laundering or terrorist financing which may arise from technological developments, new products or new practices,
    vii. Reporting (including the reporting of suspicious transactions (STRs) both to receive internal STRs and make external STRs to an Garda Siochana,
    viii. Record keeping,
    ix. Measures to be taken to keep documents and information relating to the customers up to date,
    x. Measures to be taken to keep documents and information relating to risk assessments up to date,
    xi. Internal systems and controls to identify emerging risks and keep business wide risk assessments up to date, and
    xii. Monitoring and managing compliance with, and the internal communication of, these policies, controls and procedures.
b. Approve the firms system for business risk assessment for preventing money laundering;
c. Have oversight of, and be involved in, money laundering risk assessments of the firm which requires knowledge, understanding and access to any relevant information about the business and have regard for the national and international annual risk assessment findings to inform their performance of their role, these risk assessments must be kept up to date, and their findings should be reported to the management of the firm (guidance from the accountancy bodies stipulates these should be done annually);
d. Take remedial action where controls are ineffective;
e. Draw attention to the areas in which systems and controls are effective and where improvements could be made;
f. Take reasonable steps to establish and maintain adequate arrangements for awareness and training;
g. Receive the findings of relevant money laundering compliance audits and reviews (both internal and external) and communicate these to Management of the Firm.

OmniPro – Anti Money Laundering Guidance

3. The Risk-Based Approach to Anti Money Laundering

The concept of a risk-based approach

Senior management of most firms, whatever business they are in, manage the firm's affairs with regard to the risks inherent in the business environment, the jurisdiction and services that firm operates in, those risks inherent in its business and the effectiveness of the controls it has put in place to manage these risks.

To assist the overall objective to prevent money laundering and terrorist financing, a risk-based approach:

- recognises that the money laundering/terrorist financing threat to firms varies across customers, jurisdictions, products and delivery channels;
- allows management to differentiate between their customers in a way that matches the risk in their particular business;
- allows senior management to apply its own approach to the firm's procedures, systems and controls, and arrangements in particular circumstances; and
- helps to produce a more cost effective system.

A firm therefore uses its assessment of the risks inherent in its business to inform its risk-based approach to the identification and verification of individual customers, which will in turn drive the level and extent of due diligence appropriate to that customer. No procedure will ever detect and prevent all money laundering and terrorist financing, but a realistic analysis of actual risks enables a firm to concentrate its efforts on perceived higher risk areas. A risk assessment matrix[3] is commonly used by accounting firms to categorise risk attaching to its client base.

The risk-based approach does not exempt low risk clients, services and situations from CDD, however the appropriate level of CDD is likely to be less onerous than for those thought to present a higher level of risk but ultimately senior management must decide on the extent of measures and their approach taken by the firm for each client risk rating.

The application of a Risk Based Approach in a Professional Services Provider

Section 30A(1) of the 2010 Act requires every firm to perform a risk assessment (the "Business Risk Assessment") to identify and assess the risk to that organisation of money laundering and terrorist financing and that risk factor must take account of at least the six stipulated risk factors:

1) The type of customer that the firm has;
2) The products and services that the firm provides;
3) The countries or geographical areas in which the firm operates;
4) The type of transactions that the firm carries out;
5) The delivery channels that the firm uses;
6) Other prescribed additional risk factors[4].

As part of its procedures a firm must identify and establish the main internal and external risks faced in respect of those presented by its client base and also those required to ensure that its internal controls are appropriate. Senior management is responsible for managing all the risks faced by the business, including money laundering and terrorist financing risks. These risks should be analysed, and their nature and severity identified and assessed, in order to produce a risk profile.

[3] For those firm using the newly updated OmniPro Money Laundering Procedures manual this is the client risk assessment contained in Appendix 2

[4] For a more exhaustive list of considerations see Schedule 3 and Schedule 4 of the amended 2010 Act

OmniPro – Anti Money Laundering Guidance

3. The Risk-Based Approach to Anti Money Laundering *(continued)*

As previously stipulated an annual firm AML risk business assessment is required, which could be the basis for identifying any weaknesses in the system of monitoring AML and the effectiveness of the policies and procedures that require revision having identified the risk to organisation. Senior management should then act to mitigate those identified risks by designing and implementing procedures to address the risk posed and ensure that the system of controls continues to be reviewed to ensure its effectiveness.

Accordingly a firm risk based approach should evolve in response to the findings from the review of the monitoring of the effectiveness of the systems in place.

The risk assessment can be conducted by the MLRO but must be approved by senior management. This is likely to include formal acknowledgement of adoption of the outcomes, including the resulting policies and procedures by the firm. Where revisions to existing AML policies and procedures impacts a firm significantly and those relevant employees training may be needed to ensure are knowledgeable in the AML requirements and to demonstrate compliance with Section 54(6).

Identifying and Assessing the Risks in a Professional Service Provider

The business of many firms, can be relatively simple, involving few products and limited offering of services, with most customers being of a simple client base nature. In such circumstances, a simple approach, building on the assessed risk of the firm's services provided, may be appropriate for most customers, with the focus being on those customers who fall outside the 'norm'. Thereby a single set of AML policies, controls and procedures may suffice right across its operations.

Other firms may have a greater level of business or service offering and therefore might have significantly different risks across its services such as insolvency, bankruptcy or when holding client monies, but large numbers of their customers may be predominantly simple in nature, that adopting a standardised approach to many AML procedures may be practical for the majority of situations of the firm but tailoring when a minority of customers are not straightforward will be required based on their risk assessment.

For firms which operate internationally, or which have customers based or operating abroad, there are additional risk considerations, (i.e. What is the perceived money laundering status or risk of that country, and the effectiveness of their money laundering and terrorist financing enforcement regime, other factors to consider might also include the perceived level of corruption and criminal activity in that country).

Many governments and authorities such as Transparency International5 carry out money laundering and terrorist financing risk assessments for their jurisdictions, and firms should have regard to these, as they are generally published and publicly available, which can assist in assessing the geographic AML risk posed to that client.

[5] Transparency International is a not-for-profit, non-governmental organisation dedicated to fighting corruption and active in nearly 100 countries. It is the creator of the Corruption Perceptions Index, which measures levels of perceived corruption around the world.

OmniPro – Anti Money Laundering Guidance

3. The Risk-Based Approach to Anti Money Laundering *(continued)*

In identifying its money laundering risk a firm might consider the following factors:

- its clients, the range of services provided and activity profiles;
- the structure of the firm and the manner in which services are provided to the client (i.e. Segregation of duties and limited communication between department)s;
- the complexity and volume of transactions done by the client;
- its processes and systems; and
- its operating environment.

The firm should therefore assess its risks in the context of how it might most likely be involved in money laundering or terrorist financing. In this respect, senior management should ask themselves a number of questions; for example:

- What risk is posed by the firm's clients/customers?
- What risk is posed by a client's behaviour?
- How does the way the client/customer comes to the firm affect the risk?
- What risk is posed by the products/services the customer is using?

In a fast paced digital modern society where goods and services can easily be sold across borders, firms must take account of the delivery mechanism being used, the service being provided, the end user and the beneficiary in assessing the risk associated with facilitating and providing the service that an Offence under the 2010 Act is not perpetrated.

Designing and Implementing Controls to meet the Risk-Based Approach

Once the firm has identified and assessed the risks it faces in respect of money laundering or terrorist financing through its business risk assessment process as required by Sections 30A of the revised 2010 Act. Senior management must establish and maintain policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified in its risk assessment. These policies, controls and procedures must take account of the size and nature of the firm's business and as required by Section 54(4) they must be approved by Senior Management of the firm. The policies, controls and procedures should cover risk management practices, customer due diligence, reporting, record-keeping, internal controls, compliance management and employee screening

A risk-based approach requires the full commitment and support of senior management, and the active co-operation of business units. The risk-based approach needs to be part of the firm's philosophy, and as such reflected in its procedures and controls. There needs to be a clear communication of policies, controls and procedures across the firm, along with robust mechanisms to ensure that they are carried out effectively, weaknesses are identified, and improvements are made wherever necessary.

OmniPro – Anti Money Laundering Guidance

3. The Risk-Based Approach to Anti Money Laundering *(continued)*

Before establishing a client relationship or accepting an engagement a firm must have controls in place to address the AML risks arising from it. The nature and extent of AML controls will depend on a number of factors, including:

- The nature, scale and complexity of the firm's business
- The diversity of the firm's operations, services provided, and the geographical diversity of its client base or if the firm has multiple locations
- The firm's clients, the service provided to that client and the clients activity profile i.e.
    a. The type of business the client does;
    b. The volume, frequency and size of transactions;
    c. The distribution channels used;
    d. The client is international or domestic; or
    e. The client is high net worth individual or Politically Exposed Person.
- The extent to which the firm is dealing directly with the clients or is dealing through intermediaries, third parties, correspondents or non face to face access
- The degree to which the firm outsources the operation of any procedures to other (Group) entities.
- Does the firm operate through multiple business units or through branches or subsidiaries.

The application of CDD measures as an extension of the AML controls is intended to enable a firm to form a reasonable belief that it knows the true identity of each customer and beneficial owner, and, with an appropriate degree of confidence, knows the types of business and transactions the customer is likely to undertake. The firm's procedures should include procedures to:

- Identify and verify the identity of each customer on a timely basis;
- Identify and take reasonable measures to verify the identity of any ultimate beneficial owner; and
- Obtain appropriate additional information to understand the customer's circumstances and business, including the expected nature and level of transactions.

When designing a way to analyse the risk and create a risk based assessment approach to AML within a firm, the requirements of Section 30A(1) must be addressed but, factors that reduce risk as well as those that increase risk need to be considered:

a. Is the client subject to an effective AML regime elsewhere;
b. Might the firm or the client's business:
    i. Be used to launder money (e.g. by holding criminal proceeds in a client money account or by becoming involved in an arrangement that disguises the beneficial ownership of criminal proceeds);
    ii. Be used to facilitate Money Laundering or Terrorist Financing by another person (e.g. by creating a corporate vehicle to be used for money laundering or by introducing a money launderer to another regulated entity); and
    iii. Suffer consequential legal, regulatory or reputational damage because a client (or one or more of its associates) is involved in money laundering.

OmniPro – Anti Money Laundering Guidance

3. The Risk-Based Approach to Anti Money Laundering *(continued)*

Senior management should decide on the appropriate approach to how risk-based assessments should be implemented in light of the firm's structure. The firm may adopt an approach that starts at the organisation area level, or one that starts from service streams provided.

A failure to adopt appropriate procedures would result in a breach of the legislation and result in a fine or imprisonment for term of up to 5 years.

The Client Risk Assessment Process

Based on the risk assessment carried out, where key risk categories are identified, a firm may be able to establish a basis for determining individual clients risk profiles, as low, medium or high which will determine the level of CDD that should be applied in respect of that client and beneficial owner. In considering the basis for determining those client risk profiles the firm's assessment process might take account of the client's legal form, the country in which the client is established or incorporated, and the industry sector in which the client operates. In addition, businesses should also consider the nature of the service being offered to a client and the channels through which the services/transactions are being delivered.

Accordingly when there are identified higher risk client profiles, the firm might consider addressing the risks by performing enhanced due diligence or performing more regular CDD checks or limit the service offering to the client based on controls that may be put in place to address the risk. However in the majority of client cases it is likely that there will be a standard level of CDD, based on the firm's risk appetite.

It should be noted that an assessment of low risk only allows for some reduction of the level of due diligence carried out (see simplified due diligence) – it is not a complete exemption from the application of CDD measures in respect of customer identification. Also it does not exempt the firm from carrying out ongoing monitoring of the business relationship with the customer, nor from the need for such other procedures (such as monitoring) as may be necessary to enable a firm to fulfil its responsibilities under the 2010 Act.

As outlined previously Section 30A(1) of the 2010 Act specifically details risk factors to be considered as part of the business risk assessment for that Firms business active in designing a client risk assessment which addresses these the focus might be:

- Customer Risk – the overall money laundering risk posed by a client based on key risk categories;
- Service Risk – the perceived risk that certain products or services present an increased level of vulnerability in being used for money laundering purposes
- Geographic risk – the increased level of risk that a country poses in respect of money laundering
- Sector Risk – the risk associated with certain sectors that more likely to be exposed to increased levels of money laundering
- Delivery Channel Risk – the risk to the firm can be increased where services are provided to clients who have not been met face to face
- Other Risks as identified and issued by the accounting institutes and authorities

Firms must be able to demonstrate how they assess and seek to mitigate money laundering risks, they must be kept up to date and available for review to the competent authority which for an accounting practice is it governing institute.

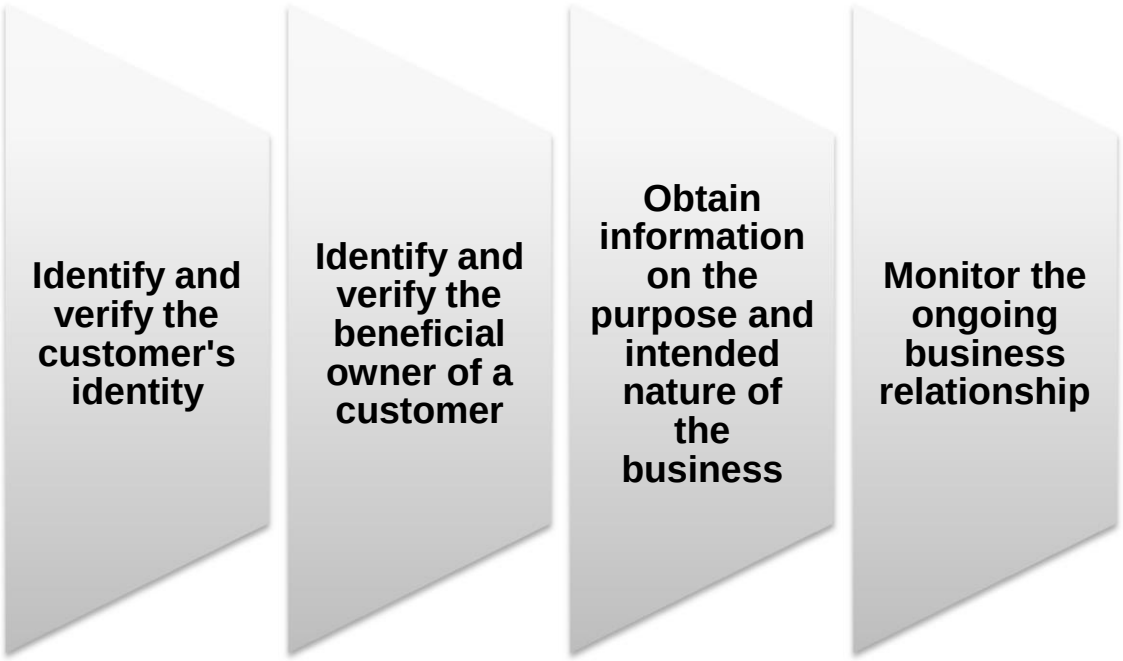
OmniPro – Anti Money Laundering Guidance

4. Customer Due Diligence (CDD)

Customer Due Diligence is a key element of the anti money laundering requirements and has 12 Sections of the new 2010 Act dedicated to it. Customer Due Diligence is required for all new clients, and is now also required for existing clients if they have not provided identification which has been verified in the past, or you are aware that the information that is held is not up to date or if there are doubts as to its validity.
Firms must determine the extent of their CDD measures and ongoing monitoring using the risk based approach, depending on the type of customer, business relationship, product or transaction. They must be able to demonstrate to their supervisory authority that the extent of their CDD measures and monitoring is appropriate in view of the risks of money laundering and terrorist financing.

Therefore, the purpose of CDD is to know and understand a client's identity and business activities so that any money laundering and terrorist financing risks can be properly managed. The CDD process can be simply summarised in the following diagram

Customer Due Diligence



OmniPro – Anti Money Laundering Guidance

4. Customer Due Diligence (CDD) *(continued)*

Identifying and Verifying the Customers Identity

The first requirement is that your firm identify and verify a customer's identity ***prior*** to:

- **establishing a business relationship with the customer**.
- **carrying out an occasional transaction for a customer,** i.e. a single transaction, or a series of transactions that are, or appear to be linked to each other, where:
    i. The designated person does *not* already have a business relationship with the customer, and
    ii. The total amount of money paid by the customer in the single transaction or series of transactions is not less than €10,000.
- carrying out any service for the client, if the firm has **reasonable grounds to believe that there is a real risk that the client is involved in**, or the service sought by the client is for the purpose of, **money laundering or terrorist financing**.
- carrying out any service for the client if the firm has **reasonable grounds to doubt the veracity or adequacy of documents or information previously obtained by it for the purposes of verifying the identity of the customer**, and it has not obtained any other documents or information that can be reasonably relied on to confirm the identity of the customer.

In general, the verification of the identity of the client and the beneficial owner, must take place ***before*** the establishment of a business relationship or the carrying out of a transaction. However, verification of the identity of the client and beneficial owner may be completed ***during*** the establishment of a business relationship if:

- this is necessary not to interrupt the normal conduct of business; and
- there is no real risk of money laundering or terrorist financing occurring provided that the verification is completed as soon as practicable after the initial contact.

Identifying and Verifying the beneficial owner of a client

Identifying who the beneficial owner is, can sometimes be problematic and not straightforward as different rules apply to different forms of entities and the obligations on the firm may change for each situation. For example, where the beneficial owner is a legal person (other than a company listed on a regulated market), trust, company, foundation or similar legal arrangement, firms must take reasonable measures to understand the ownership and control structure of that legal person, trust, company, foundation or legal arrangement.

OmniPro – Anti Money Laundering Guidance

4. Customer Due Diligence (CDD) *(continued)*

The second requirement of the CDD process is for your firm to to establish and verify the identity of a beneficial owner of the client or potential client and a beneficial owner can only be a natural person i.e., an individual (other than in the case of a trust):

Where the customer is	The beneficial owner of the customer is
A company (not listed on a stock exchange)	Any individual who: • directly or indirectly owns more than 25% of the shares (25% plus one share) or voting rights in the company, OR • exercises control over the management of the company.
A partnership	Any individual who: • directly or indirectly is entitled to or controls more than 25% of partnership profits or capital, or the voting rights in the partnership, OR • exercises control over the management of the partnership.
A trust	An individual or beneficiary who: • Has an interest in at least 25% of the trust capital, (or where some/all of the interest have not yet been determined but is the class of persons in whose main interest the trust is set up or operates for) • The settlor and trustee(s) • Any other individual who has control over the trust (e.g., a protector or trust controller).
Other legal entities	Any individual who benefits from the property of the entity where no individual beneficiaries are identified, the class of persons in whose main interest the entity or arrangement was set up or operates, any individual who exercises control over the entity/arrangement.
Estate of a deceased person	The executor or administrator of the estate.
Other cases	Any individual who ultimately owns or controls a customer, or on whose behalf a transaction is conducted.
Where all possible means of identifying the beneficial owner of a body corporate have been exhausted and recorded	The senior individual responsible for management (noting the reasons why the business was unable to obtain adequate information on the beneficial owner, and considering whether it may be appropriate to cease acting, or file a STR).

OmniPro – Anti Money Laundering Guidance

4. Customer Due Diligence (CDD) *(continued)*

Identifying who is a Beneficial owner might be a slow and sensitive process when dealing with clients, firms should be diligent in ensuring there obligation under the 2010 Act is met but beware that complex structures might be difficult to identify through information in the public domain and more direct enquiry with clients is required. In addition there may be situations in which someone is considered to be the beneficial owner by virtue of control even though their ownership share is less than 25%.

Example 1

ABC Ltd. is owned 40% by Mr A, 40% by Mr B and 20% by Mr C. Mr C is not able to exercise control over the management of ABC Ltd.

If ABC Ltd. wishes to engage with a firm it has not previously had a business relationship with, the firm will be required to identify the 'beneficial owners' of ABC Ltd., which in this case are Mr A and Mr B, as each has more than 25% of the shares or voting rights in the company.

Example 2

A Ltd. Is owned 50:50 by companies B Ltd and C Ltd,

Company B is owned 60:40 by Mr X and Mr Y

Company C is owned 55:45 by Ms W and Mr Z

Due to less than 25% ownership being held in Company A, neither Mr Y or Mr Z are deemed to be beneficial owners of A as they are not able to exercise control over the management of A Ltd.

*If A Ltd. wishes to engage with a firm it has not previously had a business relationship with, the firm will be required to identify the 'beneficial owners' of A Ltd., which in this case are Mr X (60%*50%= 30% ownership) and Ms W (55%*50%=27.5% ownership) of the shares or voting rights in the company.*

Example 3

ABC Ltd. is owned 50% by Mr A, 40% by Mr B and 10% by Mr C. However, Company XYZ has a golden share with controlling power due to loan covenants to facilitate related party lending with it as XYZ Ltd is 100% owned by Mr C.

While on the face of it, it appears that Mr A and Mr B should be the beneficial owners this is not actually the case as ultimately neither is the controlling party as Mr C through the Golden share is the controlling party through his 100% ownership of XYZ Ltd and therefore Mr C is the Ultimate Beneficial Owner even though he holds only 10% of the ordinary share capital.

Example 4

Charity Ltd. is a company limited by guarantee for charitable purposes. It has Directors of the company but there are any number of members with no one member exerting control.

Accordingly as no one shareholder has 25% plus one share ownership of the company, the beneficial owners are deemed to be those exercising control which in this organisation is the Directors, therefore if Charity Ltd wishes to engage with a firm it has not previously had a business relationship with, the firm will be required to perform procedure checks on the directors as the Ultimate Beneficial Owners

OmniPro – Anti Money Laundering Guidance

4. Customer Due Diligence (CDD) *(continued)*

Obtaining Documentation for Customer Identification

Your firm can adopt a *'risk based'* approach as to how to establish and verify the identity of a client (or beneficial owner of a customer), i.e. it can identify the most appropriate method to identify and verify the client's identity, taking account of its assessment of the risk of money laundering or terrorist financing presented by the client in question.

The identification phase requires the gathering of information about a client's identity and the purpose of the intended business relationship. Appropriate identification information for an individual would include full name, date of birth and residential address. This can be collected from a range of sources, including the client. In the case of corporates and other organisations, identification also extends to establishing the identity of anyone who ultimately owns or controls the client. These people are the Beneficial Owners.

Verification of that identification information gathered involves validating (with an independent, authoritative source), that the identity is genuine and belongs to the claimed individual or entity.

Typically, you will seek documentary or electronic verification of the customer's:

- Name and date or birth, or
- Name and current address.

Firms may secure this information about individuals using, what is called, the **'one plus one'** method, i.e.

One item of **photographic ID evidence**, such as any of the following:

- Current Passport (Irish or International);
- Current photo card driving licence;
- Current National Identity Card;
- Current Identification form with photo signed by a member of the Gardaí (ML10);
- Social Welfare card with photo ID;
- GNIB[6] card accompanied by letter from Office of Minister for Integration (signed and stamped); and
- National Age card (free of charge for social welfare recipients).

PLUS

[6] *Garda National Immigration Bureau*

OmniPro – Anti Money Laundering Guidance

4. Customer Due Diligence (CDD) *(continued)*

One item of **non photographic ID evidence**, such as any of the following:

- Current documentation/cards issued by the Revenue Commissioners showing the name of the person and their PPSN;
- Current documentation/cards issued by the Department of Social Protection showing the name of the person and their PPSN;
- Instrument of a court appointment (such as liquidator, or grant of probate);
- Current local authority document e.g. refuse collection bill, water charge bill (including those printed from the internet);
- Current bank statements, or credit/debit card statements, issued by a regulated financial sector designated person in the Ireland, EU or comparable jurisdiction (including those printed from the internet);
- Current utility bills (including those printed from the internet);
- Current Household/motor insurance certificate and renewal notice; and
- Medical card for over 18s with intellectual disability.

In cases where a plausible explanation is offered by a customer as to why the above non photographic documentation cannot be provided, a firm can choose the following to assist in confirming the identity of the customer, having regard to any data protection requirements:

- Examination of the electoral register (including online version);
- Examination of a local telephone directory or available street directory;
- Confirmation of identity by a known/recognisable employer;
- Search of a relevant agency that can confirm identity.

Non Face to Face Contact with Clients

Additional Customer Due Diligence measures are required where the firm is dealing with a new customer on a non face to face basis, e.g. exclusively over the internet or by telephone, and therefore does not physically meet the customer before establishing a business relationship with them.

Some of the additional Customer Due Diligence measures which can be used are:

- Telephone call to the customer prior to the commencement of the business relationship on a home or business number which has been verified (electronically or otherwise);
- Communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, might be required to be returned completed or acknowledged without alteration);
- Internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address; and
- Verification through third party service providers who are also determined as designated persons as per the 4th EU AML Directive.

OmniPro – Anti Money Laundering Guidance

4. Customer Due Diligence (CDD) *(continued)*

Obtaining information on the purpose of the business relationship

As detailed earlier the third requirement in performing customer due diligence, using a risk based approach, information from all clients is gathered, on the purpose and intended nature of their business relationship prior to the establishment of the relationship.

However, in most cases, the purpose of the business relationship will be self-evident given the nature of the product or service that the client is seeking, e.g. an individual is a state employee but in receipt of rental income from a property and is looking to have a personal income tax return done.

An initial risk assessment is based on the information gathered during stage one (identification), but this may prompt the gathering of additional information following verification of the evidence gathered. Accordingly, where a firm proposes to enter into a business relationship with a client and your assessment of the risk associated with the client or with the nature of the products or services to be provided to the client indicate a higher than standard risk of money laundering or terrorist financing, then the firm may typically seek to obtain the following information during the establishment of the business relationship:

- nature and details of the business/occupation/employment of the client;
- the expected source and origin of the funds to be used in the relationship, e.g. the client is owns and manages a hotel or the individual is a self-employed sole trader builder, and;
- the anticipated level and nature of the activity that is to be undertaken through the relationship (i.e. Advisory, bookkeeping, payroll, audit, taxation etc).

Refusal to supply Customer Due Diligence information

Where a firm is unable to identify and verify a prospective or existing client's identity or establish the purpose of the business relationship, because of the failure of the prospective or existing client to provide the documentation or information sought, the firm must:

- not provide the service sought by that prospective or existing client or carry out any proposed transaction for so long as the failure to supply the relevant information remains unrectified, and
- terminate the existing business relationship (if any) with the prospective or existing client.

However it is important to note in many cases inability to complete CDD is not a circumstance where an insolvency practitioner can resign and so an appropriate risk based approach should be adopted where the client's management are not cooperative. This risk based approach in this circumstance should take account of the Schedule 3 and Schedule 4 risk factors of the 2010 Act at a minimum with the firm clearly documenting the evidence-based decision-making taken by the firm to better target the risks present.

OmniPro – Anti Money Laundering Guidance

4. Customer Due Diligence (CDD) *(continued)*

Ongoing monitoring of the client relationship

The fourth requirement of standard customer due diligence is to monitor the client relationship on an ongoing basis. Using a risk based approach and the completion of the firm's annual risk-assessment, a firm must monitor dealings with all existing clients periodically by scrutinising transactions and the source of wealth or of funds for those transactions, to determine whether or not the transactions are consistent with:

- The firm's knowledge of the clients and the client's business and pattern of transactions, this is done through ensuring CDD is kept up to date through annual enquiry of:
    - a change in the client's identity;
    - a change in beneficial ownership of the client;
    - a change in the service provided to the client; and
    - information that is inconsistent with the business' knowledge of the client.

  A revision to the CDD might be required as a result of a specific trigger event to ensure knowledge kept by the firm is up to date. Such circumstances might be identified at:
    - the start of a new engagement;
    - planning for recurring engagements;
    - a previously stalled engagement restarting;
    - a significant change to key office holders; and
    - a significant change in the client's business activity (this would include new operations in new countries.
- Any knowledge or suspicion that the firm may have that the clients may be involved in money laundering or terrorist financing. Accordingly in the event there has been a STR (Suspicious Transaction Report) made, due to knowledge, suspicion of money laundering or terrorist financing, care must also be taken to avoid making any disclosures which could constitute tipping off.

Note that in performing ongoing CDD for existing clients the procedures and the extent of information required may not be the same as those for new clients when a new business relationship is established at the start.

Simplified Customer Due Diligence

Simplified Due Diligence (SDD) can be applied when a client is low risk, in accordance with the businesses' risk assessment criteria. While the CDD requirements of:

- identifying and verifying the client;
- identifying and verifying the beneficial owner of the client, if relevant,
- obtaining information on the purpose and intended nature of the business relationship, and
- the ongoing monitoring for unusual or suspicious transactions,

Are still required the extent and frequency of timing may change to reflect the low risk however this does not remove the obligation to conduct ongoing monitoring of the business relationship.

The firms' internal procedures should set out clearly what constitutes reasonable grounds for a client to qualify for SDD and must take into account at least the factors of section 30A of the 2010 Act and the potential low and high risk factors of schedules 3 and of that Act.

OmniPro – Anti Money Laundering Guidance

4. Customer Due Diligence (CDD) *(continued)*

SDD measures must not be applied, or continue to be applied, where the firm's risk assessment changes and it no longer considers that there is a low degree of risk of money laundering or terrorist financing or where the firms suspect or has doubts regarding money laundering or terrorist financing (including the accuracy of information and documents for identification purposes). Accordingly a duty to report knowledge or suspicion of money laundering or terrorist financing may exist.

Enhanced Customer Due Diligence

Enhanced Customer Due Diligence (EDD), i.e. over and above Standard CDD, applies where the risk based approach to CDD identify situations in which there is a higher risk of money laundering and terrorist financing and for specific classes of persons and situations as specified in the 2010 Act, these include:

- where there is a high risk as per Schedule 4 of the 2010 Act or the client risk assessment identifies a high risk of money laundering;
- in any occasional transaction or business relationship with a person established in a high-risk third country;
- if a business has determined that a client or potential client is a PEP, or a family member or known close associate of a PEP;
- in any case where a client has provided false or stolen identification documentation or information on establishing a business relationship;
- in any case where a transaction is complex and unusually large, there is an unusual pattern of transactions which have no apparent economic or legal purpose; and
- in any other case which by its nature can present a higher risk of criminal activity, money laundering and terrorist financing.

The firms' internal procedures should set out clearly what constitutes reasonable grounds for a client to qualify for EDD and must take into account the above considerations.

For EDD, a firm should hold a fuller set of information in respect of those business relationships it assessed as carrying a higher money laundering or terrorist financing risk, or where the customer is seeking a product or service that carries a higher risk of being used for money laundering or terrorist financing purposes.

When someone becomes a new client, or avails of a higher risk service offering, or where there are indications that the risk associated with an existing business relationship might have increased, the firm should, depending on the nature of the service being applied, request information as to the:

- client's residential status;
- employment and salary details; and
- other sources of income or wealth (e.g., inheritance, property sale, trade etc

in order to decide whether to accept the application or continue with the relationship.

OmniPro – Anti Money Laundering Guidance

4. Customer Due Diligence (CDD) *(continued)*

The firm should consider whether, in some circumstances, evidence of source of wealth or income should be required (for example, if from an inheritance, see a copy of the will). The performance of EDD measures may also include one or more of the following measures:

- seeking additional independent, reliable sources to verify information, including identity information, provided to the business;
- taking additional measures to understand better the background, ownership and financial situation of the client, and other parties relevant to the engagement;
- taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship; and
- Increasing the monitoring of the business relationship, including greater scrutiny of transactions

When seeking additional information, firms should bear in mind their obligations under the GDPR legislation Act only to seek information that is needed for the declared purpose, not to retain personal information longer than is necessary, and to ensure that information that is held is kept up to date.

In addition, a firm should have a clear policy regarding the escalation of decisions to senior management concerning the acceptance or continuation of high-risk business relationships.

Politically Exposed Persons

The most frequent application of Enhanced Customer Due Diligence is when clients of a firm identify as a Politically Exposed Person (PEP). A PEP is an individual who is or, has been entrusted with prominent public functions, or an immediate family member, or a known close associate of such a person. The definition includes persons holding a prominent position in the European Union and international bodies such as the UN, World Bank or IMF.

Examples of PEPs include:

- Heads of state, heads of government, ministers and deputy or assistant ministers;
- Members of parliaments or head of governing body of a political body;
- Members of supreme courts, of constitutional courts or of other high level judicial bodies;
- Members of courts of auditors or of the boards of Central Banks;
- Ambassadors, charges d'affaires and high-ranking officers in the armed forces, and
- Members of the administrative, management or supervisory boards of State-owned enterprises.

Under the 2010 Act these categories do not include middle-ranking or more junior officials. An individual ceases to be a PEP after he has left office for one year.
Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to designated persons as their position makes them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates. PEP status therefore puts a customer into a higher risk category although if the business is not aware of any factors that would place the individual in a higher risk category, the individual may be categorised as a low risk PEP.

OmniPro – Anti Money Laundering Guidance

4. Customer Due Diligence (CDD) *(continued)*

In relation to PEPs, a firm is required to take the following steps prior to establishing a business relationship with a client (or beneficial owner) or carrying out a transaction:

- Have appropriate risk-based procedures to determine whether the customer is a PEP;
- Obtain appropriate senior management approval prior to establishing a business relationship with a PEP; and
- Take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction

Firms must treat PEPs on a case-by-case basis, and apply EDD on the basis of their assessment of the money laundering risk associated with any individual PEPs. Regardless however of the risk rating of the PEP the firm is required to conduct enhanced ongoing monitoring of the business relationship.

Relying on third parties to carry out CDD

In certain circumstances a firm can rely on CDD carried out on a potential customer or beneficial owner by another third party. This is permitted only if the other third party is a member of the regulated sector in an EEA or non-EEA state, to an equivalent regulatory regime which includes compliance supervision requirements equivalent to the EU Directive.

Reliance on the third party for CDD is conditional that both parties enter into an agreement (that should be in writing) to ensure that the other party will provide the CDD documentation immediately on request. The CDD carried out is for the purposes of:

- identifying and verifying a customer;
- identifying and verifying the beneficial owner of a customer, if relevant, and
- obtaining information on the purpose and intended nature of the business relationship.

It is important to note that, the firm engaging in the business relationship with the customer remains liable for any failure by the third party to carry out the CDD correctly.

Accordingly the firm must confirm with the third party that they (the third party) will keep the identification and verification data and other relevant documentation on the identity of the customer and that the third party accepts the obligation to provide information to the firm as soon as practicable on request.

OmniPro – Anti Money Laundering Guidance

4. Customer Due Diligence (CDD) *(continued)*

Examples of circumstances where a firm might rely on the fact that a third party has already undertaken CDD measures in relation to a customer include:

- where a firm enters into a business relationship with, or undertakes a service for, a customer through a network group referral.
- where one member of a financial group introduces a client to another member company of the same group.
- Where a firm is providing subcontracted work for another firm, on behalf of a client

Example

Firm, A, is engaged by another firm, B, to help with work for one of its clients or some other underlying party, C, then A should consider whether its client is in fact B, not C. For example, where there is no business relationship formed, nor is there an engagement letter between A and C, it may be that CDD on C is not required but should instead be completed for B.

However, on the other hand, where there is significant contact with the underlying party, or where a business relationship with it is believed to have been established, then C may also be deemed a client and CDD may be required for both C and B.

Gathering Evidence and Certifying Copies of Documents

Client verification means to verify on the basis of documents or information 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 can be regarded as being independent.

It is important that verification procedures are undertaken on a risk-sensitive basis. Therefore the collection of information and its extent is linked to firm risk assessment and the client specific risk assessment.

To support compliance and proof of the verification the firm's staff should certify that the original documents were seen by the relevant employee prior to making or receiving the document. Effectively that relevant employee is endorsing the copy with a clear indication of the date in which they are doing so. The relevant person should also state their position within the firm to clearly identify that the relevant person has the knowledge and understanding of what they are certifying having obtained the appropriate training to do so in accordance with the firms policies and procedures and firms risk assessment criteria.

In the event the relevant person in receipt of the documents has not viewed the original documents that relevant person should clearly document that it is not an original and the original has not been viewed to ensure the firm in assessing the client risk profile is aware of the risk posed by the information supplied. If possible the information should be validated by way of firm verification checks, such as independent confirmation and follow up procedures.

In summary for all documents received the source of the document and date received to the firm should be indicated

OmniPro – Anti Money Laundering Guidance

4. Customer Due Diligence (CDD) *(continued)*

Delays in the provision of Information

Customer due diligence procedures are not required before a prospective client agrees to become a client of the firm. However, they may sometimes request that you start work straightaway if there is an imminent deadline such as that for filing a tax return or making an investment before the tax year end, and some clients will not like the delay whilst you undertake identification procedures.

Section 33 of the 2010 Act allows 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 must be completed as soon as practicable after the initial contact.

So essentially it may be acceptable to have a short extension (to allow for information collection to be completed) provided the cause of the delay is administrative or logistical, not the client's reluctance to cooperate. It should be noted however that these circumstances are expected to be rare and it should be approved by the MLRO or senior management before starting work without full customer due diligence information.

A firm should understand that if the client is able to deliver books, records or other documents to be worked on it should also be practicable to provide proof of identity at the same time. Therefore the firm should be in a heightened situation of AML at preliminary stages which may impose a duty to report to the authorities while the service is given the perception of being performed to ensure tipping off does not occur until the firm obtains satisfactory evidence of identity, or decides not to continue with the business relationship.

The key is to train staff (including the administration staff) to request this information when setting up meetings, rather than first raising it during the meetings.

OmniPro – Anti Money Laundering Guidance

5. Reporting of suspicious transactions

Identifying a Suspicious Transaction

For an accountancy firm or its employees to recognise what is suspicious to a certain client means that the individuals working on the assignment must have a good knowledge of the client and of the industry sector in which that client operates and in addition be able to recognise what is suspicious.

A suspicious transaction is one which makes you question what it is, or what it is for thereby raising a suspicion that it does not sit comfortably within the client profile.

For example:

- If there is a complex business structure for no apparent reason;
- If deals are set up using large amounts of cash;
- If the client has in the past changed financial adviser frequently for no apparent reason;
- If the client wants the firm to handle or hold large amounts of money for no apparent purpose;
- If they are using overseas representatives or agents;
- If there are large amounts of travel that cannot be commercially justified;
- If they have been or want to invest in financial products but appear more interested in cancellation terms rather than performance;
- If the client has no clear source of funds; or
- If the client wants to utilise trust vehicles for no apparent reason.

In addition there are other issues to consider as an accountant;

- Does the client receive large payments from overseas which are matched to equal payments leaving the clients account at a similar time;
- Has the client purchased or sold services or products at a price which is significantly above or below its commercial worth;
- Without commercial justification have they become unexplainably more profitable;
- Are they paying fees or commissions which are unusual for the business sector in which they operate;
- Do they not keep proper records; or
- Is there a high turnover compared to other clients in the same sector.

To be able to carry out an appropriate assessment of these factors it is essential that the firm knows its client and the client's business sector in great detail.

The Reporting Obligations

A firm is required to have internal reporting procedures in place that facilitate their employees disclosing their concerns if they know or suspect that someone (whether a client or not) is involved in money laundering activities through reports to the firm's MLRO.

Prior to submitting a report they may wish to discuss the issue with the partner, manager or principal in charge of the assignment, who may be able to provide additional information that will help them decide whether a report is needed. However, the decision to report or not is their personal decision, since the liability for failure to report is also theirs to bear.

NOTE Discussing the issue with your partner, manager or principal is not a report to the firm's MLRO.

OmniPro – Anti Money Laundering Guidance

5. Reporting of suspicious transactions *(continued)*

Once an internal report has been made to the MLRO regarding a suspicion with a client or a suspicious transaction it is up to the MLRO to consider the report in the light of any relevant available information and determine whether it gives rise to such knowledge or suspicion (or reasonable grounds for knowledge or suspicion). If so and external report must be reported to An Garda Siochana and the Financial Intelligence Unit[7] via GoAML (https://fiu-ireland.ie/Home)

Making an External Report

Since 12 June 2017, reports by accountants about money laundering suspicion can only be submitted electronically to An Garda Síochána via the new goAML website.
goAML is an online software solution specifically designed by the United Nations Office on Drugs and Crime (UNODC) for use by state Financial Intelligence Units (FIUs) throughout the world.

Suspicious Transaction Reports (STRs) pursuant to section 42 Criminal Justice (Money Laundering & Terrorist Financing) Act 2010 were previously received by the FIU and Office of the Revenue Commissioners in paper format. However, from 12 June 2017, goAML is the online system through which designated bodies, including accountants, will submit money laundering suspicion reports to An Garda Síochána and in paper form to the Revenue Commissioners. **An Garda Síochána have advised that they will no longer accept paper reports on the ML1 Standard Reporting Form and all designated bodies, including solicitors, must submit reports using goAML.**

Once a report has been made to the Garda Síochána the Financial Investigation Unit will provide the firm with an acknowledgement and every user of goAML can view his or her already submitted reports along with their current status.

If either the suspect or the transaction cannot be linked to criminal conduct then the MLRO will receive feedback that no further action will be taken.
A detailed user guide to goAML can be viewed at the following location,
http://www.antimoneylaundering.gov.ie/en/AMLCU/ITS_goAMLWeb_Userguide.pdf/Files/ITS_goAMLWeb_Userguide.pdf

In the event the MLRO has determined an External Report is required to be made, the MLRO should ensure a copy of the submission made to the Financial Intelligence Unit is retained. The MLRO should print a copy of the submission made for the firm records, and in addition a copy of the submission made should be sent to the Revenue Commissioners.

A suspicious activity report may be followed by requests for further information from FIU Ireland or the Revenue Commissioners. Firms need to have in place procedures for checking the validity of any such requests and for ensuring a proper response is made.

[7] The Financial Intelligence Unit (FIU) is part of the efforts of Government in combating money laundering and the financing of terrorist activity. The core role of the FIU is to serve as the country's central reception point for the receipt, analysis and dissemination of information contained in Suspicious Transaction Reports (STRs) and other reports from competent authorities regarding suspicions of money laundering and terrorist financing.

OmniPro – Anti Money Laundering Guidance

5. Reporting of suspicious transactions *(continued)*

It is an offence for an suspicion or known knowledge of money laundering and terrorist financing having not been reported to the FIU Ireland however there are the following defences against failure to disclose:

- There is a reasonable excuse for not making the disclosure. However, it is anticipated that only relatively extreme circumstances – such as duress or threats to safety – would be accepted;
- The privileged circumstances exemption applies; (**NOTE** - Audit work, book-keeping, preparation of accounts or tax compliance assignments are unlikely to take place in privileged circumstances)
- The relevant employee concerned did not know about or suspect MLTF and had not received the training required by Regulation 54 of the 2010 Act. As no training was provided, the relevant employee is not bound by bjective test – i.e., to always report when there are 'reasonable grounds' for knowledge or suspicion – but the business has committed an offence by failing to provide training.

Only sole practitioners, who employ no relevant employees, have a duty to submit suspicious transaction reports straight to the FIU Ireland.

Failure to report can carry a fine of up to €5,000 or on conviction an imprisonment term of up to 5 years.

Tipping Off or Prejudicing an Investigation

Once a report has been made it is important for the firm and for its employees to ensure that they do not tip off the client that a report has been made or carry out any actions which could prejudice any investigation which may be undertaken.

The term 'Tipping Off' refers to the firm or individual within the firm alerting the client or other third parties to the fact that a report has been made in respect of a suspicion of money laundering or terrorist financing or that an investigation is underway or maybe carried out.

Tipping off is not only prohibited by the Act but is listed as an offence which can carry a fine of up to €5,000 or on conviction an imprisonment term. Tipping off would be any activity which would prejudice an investigation.

An offence is not committed if a relevant professional adviser makes a disclosure to another within the same profession (e.g. accountancy) but from a different business, who is of the same professional standing (including with respect to their duties of professional confidentiality and protection of personal data), when that disclosure:

- relates to a single client or former client of both advisers; and
- involves a transaction or the provision of a service that involves both of them; and
- is made only for the purpose of preventing a money laundering offence; and
- is made to a person in an EU member state or a state imposing equivalent AML requirements.

The MLRO needs to ensure that they are familiar with the 2010 Act to ensure they know what disclosures can or cannot be made.

OmniPro – Anti Money Laundering Guidance

5. Reporting of suspicious transactions *(continued)*

The firm, for example, is permitted to make normal commercial enquiries to understand a transaction which has been carried out in the course of an engagement and this will not generally lead to the prejudicing of an investigation however care must be taken not to alert the client and it is important to restrict any enquiries to only those which would be required in the normal course of the engagement.

In particular a firm must not attempt to investigate the matter unless the matter falls within the scope of the professional engagement.

In complex circumstances consultation with the Garda Síochána may be necessary before enquiries are continued.

If any doubt exists the firm or individual should seek legal advice.

OmniPro – Anti Money Laundering Guidance

6. Record Keeping

The Core Obligations for Keeping Records

Firms must retain:

- copies of, or references to, the evidence they obtained of a customer's identity, for not less than five years after the end of the customer relationship; and
- details of customer transactions for five years from the date of the transaction.

Firms should retain:

- details of actions taken in respect of internal and external suspicious transaction reports; and
- details of information considered by the MLRO in respect of an internal report where no external report is made.

Firms must delete any personal data relating to CDD and client transactions in accordance with Section 55 of the 2010 Act revised, firm should also be mindful that this has a correlation with a firms GDPR obligation not to retain personal client information for a period longer than is necessary once the business relationship has ceased and there is no longer a legal basis for the holding or processing of that data.

What records have to be kept?

The precise nature of the records required is not however the objective is to ensure that a firm meets its obligations and that, in so far as is practicable, in any subsequent investigation the firm can provide the authorities with its section of the audit trail.

The firm's records should cover:

- Customer information
- Transactions
- Internal and external suspicion reports
- Other records being;
    - MLRO annual firm review (and other institute or external review) reports;
    - Information not acted upon; and
    - Training and AML compliance monitoring.

Customer information

For the purpose of verifying a customer's identity, firms must keep a copy of any documents or information it obtained to satisfy the CDD measures required for AML under the 2010 Act.

In the event a firm identifies a customer as requiring enhanced customer due diligence or ongoing monitoring additional information will be sought and this will also be required to be retained.

Where a firm is relying on third party verification and has received a certificate confirming identity, this certificate will in practice be the evidence of identity that must be kept.

Any records of identification evidence must be kept for a period of five years after the business relationship with the customer has ended, i.e. the ceasing of service or receipt of final payment.

OmniPro – Anti Money Laundering Guidance

6. Record Keeping *(continued)*

Upon the expiry of the five year period referred, firms must delete any personal data unless:

- the firm is required to retain records containing personal data by, or for the purposes of any court proceedings, or under, any other enactment; or
- the firm has reasonable grounds for believing that records containing the personal data need to be retained for the purpose of legal proceedings; or
- the data subject has given consent to the retention of that data.

If a firm if acting as a third party verifier as that firm is being relied on by another firm for customer due diligence purposes, that firm must keep the records of the verified client and the certification provided for five years from the ending of the business relationship with the client.

Where documents verifying the identity of a client are held in one part of a group, they do not need to be held in duplicate form in another. The records do, however, need to be accessible to the nominated officer or MLRO of the Group and to all areas that have contact with the client, and be available on request, to enforcement bodies.

When an introducing branch or subsidiary undertaking ceases to trade or have a business relationship with that client, but the wider group continues to have an active business relationship the group must ensure copies of records are retained for at least five years as the business relationship has not ceased for the group as a whole. Likewise this is relevant if the branch or subsidiary ceased to be part of the group.

Most firms have standard procedures which they keep under review, and will seek to reduce the volume of records which need 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;
- in scanned form; or
- other electronic form.

Regardless of the format in which they are kept, or whether the transaction was undertaken by paper or electronic means, the record retention requirements are the same.

Transactions

All transactions carried out on behalf of or with a client in the course of relevant business relationship must be recorded within the firm's records. Transaction records in support of entries in the accounts, should be maintained in a form from which a satisfactory audit trail may be compiled.

Records of all transactions relating to a client must be retained for a period of five years from:

- where the records relate to an occasional transaction, the date when the transaction is completed; or
- in other cases, the date the business relationship ended, i.e. the ending of the service provided.

OmniPro – Anti Money Laundering Guidance

6. Record Keeping *(continued)*

But: a firm is not required to retain records relating to transactions occurring in a business transaction relationship for more than 6 years[8]. Upon the expiry of this period, as previously stated firms must delete any personal data unless:

- the firm is required to retain records containing personal data by, or for the purposes of any court proceedings, or under, any other enactment; or
- the firm has reasonable grounds for believing that records containing the personal data need to be retained for the purpose of legal proceedings; or
- the data subject has given consent to the retention of that data.

Internal and external reports

A firm should make and retain:

- records of actions taken under the internal and external reporting requirements; and
- when the MLRO has considered information or other material concerning possible money laundering, but has not made a report to the FIU Ireland / GoAML, a record of the other material that was considered.

In addition, copies of any Suspicious Transaction Reports made to the FIU Ireland / GoAML should be retained.

As with other AML records, records of all internal and external reports should be retained for at least five years from the date the report was made.

Other Records

Section 54 (6) of the 2010 Act states "*A designated person shall ensure that persons involved in the conduct of the designated person's business are—*

a) instructed on the law relating to money laundering and terrorist financing, and

b) *provided with ongoing training on identifying a transaction or other activity that may be related to money laundering or terrorist financing, and on how to proceed once such a transaction or activity is identified.*"

Therefore in support of this at a minimum a firm's records in relation to training should include:

- dates AML training was given;
- the nature of the training; and
- the names of the staff who received training.

The next section of this guidance document will deal with specific obligations on training of staff.

A firm's records should also demonstrate compliance with the monitoring of AML internally and should include: -

- any reports by the MLRO to senior management; and
- any records of consideration of those reports and of any action taken as a consequence.

[8] GDPR requires that personal information be subject to appropriate security measures and retained for no longer than necessary for the purpose for which it was originally acquired. Note that the period of Statute of Limitations in Ireland for a civil case is 6 years.

OmniPro – Anti Money Laundering Guidance

6. Record Keeping *(continued)*

A firm must establish and maintain systems which enable it to respond fully and rapidly to enquiries from the FIU Ireland or a member of Garda Síochána not below the rank of Sergeant, relating to:

- whether it maintains, or has maintained during the previous five years, a business relationship with any person;
- the nature of that relationship;

and if necessary the provision of documents or records.

There is no restriction on the relevant records required to be maintained in Ireland so long as the information can be accessed and provided promptly. However, where identification records are held outside Ireland, it is the responsibility of the Irish firm to ensure that the records available do in fact meet Irish legislative requirements. No secrecy or data protection legislation should restrict access to the records either by the firm, or by Irish law enforcement agencies upon request. If it is found that such restrictions exist, copies of the underlying records of identity should, wherever possible, be sought and retained within the Ireland.

OmniPro – Anti Money Laundering Guidance

7. Training and Awareness

Responsibilities of the Firm for the training of Staff and awareness for AML

Section 54(6) requires a firm ensures that persons involved in the firms day to day business are:

- instructed on the law relating to money laundering and terrorist financing, and
- provided with ongoing training on identifying a transaction or other activity that may be related to money laundering or terrorist financing, and on how to proceed once such a transaction or activity is identified.

One of the most important controls over the prevention and detection of money laundering is to have staff who are alert to the risks of money laundering/terrorist financing and well trained in the identification of unusual activities or transactions which may prove to be suspicious. The effective application of even the best designed control systems can be quickly compromised if the staff applying the systems are not adequately trained.

Accordingly employees should be

- made aware of the risks of money laundering and terrorist financing, the relevant legislation, and their obligations under that legislation
- made aware of the identity and responsibilities of the firm's nominated officer and MLRO
- trained in the firm's procedures and in how to recognise and deal with potential money laundering or terrorist financing transactions or activity

To support the ongoing aspect of the legislation the staff training should be given at regular intervals, and details appropriately recorded.

In accordance with paragraph (7) of section 54 of the 2010 Act an MLRO is responsible for oversight of the firm's compliance including its requirements in respect of staff training and in support of this a director or senior manager has overall responsibility for the establishment and maintenance of the effectiveness of the training arrangements as per paragraph (8) of the same section.

The overall objective of training is not for employees to develop a specialist knowledge of criminal law. However, failure of the firm to provide such training as a result of staff being unable to identify money laundering and terrorist activity can result in a fine and or imprisonment of up to five years.

Training methods and its content

There is no single solution when determining how to deliver training; a mix of training techniques may be appropriate. On-line learning can often provide an adequate solution for many employees, but there will be those types of employees for whom such an approach is not suitable and so focused classroom training can be more effective.

Ongoing training should be given at appropriate intervals to all employees. Particularly in larger firms, this may be required at regular frequent intervals where there is regular intake of new employee's and to ensure new employee have appropriate training and fully understand the money laundering requirements and procedures of the firm.

OmniPro – Anti Money Laundering Guidance

7. Training and Awareness *(continued)*

Training programmes should be tailored so that employees understand the AML risks posed by the specific services they provide and types of client they deal with, and so are able to appreciate, on a case-by-case basis, the approach they should be taking in accordance with the firms AML procedures. Furthermore, firms should aim to create an AML culture in which employees are always applying a risk based approach to CDD and ongoing monitoring so they are alert to the risks of money laundering and terrorist financing.

Frequency of Training

As described in the previous section, records should be kept showing who has received training, the training received and when training took place.

However, the frequency of the training can be influenced by changes in legislation, regulation, professional guidance, case law and judicial findings (both domestic and international), also as explained earlier the country and profession risk assessments/profiles may require specific consideration. A change in a firms service offering may also require a revision in the AML training required to be given to employee's (i.e. Investment Business authorisation).

Therefore, it may be appropriate to provide employees with concise updates to help refresh and expand their knowledge and to remind them how important effective anti-money laundering work is.

We believe that being an accountant should be a profitable and rewarding experience. We support accountants technically and strategically to ensure you meet your regulatory compliance requirements in the most efficient and profitable manner possible. Accountants are uniquely placed to successfully lead Ireland into the future. We want to work with you to ensure that you are fully equipped for the task.

As the largest independent solution provider to Irish accountants, we have worked with hundreds of practices from the largest international firms to sole practitioners and everything in between. We offer Technical Practice Advisory, File Review Services, Practice Management & Growth Services, Company Law and Company Secretarial Services, Company Formations, Tax Planning and Consultancy Services, Public CPD Training and In-house Training.

OMNIPRO PRACTICE SUPPORT

+ Technical Support Service
+ File Review Services
+ Practice Development Services
+ In-House Training

OMNIPRO COMPANY SECRETARIAL

+ Company Law Advice
+ Company Secretarial Compliance
+ Annual Compliance Services
+ Company Formations

OMNIPRO

OMNIPRO EDUCATION & TRAINING

+ Technical CPD
+ Non-Technical CPD
+ Online CPD
+ CPD Planning Services

OMNIPRO TAX & LEGAL

+ Tax Support Services for Accountants
+ Your Outsourced Tax Department
+ Advanced Tax Planning
+ Tax Efficient Structures

OMNIPRO PRACTICE GROWTH

+ Value Added Tools for Revenue Growth
+ Marketing Strategy Development
+ Marketing Consultancy
+ Marketing Campaign Management

For further information visit www.OmniPro.ie

+ Practice Support + Company Secretarial + Tax & Legal + Practice Growth + Education & Training

info@omnipro.ie | +353 1 411 0000 | +353 53 910 0000

Firm Address
Firm Address

Anti-Money Laundering Declaration of a Third Party

If you have any queries in relation to completing this form, please contact us at xxxxxxxxxx

Name of Practice	
Address of Practice	
Name of Designated Accountancy Body Or Other Professional Body or Financial Institution	
Name of Declarant	

I hereby confirm that we are a Relevant Third Party as defined as in the Criminal Justice (Money Laundering & Terrorist Financing) Act 2010 and 4th EU AML Directive being:-

1	A credit institution	
2	A financial institution	
3	An external accountant or auditor and who is a member of a designated accountancy body	
4	A tax adviser and who is also a solicitor or a member of a designated accountancy body or of the Irish Taxation Institute	
5	A relevant independent legal professional	
6	A trust or company service provider and who is also a member of a designated accountancy body, a solicitor or individual authorised to carry on business by the Central Bank and Financial Services Authority of Ireland or Other appropriately authorised individual	

I hereby confirm that we will perform appropriate Customer Due Diligence in respect of the Client Name on all future engagements when Client Name shall be engaged with FIRM NAME in full compliance with the Criminal Justice (Money Laundering & Terrorist Financing) Act 2010 and 4th EU AML Directive.

I hereby confirm that if requested to do so, we will forward to FIRM NAME, as soon as practicable, any documents (whether or not in electronic form) or information relating to the customer that we have obtained in applying CDD.

And I make this declaration conscientiously believing the same to be true.

_____ _____

Date

For and on behalf of