The Irish Accounting & Tax Summit 2020

Session 7

Anti-Money Laundering for Accountants in 2020

Presenter:
Colm Owens & Mike O'Halloran - OmniPro

OmniPro Education & Training
Main Street, Ferns, Enniscorthy, Co. Wexford
053 9100000
www.omnipro.ie info@omnipro.ie

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

OMNIPRO
Let Your Expertise Benefit From Ours

www.omnipro.ie

Anti Money Laundering Update

- Webevent Timing - 11:00 – 12:00
- Teaching Space – 50 Minutes
- Questions and Answers – 10 Minutes

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**: Risk Assessment and Customer Due Diligence
- **Topic 4:** Reporting Procedures and Privilege Exemption
- **Topic 5:** Update on COVID-19 and legislative updates

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

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).

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)**

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

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

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

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

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

OMNIPRO
Let Your Expertise Benefit From Ours

www.omnipro.ie

What do you need to 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

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

OMNIPRO
Let Your Expertise Benefit From Ours

www.omnipro.ie

Customer Due Diligence

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

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

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

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

Customer Due Diligence

- Different types of CDD
  - Standard Due Diligence
  - Simplified Due Diligence
  - Enhanced Due Diligence
  - Politically Exposed Persons
  - Third Party Reliance

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

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

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 and where clients are not met in person

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

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

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

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

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'

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

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

OMNIPRO
Let Your Expertise Benefit From Ours

www.omnipro.ie

How to make reports

- New 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
- The Office of the Revenue Commissioners will accept a printed copy of the STRs submitted on goAML

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)

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.

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

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

OMNIPRO
Let Your Expertise Benefit From Ours

www.omnipro.ie

5th Money Laundering Directive

- Key Features
  - Centralised beneficial ownership register
  - Preventing the use of letterbox companies
  - Enhanced due diligence for nationals from risky countries
  - Extending the scope of industries subject to AML legislation
  - Limit the use of electronic money currencies
  - Enhance the powers of the EU FIUs
  - Provide protection for whistleblowers

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

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

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

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.

COVID-19

- Reporting to MLRO issues
- AML Reporting
  - GO AML
  - Revenue

OMNIPRO
Let Your Expertise Benefit From Ours

www.omnipro.ie

Q&A

??

Why OmniPro

Our Why -

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

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

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.

OMNIPRO
Let Your Expertise Benefit From Ours

www.omnipro.ie

OmniPro
Supporting Irish Accountants

Main Street,

Ferns,

Enniscorthy,

Co. Wexford.

053 9100000

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	Low risk	No single client can be said to be any more focused than usual on their reduction of tax
		Y	Medium Risk	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	Low risk	The firm has no offshore clients
		Y	Low risk	While the firm does act for Offshore trusts and/or companies, the beneficial owners and intended purpose of the Trust/Company is known
		Y	Medium Risk	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	Low 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
		Y	Medium Risk	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	Low risk	There are no identified clients or beneficial owners of clients located in higher risk jurisdictions.
		Y	High Risk	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				

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.

TECHNICAL RELEASE 01/2019

Anti-Money Laundering Guidance
Republic of Ireland

This publication is based on requirements of Irish legislation regarding anti-money laundering and prevention of terrorist financing. It has been developed having appropriate reference to the Consultative Committee of Accountancy Bodies (CCAB) document 'Anti-Money Laundering Guidance for the Accountancy Sector (UK)'. Members of CCAB-I acknowledge the permission given by CCAB for the use of their document in the development of this publication.

May 2019

DISCLAIMER

This publication has been jointly developed by the member bodies of the Consultative Committee of Accountancy Bodies – Ireland (CCAB-I), being the Institute of Chartered Accountants in Ireland, The Association of Chartered Certified Accountants, The Institute of Certified Public Accountants and Chartered Institute of Management Accountants.

The content of this publication is provided as a guide only and does not purport to give professional advice. It should, accordingly, not be relied upon as such. No party should act or refrain from acting on the basis of any material contained in this publication without seeking appropriate professional advice. While every reasonable care has been taken by the member bodies of the Consultative Committee of Accountancy Bodies - Ireland (CCAB-I) in the preparation of this publication we do not guarantee the accuracy or veracity of any information or opinion, or the appropriateness, suitability or applicability of any practice or procedure contained therein. The member bodies of the CCAB-I are not responsible for any errors or omissions or for the results obtained from the use of the information contained in this publication.

To the fullest extent permitted by applicable law, the member bodies of the CCAB-I exclude all liability for any damage, costs, claims or loss of any nature, including but not limited to indirect or consequential loss or damage, loss of business profits or contracts, business interruption, loss of revenue or income, loss of business opportunity, goodwill or reputation, or loss of use of money or anticipated saving, loss of information or loss, damage to or corruption of data, whether arising from the negligence, breach of contract or otherwise of the member bodies of the CCAB-I, their committee members, employees, servants or agents, or of the authors who contributed to the text, even if advised of the possibility of such damages.

Similarly, to the fullest extent permitted by applicable law, the member bodies of the CCAB-I shall not be liable for any indirect or consequential losses including but not limited to, loss of business profits or contracts, business interruption, loss of revenue, loss of business opportunity, goodwill or reputation, or loss of use of money or anticipated saving, loss of information or damage to or corruption of data, nor shall it be liable for any damage, costs or losses of any nature (whether direct or indirect) occasioned by actions, or failure to act, by users of this publication or by any third party, in reliance upon the contents of this publication, which result in damages or losses incurred either by users of this publication, for whom they act as agents, those who rely upon them for advice, or any third party, or for any breach of contract by the member bodies of the CCAB-I in respect of any inaccurate, mistaken or negligent misstatement or omission contained in this publication.

Any issues arising out of the above will be governed by and construed in accordance with the laws of Ireland and the courts of Ireland shall have exclusive jurisdiction to deal with all such issues.

Introduction

Accountants, together with other professionals and *financial institutions,* are key gatekeepers for the financial system, facilitating vital *transactions* that underpin the Irish economy. As such, they have an important role to play in ensuring their services are not used to further or assist a criminal purpose. As professionals, accountants must act with integrity and uphold the law, and they must not engage in criminal activity.

This Anti-Money Laundering Guidance has been developed by a *CCAB-I* working party comprising staff and volunteer practitioners and has been approved for issue by bodies affiliated to the CCAB-I. **This guidance is based on the law as of November 2018. It covers the prevention of money laundering and the countering of *terrorist financing*. It is intended to be read by any member who provides audit, accountancy, tax advisory, insolvency, or trust and company services in the Republic of Ireland.**

CONTENTS

Contents

1 ABOUT THIS GUIDANCE

- What is the purpose of this guidance?
- Who is the guidance for?
- What is the legal status of this guidance?

1.1 What is the purpose of this guidance?

1.1.1 **The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 has been amended by the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018, which gives effect to certain provisions of the Fourth Money Laundering Directive (Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015).** In this document, the '*2010 Act*' refers to the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 as amended by the Criminal Justice Act 2013 and the Criminal Justice (Money Laundering and Terrorist Financing (Amendment) Act 2018.

1.1.2 Key changes introduced by the amending Act include greater emphasis on identification of beneficial owners of businesses, a wider definition of politically exposed persons, a requirement to apply procedures based on an enhanced risk based approach to assess and respond to potential money laundering or terrorist financing, enhanced requirements relating to client identification, and the removal of an earlier duty to report in relation to conduct of business with parties connected with a *high risk jurisdiction*, regardless of specific assessed risks arising from such business. This guidance has been prepared to help accountants undertaking activities that bring them within the definition of *designated persons* as set out in section 25 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2019 (see paragraph 1.2.1) to fulfil their obligations under the updated Irish legislation (in effect from 26 November 2018) to prevent, recognise and report money laundering. Compliance with it will assist compliance with the relevant legislation (including that related to counter *terrorist financing*) and professional requirements.

1.1.3 Terms that appear in *italics* in this Guidance are explained in the Glossary.

1.1.4 The term 'must' is used throughout to indicate a mandatory legal or regulatory requirement. *Accountancy firms* may seek an alternative interpretation of the Irish anti-money laundering and terrorist financing (AML) regime, but they must be able to justify their decision to their competent authority.

1.1.5 Where the law requires no specific course of action, 'should' is used to indicate good practice sufficient to satisfy statutory and regulatory requirements. *Accountancy firms* should consider their own particular circumstances when determining whether any such 'good practice' suggestions are indeed appropriate to them. Alternative practices can be used, but *firms* must be able to explain their reasons to their *competent authority*, including why they consider them compliant with law and regulation.

1.1.6 The Irish anti-money laundering regime applies only to *defined services* carried out by designated *businesses*. This guidance assumes that many a*ccountancy firms* will find it easier to apply certain AML processes and procedures to all of their services, but this is a decision for the *firm* itself. It may be unnecessarily costly to apply anti-money laundering provisions to services that do not fall within the *Irish AML regime*.

1.1.7 This guidance takes account, where relevant, to guidance issued by bodies other than *CCAB-I*. When those bodies revise or replace their guidance, the references in this document should be assumed to refer to the latest versions.

1.1.8 An *accountancy firm* may use AML guidance issued by other trade and professional bodies, where that guidance is better aligned with the specific circumstances faced by the *firm*. Where the *firm* relies on alternative guidance, it must (in accordance with 1.1.2 of this guidance) be in a position to explain this reliance to their *competent authority.*

1.1.9 The law which comprises the *Irish AML regime* is largely contained in the following legislation and relevant statutory instruments (SIs):

Legislation:

- Criminal tice (Money Laundering and Terrorist Financing) Act 2010;
- Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018;
- Criminal Justice (Corruption Offences) Act 2018;
- Criminal Justice Act 2011;
- Criminal Justice Act 2013, Part 2;
- Criminal Justice (Terrorist Offences) Act 2005.

Statutory Instruments:

- SI 486 of 2018 Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018 (Commencement) Order 2018
- SI 487 of 2018 Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Section 25) (Prescribed Class of Designated Person) Regulations 2018;
- SI 298 of 2018 Criminal Justice (Corruption Offences) Act 2018 (Commencement) Order 2018;
- SI No. 342 of 2010 Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Commencement) Order 2010
- SI No. 453 of 2016 Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Competent Authority and State Competent Authority) Regulations 2016;
- SI No. 79 of 2014 Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Competent Authority) Regulations 2014;
- SI No. 167 of 2013 Trust or Company Service Provider Authorisation (Appeal Tribunal) (Establishment) Order 2013;
- SI No. 347 of 2012 Criminal Justice (Money Laundering and Terrorist Financing) (Section 31) Order 2012;
- SI No. 348 of 2010 Trust or Company Service Provider (Authorisation) (Fees) Regulations 2010;
- SI No. 343 of 2010 Criminal Justice (Money Laundering and Terrorist Financing) (Section 31) Order 2010;

- SI No. 342 of 2010 Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Commencement) Order 2010.

1.1.10 The *2005 Act* and *2010 Act* contain the Money Laundering and Terrorist Financing offences that can be committed by *individuals* or organisations. The *2010 Act* sets out the systems and controls that *firms* are obliged to possess, as well as the related offences that can be committed by *firms* and key *individuals* within them.

1.2 Who is this guidance for?

1.2.1 The guidance is addressed to those *designated persons* which are *accountancy firms* and members of the *CCAB-I* bodies, covered by Section 25 of the *2010 Act,* who act in the course of a business carried on by them in Ireland as

- an auditor,
- *an external accountant,*
- an insolvency practitioner,
- a *tax advisor*
- a provider to of investment advice under the Investment Business Regulations, and
- those who act in the course of business as *trust or company service providers* under Section 84 of the *2010 Act*.

For the purposes of this guidance the services listed above are collectively referred to as *defined services*. The scope of what would be considered carrying on business in Ireland is broad, and would include certain cross border business models where day to day management takes place from an Irish registered office or Irish head office.

1.2.2 Section 24 of the *2010 Act* defines an *external accountant* as someone who provides *accountancy services* to other persons by way of business. There is no definition given for the term *accountancy services*, however for the purposes of this guidance it includes any service which involves the recording, review, analysis, calculation or reporting of financial information, and which is provided under arrangements other than a contract of employment.

1.2.3 This guidance does not cover any other services, guidance for which may be available from other sources.

1.2.4 Guidance related to secondees and subcontractors can be found in APPENDIX A.

1.3 What is the legal status of this guidance?

1.3.1 This guidance has been prepared to assist accountants fulfil their legal obligations under legislation in force at the time of issue. This guidance is not intended to be exhaustive. If in doubt, seek appropriate advice or consult your supervisory authority. A copy of the guidance has been provided to the Department of Justice for information: however, formal approval has not been issued. The guidance will be updated for any matters of concern notified to us by the Department.

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.

2 MONEY LAUNDERING DEFINED

- What is money laundering?
- What is the legal and regulatory framework?

2.1 What is money laundering?

2.1.1 Definitions can be found in the Glossary section of this guidance. In this section, the definition of money laundering is discussed.

2.1.2 Money laundering is defined very widely in Irish law. It includes all forms of handling or possessing the *proceeds of criminal conduct* (as well as facilitating the use or possession) regardless of how it was obtained.

2.1.3 The '*proceeds of criminal conduct*' may take any form, including:

- Money or money's worth;
- Saved costs;
- Securities; and
- Tangible or intangible property.

Money laundering can involve the proceeds of offences committed in Ireland but also, in certain circumstances, of conduct overseas that; (i) is an offence in the place where the conduct takes place; and (ii) would have been an offence had it taken place in Ireland. There is no need for the proceeds to pass through Ireland. For the purposes of this guidance, except where otherwise stated, money laundering also includes *terrorist financing*. There are no materiality or 'de minimis' exceptions to *money laundering* or *terrorist financing* (*MLTF*) *offences*.

2.1.4 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 the *proceeds of criminal conduct*; or
- Concealing the *proceeds of criminal conduct* or entering into arrangements to assist others to do so.

2.1.5 *Accountancy firms* need to be alert to the risks posed by:

- *Client*s;
- Suppliers;
- Employees; and
- The customers, suppliers, employees and associates of *client*s.

2.1.6 Neither the *firm* nor its *client* needs to have been party to money laundering for a reporting obligation to arise (see Section 6 of this guidance).

2.2 What is the legal and regulatory framework?

2.2.1 Sections 6 to 11 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (the "***2010 Act***") define the primary *money laundering offences*. Inside or outside the *regulated sector* someone commits a *money laundering offence* if they,

knowing or believing (or being reckless as to whether or not) that property is or 'probably comprises' the *proceeds of criminal conduct*, engages in any of the following acts in relation to the property:

- Concealing or disguising the true nature, source, location, disposition, movement or ownership or the property, or any rights relating to the property;
- Converting, transferring, handling, acquiring, possessing or using the property;
- Removing the property from, or bringing the property into, the State.

Any of these offences is punishable by up to 14 years' imprisonment and/or an unlimited fine.

2.2.2 None of these offences is committed if:

- The persons involved did not know or suspect (and were not reckless as to whether or not) that they were dealing with the *proceeds of criminal conduct*; or
- In advance of the possession or handling of the *proceeds of criminal conduct*, a report of the suspicious *transaction* is made promptly either by an *individual* internally in accordance with the procedures established by the accountancy firm (an *internal report*) or by an *individual* or an *accountancy firm* direct to:
    - *FIU Ireland* within the Garda Síochána (via the GoAML online reporting system); and
    - The Revenue Commissioners,

  before the act is committed. Section 42(7) of the *2010 Act* allows for such a report to be made immediately afterwards if it is not practicable to delay or stop the *transaction* or service from proceeding or the *accountancy firm* 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 ('*tipping off*'); or
- The conduct giving rise to the *proceeds of criminal conduct* has taken place outside of Ireland, and the conduct was in fact lawful under the criminal law of the country/territory in which the act occurred.

2.2.3 The following offences apply to *designated persons* and *individuals* connected with a *designated person*:

- Failure to report (Section 42 of the *2010 Act*) a suspicion (or reasonable grounds for suspicion) of money laundering. Remember: there is **no 'de minimis' threshold value for reporting**.
- Disclosing that a suspicious transaction report *(STR)* has been made, or is required to be made, in a way that is likely to prejudice any subsequent investigation (which may also be referred to as a '*tipping off*' offence . For further information on the offences of ***prejudicing and investigation*** or ***tipping off'*** (Section 49 of the *2010 Act*) see Section 6 of this guidance.

2.2.4 In addition, there are reportable offences under the Criminal Justice (Terrorist Offences) Act 2005 (the "***2005 Act***"). These offences focus on the expected use of funds, regardless of their source.

3 RESPONSIBILITY & OVERSIGHT

- What are the responsibilities of *Accountancy firms*?
- What are the responsibilities of *senior management*, *MLRO* or other *nominated officer*?
- What policies, procedures and controls are required?

3.1 What are the responsibilities of *Accountancy firms*?

3.1.1 For *Accountancy firms* providing *defined services*, the *2010 Act* requires anti-money laundering systems and controls that meet the requirements of the *Irish anti-money laundering regime*. The *2010 Act* imposes a duty to ensure that persons involved in the conduct of the *firm's* business (see Section 8 of this guidance) are kept aware of these systems and controls and are trained to apply them properly. *Accountancy firms* are explicitly required to:

- Monitor and manage their own compliance with the *2010 Act*; and
- Ensure that policies, controls and procedures adopted in accordance with the *2010 Act* are approved by *senior management* and that such policies, controls and procedures are kept under review, in particular when there are changes to the business profile or risk profile of the *firm*.

3.1.2 *Accountancy firms* need to establish systems that create an internal environment or culture in which people are aware of their responsibilities under the *Irish anti-money laundering* regime and where they understand that they are expected to fulfil those responsibilities with appropriate diligence. In deciding what systems to install, an *accountancy firm* will need to consider a range of matters including:

- the type, scale and complexity of its operations;
- the different business types it is involved in;
- the types of services it offers, and its *client* profiles;
- how it sells its services;
- the risks associated with each area of its operations in terms of the risks of the *accountancy firm* or its services being used for *money laundering* or terrorist operations, or the risks of its *clients* and their counterparties being involved in such operations.

3.1.3 If a *firm* fails to meet its obligations under the *2010 Act*, civil penalties or criminal sanctions can be imposed on the *firm* 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.

3.1.4 The primary *money laundering offences* defined under the *2010 Act* (see 2.2 of this guidance) can be committed by anyone inside or outside the regulated sector but *the 2010 Act* imposes specific provisions on *designated persons*.

3.1.5 *Accountancy firms* must have systems and controls capable of: assessing the risk associated with a *client*; performing CDD; *monitoring* existing *client*s; keeping

appropriate records; and enabling staff to make an internal *STR* (i.e. *to the firm's Money Laundering Reporting Officer* ('*MLRO*') or other nominated person having responsibility for oversight of the *firm's* anti-money-laundering and reporting procedures. *).*

3.1.6 All persons involved in the conduct of the *accountancy firm's* business must be trained appropriately so that they understand both their own personal AML obligations and the firm-wide systems and controls that have been developed to prevent *MLTF*.

3.1.7 Effective internal risk management systems and controls must be established and the relevant *senior management* responsibilities clearly defined.

3.1.8 The *Competent Authority* for the *Accountancy firm* may, by formal request in writing, require that the *firm:*

- 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*;
- Appoint a member of *senior management* with primary responsibility for the implementation and management of anti-money laundering measures; and/or
- Undertake an independent, external audit to test the effectiveness of the internal policies, controls and procedures outlined in this section.

3.2 What are the responsibilities of *Senior Management/MLRO*?

3.2.1 The *2010 Act* defines *senior management* as: an officer or employee of the *Accountancy firm* with sufficient knowledge of the *firm's MLTF* risk exposure, and with sufficient authority, to take decisions affecting its risk exposure.

3.2.2 The *2010 Act* requires that the approval of *senior management* must be obtained:

- for the *firm's business risk assessment* (section 30A(5) of the *2010 Act*)
- for the policies, controls and procedures adopted by the *firm* (*2010 Act* section 54(4)).

3.2.3 Members of *senior management* undertaking such responsibilities should receive Continuing Professional Development (CPD) appropriate to their role.

3.2.4 Where requested under the *2010 Act* sections 54(7) or 54(8) to appoint an *individual* at management level to monitor and manage the *Accountancy firm's* internal policies, controls and procedures or to appoint a member of *senior management* with primary responsibility for the implementation and management of the *Accountancy Firm's* anti-money laundering measures the appointed *individual* should have:

- an understanding of the *accountancy firm*, its service lines and its *client*s;
- sufficient seniority to direct the activities of all members of staff (including senior members of staff);
- the authority to ensure the *firm's* compliance with the regime;
- the time, capacity and resources to fulfil the role;
- authority to represent that firm in legal proceedings.

3.2.5 A Money Laundering Reporting Officer ("*MLRO")* or other *nominated officer* may be appointed by the *accountancy firm* to manage its internal reporting procedures, taking responsibility for receiving internal *STRs* and making external *STRs* to the State Financial Intelligence Unit (*FIU Ireland*) and the Revenue Commissioners. This individual should also have the characteristics noted above.

3.2.6 Although not required under the *2010 Act*, unless requested by the *Competent Authority* under section 54 of the *2010 Act*, depending on the size, complexity and structure of an *Accountancy firm*, the *firm* may find it beneficial to appoint an *individual* at management level or to appoint a member of *senior management* with responsibility for ensuring the *firm's* compliance with the Irish anti-money laundering regime.

3.2.7 This role of ensuring the *firm's* compliance with the Irish anti-money laundering regime and that of the *MLRO* 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 *MLRO.* The role of the *MLRO* is not defined in legislation but has traditionally included responsibility for internal controls and risk management around *MLTF*, in accordance with sectoral guidance. *Accountancy firms* 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 *firm* in relation to the effective management of *MLTF* risk; and
- the *MLRO* has the seniority, authority, governance responsibility, time, capacity and resources to fulfil the brief.

3.2.8 The *accountancy firm* should ensure that there are sufficient resources to undertake the work associated with the *MLRO*'s role. This should cover normal working, planned and unplanned absences and seasonal or other peaks in work. Arrangements may include appointing deputies and delegates. When deciding upon the number and location of deputies and delegates, the firm should have regard to the size and complexity of the *firm's* service lines and locations. Particular service lines or locations may benefit from a deputy or delegate with specialised knowledge or proximity. Where there are deputies, delegates or both (or when elements of *firm's* AML policies, controls and procedures are outsourced), the *MLRO* retains ultimate responsibility for the *firm's* compliance with the Irish anti-money laundering regime.

3.2.9 All *MLROs*, deputies and delegates should undertake CPD appropriate to their roles.

3.2.10 The *MLRO* should:

- have oversight of, and be involved in, *MLTF* risk assessments;
- take reasonable steps to access any relevant information about the *firm*;
- obtain and use national and international findings to inform their performance of their role;
- create and maintain the firm's risk based approach to preventing *MLTF*;
- support and coordinate management's focus on *MLTF* risks in each individual business area. This involves developing and implementing systems, controls, policies and procedures that are appropriate to each business area;

- take reasonable steps to ensure the creation and maintenance of *MLTF* documentation;
- develop *Customer Due Diligence (CDD)* and on-going *monitoring* policies and procedures (including whether a customer is a 'politically exposed person' or '*PEP*'), consultation with and internal reporting to the *MLRO* (where applicable) or other *individual*(s) within the organisation as appropriate, and dissemination of such policies and procedures to all relevant staff;
- ensure the creation of the systems and controls needed to enable staff to make internal *STRs* in compliance with *2010 Act*;
- receive internal *STRs* and make external *STRs* to the *FIU Ireland* and the Revenue Commissioners;
- take remedial action where controls are ineffective;
- draw attention to the areas in which systems and controls are effective and where improvements could be made;
- take reasonable steps to establish and maintain adequate arrangements for awareness and training;
- monitoring the compliance of the *Accountancy firm* with the policy and procedures including reporting to *senior management* on compliance and addressing any identified deficiencies;
- receive the findings of relevant audits and compliance reviews (both internal and external) and communicate these to the board (or equivalent managing body);
- report to the *Accountancy firm's* leadership team (or equivalent managing body) at least annually, providing an assessment of the operations and effectiveness of the *firm's* AML systems and controls. This should take the form of a written report. These written reports should be supplemented with regular ad hoc meetings or comprehensive management information to keep *senior management* engaged with AML compliance and up-to-date with relevant national and international developments in AML, including new areas of risk and regulatory practice. The firm's leadership team (or equivalent managing body) should be able to demonstrate that it has given proper consideration to the reports and ad hoc briefings provided by the *MLRO* and then take appropriate action to remedy any AML deficiencies highlighted.

3.3 What policies, procedures and controls are required?

3.3.1 The *2010 Act* places certain requirements on *Accountancy firms* regarding *CDD* (Chapter three of Part 4 of the *2010 Act*) and 'record keeping, procedures and training' (Chapter six of Part 4 of the *2010 Act*). The following topics, all of which form part of the *MLTF* framework, need to be considered:

- risk based approach, risk assessment and management;
- *CDD*;
- record keeping;
- internal control;

- ongoing *monitoring*;
- reporting procedures;
- compliance management;
- communication;
- training and awareness.

3.3.2 The *2010 Act* provides different amounts of detail about the policies and procedures required in each area. *Accountancy firms* must implement and document policies, controls and procedures that are proportionate to the size and nature of the *firm*. These should be subject to regular review and update, and a written record of this exercise maintained.

Risk assessment and management

3.3.3 Every *Accountancy firm* must have appropriate policies and procedures for assessing and managing *MLTF* risks. To focus resources on the areas of greatest risk, a risk based approach must be adopted. The *firm* must carry out a *firm* risk assessment to identify and assess the risks of money laundering and *terrorist financing* involved in the *firm's* business activities. Such a *firm* risk assessment must at least take account of the risk factors set out in Section 30(A), Schedule 3 and Schedule 4 of the *2010 Act* (Schedule 3 and Schedule 4 of the *2010 Act* are reproduced in Appendix E to this guidance) (e.g. the type of customer, the products and services that are provided etc.) and the *firm* risk assessment must be approved by *senior management*. The *firm* risk assessment, and any related documents, should be kept up to date in accordance with the a*ccountancy firm's* internal policies, controls and procedures with new and changing risks considered as and when they are identified. Resources like the National Risk Assessment for Ireland, the Financial Action Task Force (*FATF*) mutual evaluations and Transparency International's corruption perception index can be useful when determining the *MLTF* risk faced by a firm. Information from the firm's *Competent Authority* must be taken into account. Further information on the risk based approach, types and categories of risk can be found in Section four of this guidance.

Customer Due Diligence (CDD)

3.3.4 *Accountancy firms* are responsible for developing *CDD* policies and procedures. These procedures should ensure that staff are aware of the factors to consider when assessing whether or not to establish a *business relationship* or undertake an *occasional transaction*, in light of the *MLTF* risks associated with the *client* and *transaction*. To ensure that the correct procedures are being followed, staff must be made aware of their obligations under the *2010 Act* and given appropriate training.

3.3.5 *Accountancy firms* already have procedures to help them avoid conflicts of interest and ensure they comply with professional requirements for independence. The requirements of the *2010 Act* can either be integrated into these procedures, to form a consolidated approach to taking on a new *client*, or addressed separately. For more on *CDD* see Section 5 of this guidance.

Reporting

3.3.6 Under *the 2010 Act* the reporting of knowledge or suspicion of money laundering is a legal requirement. It is the responsibility of the *Accountancy firm* to develop and

implement internal policies, procedures and systems that are able to satisfy the *2010 Act* reporting requirements. Those policies must set out clearly, (a) what is expected of an *individual* who becomes aware of, or suspects, money laundering, and (b) how they report their concerns to the *MLRO.* All *staff* must be trained in these procedures.

More information on reporting suspicious *transactions* can be found in Section 6 of this guidance.

Record keeping

3.3.7 All records created as part of the *CDD* process, including any non-engagement documents relating to the *client* relationship and ongoing *monitoring* of it, must be retained for five years after the relationship ends. All records related to an *occasional transaction* must be retained for five years after the *transaction* is completed. A disengagement letter could provide documentary evidence that a *business relationship* has terminated, as could other forms of communication such as an unambiguous email making it clear that the *Accountancy firm* does not wish to engage or is ceasing to act.

3.3.8 Although no comparable retention period is specified for information and communications relating to internal and external *STRs*, a firm may wish to retain these securely for at least a period that meets the criteria set out by the Statute of Limitations.

3.3.9 *Accountancy firms* should bear in mind their obligation under the Data Protection Legislation 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 as necessary.

3.3.10 Where directed by a member of the Garda Síochána, not below the rank of Sergeant, the *Accountancy firm* may be required to retain documents and other records for a period up to a maximum of five years, additional to the initial period referred to at 3.3.8, for the purposes of an investigation related to money laundering or *terrorist financing*.

3.3.11 *Senior management* must ensure that all staff are made aware of these retention policies and that they remain alert to the importance of following them. There is more information on record keeping in Section 7 of this guidance.

Training and awareness

3.3.12 The *2010 Act* requires persons involved in the conduct of the *Accountancy firm's* business are made aware of the law relating to *MLTF* and given regular training in how to recognise and deal with suspicious *transactions* which may be related to *MLTF.* Though the *2010 Act* contains no express requirement, it is considered to be best practice for these provisions to be applied to all partners in *Accountancy firms* and to sole practitioners and to train all client-facing staff. In considering a training plan, *accountancy firms* need to keep in mind the objectives they are trying to achieve, which is to create an environment in relation to its business to prevent and detect the commission of money laundering and which thereby helps protect *individuals* and the *accountancy firm*.

3.3.13 The firm/*MLRO* should establish training capable of ensuring that staff:

- Are aware of what money laundering and *terrorist financing* is and how it is undertaken;

- Are aware of their legal and regulatory duties;
- Understand how to put those requirements into practice in their roles; and
- Are continuously updated about changes in
  (a) the *firm's* AML policies, systems and controls, and
  (b) the *MLTF* risks faced.

3.3.14 A formal training plan can help make sure that *staff* receive the right training to enable them to comply with their AML obligations.

3.3.15 Training should be tailored to suit the particular role of the *individual*.

3.3.16 Training methods may be selected to suit the size, complexity and culture of the *firm*, and may be delivered in a variety of ways including face to face, self-study, e-learning and video, or a combination of methods. *Accountancy firms* should keep records of attendance at, or completion of, training.

3.3.17 *Accountancy firms* need to make arrangements to ensure new members of staff or other *individuals* are trained as soon as possible after they join.

3.3.18 An *Accountancy firm* that fails to provide training for *staff* could be in breach of the *2010 Act* and at risk of prosecution. It would also risk failing to comply with Section 42 of *the 2010 Act*, which requires *Accountancy firms* to disclose any suspicions of money laundering. Although a 'reasonable excuse' defence against a failure to disclose for the *individual* (note that there is no money laundering case law on this issue and it is anticipated that only relatively extreme circumstances, such as duress and threats to safety, might be accepted) or the *professional privilege reporting exemption* provided under Section 46 of the *2010 Act* may be availed of, the *2010 Act* may still have been breached by the *Accountancy firm* because adequate training was not provided. For further information on training and awareness refer to Section 8 of this guidance.

Monitoring policies and procedures

3.3.19 The *MLRO* and/or appropriate *senior management* should together monitor the effectiveness of policies, procedures and processes so that improvements can be made when inefficiencies are found. Risks should be monitored and any changes must be reflected in changes to policies and procedures; keeping them up-to-date, in line with the risk assessment of the *Accountancy firm.* For more information, see Section 4 of this guidance.

3.3.20 In their efforts to improve AML policies, controls and procedures, and better understand where problems can arise, *senior management* should encourage staff to provide feedback. When changes are made to policies, procedures or processes these should be properly communicated to staff and supported by appropriate training where necessary.

3.3.21 *Accountancy firms* must introduce a system of regular, independent reviews to understand the adequacy and effectiveness of the *MLTF* systems and any weaknesses identified. Independent does not necessarily mean external, as some *firms* will have internal functions (typically audit, compliance or quality functions) that can carry out the reviews. Any recommendations for improvement should be monitored. Existing *monitoring* programmes and their frequency can be extended to include AML. The reviews should be proportionate to the size and nature of the *Accountancy firm.* A

sole practitioner with no employees need not implement regular, independent reviews unless required by their *Competent Authority*.

3.3.22 As part of their improvement efforts the *senior manager* responsible for compliance and/or the *MLRO* should monitor publicly-available information on best practice in dealing with *MLTF* risks. For example, thematic reviews by regulators can be useful ways to improve understanding of good and poor practice, while reports on particular enforcement actions can illuminate common areas of weakness in AML policies, controls and procedures.

4 RISK BASED APPROACH

- What is the role of the risk based approach?
- What is the role of *senior management*?
- How should the risk analysis be designed?
- What is the risk profile of the *accountancy firm*?
- How should procedures take account of the risk based approach?
- What are the different types of risk?
- How important is documentation?

4.1 What is the role of the risk based approach?

4.1.1 The risk based approach is fundamental to satisfying the *FATF* recommendations, the *EU Directive* and the overall Irish *MLTF* regime. It requires governments, supervisors and *accountancy firms* alike to analyse the *MLTF* risks they face and make proportionate responses to them. It is the foundation of any *firm's* AML policies, controls and procedures, particularly its *CDD* and staff training procedures.

4.1.2 The risk based approach recognises that the risks posed by *MLTF* activity will not be the same in every case and so it allows the *firm* to tailor its response in proportion to its perceptions of risk. The risk based approach requires evidence-based decision-making to better target risks. No procedure will ever detect and prevent all *MLTF*, but a realistic analysis of actual risks enables a *firm* to concentrate the greatest resources on the greatest threats.

4.1.3 The risk based approach does not exempt low risk *client*s, 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.

4.1.4 This section provides guidance on the analyses the *firm* will need to perform to properly underpin a risk based approach. Guidance on applying the risk based approach to particular AML procedures and controls can be found in the relevant sections of this guidance dedicated to those procedures.

4.2 What is the role of *senior management*?

4.2.1 *Senior management* is responsible for managing all of the risks faced by the *firm*, including *MLTF* risks. *t* should ensure that *MLTF* risks are analysed, and their nature and severity identified and assessed, in order so as to produce a risk profile. *Senior management* should then act to mitigate those risks in proportion to the severity of the threats they pose.

4.2.2 Where a risk is identified, the *firm* must design and implement appropriate procedures to manage it. The reasons for believing these procedures to be appropriate should be supported by evidence, documented and systems created to monitor effectiveness. A *firm's* risk based approach should evolve in response to the findings of the systems monitoring the effectiveness of the AML policies, controls and procedures.

4.2.3 The risk analysis can be conducted by the *MLRO*, but must be approved by *senior management* (see section 30A of the *2010 Act*) . This is likely to include formal

ratification of the outcomes, including the resulting policies and procedures, but may also include close *senior management* involvement in some or all of the analysis itself.

4.2.4 The risk profile and operating environment of any *firm* changes over time. The risk analysis must be refreshed regularly by periodic reviews, the frequency of which should reflect the *MLTF* risks faced and the stability or otherwise of the business environment. In addition, whenever *senior management* sees that events have affected *MLTF* risks, the risk analysis should also be refreshed by an event-driven review. A fresh analysis may require AML policies, controls and procedures to be amended, with consequential impacts upon, for example, the training programs for relevant employees.

4.3 How should a risk analysis be designed?

4.3.1 One possible first step is to consider the *MLTF* risks faced by each different part of the *firm*. The *firm* may already have general risk analysis processes, and these could form the basis of its *MLTF* risk analysis.

4.3.2 When designing an analysis process the *firm* should look not only at itself but at its *client*s and markets as well. Consider factors that lower risks as well as those that increase them; a *client* subject to an effective *AML regime* may pose a lower risk than one not. *Accountancy firms* should take into account the findings of the most recent National Risk Assessment, together with any guidance issued by the relevant *competent authority,* including Schedules 3 and 4 of the *2010 Act* (as reproduced in Appendix D of this guidance).

4.3.3 *MLTF* risks include the possibility that the *firm* might:

- Be used to launder money (e.g. by holding criminal proceeds in a fund or a *client* money account, or by becoming involved in an arrangement that disguises the beneficial ownership of criminal proceeds);
- Be used to facilitate *MLTF* 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);
- Suffer consequential legal, regulatory or reputational damage because a *client* (or one or more of its associates) is involved in money laundering;
- Fail to report a suspicion of MLTF.

4.3.4 Risks should be grouped into categories, such as '*client*', 'service' and 'geography'. Some risks will not easily fit under any one heading but that should not prevent them from being considered properly. Nor should a *firm* judge overall risk simply by looking at individual risks in isolation. When two threats are combined they can produce a total risk greater than the sum of the parts. A particular industry and a particular country may each be thought to pose only a moderate risk. But when they are brought together, perhaps by a particular *client* or *transaction*, then the combined risk could possibly be high. *Firms* should avoid taking a 'tick-box' approach to assessing *MLTF* risk in relation to any individual *client* but should, instead, take reasonable steps to assess all information relevant to its consideration of the risk.

4.4 What is the risk profile of the *accountancy firm*?

4.4.1 An *accountancy firm* with a relatively simple *client* base and a limited portfolio of services may have a simple risk profile. In which case, a single set of AML policies,

controls and procedures may suffice right across its operations. On the other hand, many *firms* will find that their risk analysis reveals quite different *MLTF* risks in different aspects of the *firm*. *Accountancy services*, for example, may face significantly different risks to insolvency, bankruptcy and recovery services. A risk analysis allows resources to be targeted, and procedures tailored, to address those differences properly.

4.4.2 When a *firm* decides to have different procedures in different parts of its operations, it should consider how to deal with *client*s whose needs straddle departments or functions, such as:

- A new *client* who is to be served by two or more parts of the *firm* with different AML policies, controls and procedures;
- An existing *client* who is to receive new services from a part of the *firm* with its own distinct AML policies, controls and procedures.

4.4.3 The risk based approach can also take into account the *firm's* experience and knowledge of different commercial environments. If, for example, it has no experience of a particular country, it could treat it as a normal or high risk even though other *firms* might consider it low risk. Similarly, if it expects to deal with only Irish individuals and entities, it may treat as high risk any *client* associated with a non-Irish country.

4.5 How should procedures take account of the risk based approach?

4.5.1 Before establishing a *client* relationship or accepting an engagement an *accountancy firm* must have controls in place to address the risks arising from it. The risk profile of the *firm* should show where particular risks are likely to arise, and so where certain procedures will be needed to tackle them.

4.5.2 Risk based approach procedures should be easy to understand and easy to use for all staff who will need them. Sufficient flexibility should be built in to allow the procedures to identify, and adapt to, unusual situations.

4.5.3 The nature and extent of AML policies, controls and procedures depend on:

- The nature, scale, complexity and diversity of the *firm*;
- The geographical spread of *client* operations, including any local AML regimes that apply; and
- The extent to which operations are linked to other organisations (such as networking businesses or agencies).

4.5.4 *Accountancy firms* should have different *client* risk categories such as: low, normal, and high. The procedures used for each category should be suitable for the risks typically found in that category. For example, if it is normal for a *firm* to deal with *client*s from a *high-risk country*, the *firm's* procedures for what they regard as normal *client*s must be designed to address the risks associated with the *high-risk country*. Some low and high risk indicators can be found in APPENDIXD.

4.5.5 Regardless of the risk categorisation, *firms* will still be expected to undertake *monitoring* of the *client* relationship. Such *monitoring* must be done on a risk based approach, with levels of *monitoring* varying depending on the *MLTF* risk associated with individual *client*s.

4.5.6 Taking into account key risk categories, an *accountancy firm* may be able to draw up a simple matrix in order to determine a *client*'s risk profile. Such risk categories may include a *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, *firms* should also consider the nature of the service being offered to a *client* and the channels through which the services/*transactions* are being delivered.

4.5.7 Elevated risks could be mitigated by:

- Conducting enhanced levels of due diligence – i.e., increasing the level of *CDD* that is gathered.
- Carrying out periodic *CDD* reviews on a more frequent basis.
- Putting additional controls around particular service offerings or *client*.

4.6 What is *client* risk?

4.6.1 A *firm* should consider the following question, "Does the *client* or its beneficial owners have attributes known to be frequently used by money launderers or terrorist financiers?"

4.6.2 *Client* risk is the overall *MLTF* risk posed by a *client* based on the key risk categories, as determined by a *firm*.

4.6.3 The *client*'s risk profile may also inform the extent of the checks that need to be performed on other associated parties, such as the *client*'s beneficial owners.

4.6.4 Undue *client* secrecy and unnecessarily complex ownership structures can both point to heightened risk because company structures that disguise ownership and control are particularly attractive to people involved in *MLTF*.

4.6.5 In cases where a *client* (an individual) or beneficial owner of a *client* is identified as a *PEP* (including a domestic *PEP*), an enhanced level of due diligence must be performed on the *PEP*. Further details on the approach to be taken in such circumstances are set out in 5.3.11 - 5.3.22 of this guidance.

4.7 What is service risk?

4.7.1 A *firm* should consider the following question "Do any of our products or services have attributes known to be used by money launderers or terrorist financiers?"

4.7.2 Service risk is the perceived risk that certain products or services present an increased level of vulnerability in being used for *MLTF* purposes.

4.7.3 *Firms* should consider carrying out additional checks when providing a product or service that has an increased level of *MLTF* vulnerability.

4.7.4 Services and products in which there is a serious risk that the *accountancy firm* itself could commit a *money laundering offence* should also be treated as higher risk. For example, wherever the *accountancy firm* may commit an offence under Sections 7 and 10 to 11 or 30A(1)(b) of the *2010 Act* such as the use of the *accountancy firm's client* monies account to inadvertently facilitate money laundering.

4.7.5 Before a *firm* begins to offer a service significantly different from its existing range of products or services, it should assess the associated *MLTF* risks and respond appropriately to any new or increased risks.

4.8 What is geographic risk?

4.8.1 A *firm* should consider the following question "Are our *client*s established in countries that are known to be used by money launderers or terrorist financiers?"

4.8.2 Geographic risk is the increased level of risk that a country poses in respect of *MLTF*.

4.8.3 When determining geographic risk, reference should be made to the EU identification of higher risk jurisdictions (see Appendix D): other factors to consider may include the perceived level of corruption, criminal activity, and the effectiveness of *MLTF* controls within the country.

4.8.4 *Firms* should make use of publicly available information when assessing the levels of *MLTF* of a particular country, e.g. information published by civil society organisations such as Transparency International and public assessments of the *MLTF* framework of individual countries (such as *FATF* mutual evaluations and the EU designation of *high risk financial jurisdictions*).

4.8.5 Although some countries may carry a higher level of *MLTF* risk, those *firms* that have extensive experience within a given country may reach a geographical risk classification that differs to those that that only have a limited exposure (refer to http://www.centralbank.ie/ for a list of countries).

4.9 What is sector risk?

4.9.1 A *firm* should consider the following question "Do our *client*s have substantial operations in sectors that are favoured by money launderers or terrorist financiers?"

4.9.2 Sector risks are the risks associated with certain sectors that are more likely to be exposed to increased levels of *MLTF*.

4.9.3 *Firms* should consider the sectors in which their *client* has significant operations, and take this into account when determining a *client*'s risk profile. When considering what constitutes a high risk sector, *firms* should take into account the findings of the most recent National Risk Assessment (available at www.justice.ie) for Ireland, together with any guidance issued by the relevant *competent authority* for the *designated person*.

4.10 What is delivery channel risk?

4.10.1 A *firm* should consider the following question "Does the fact that I am not dealing with the *client* face to face pose a greater *MLTF* risk?"

4.10.2 Certain delivery channels can increase the *MLTF* risk, because they can make it more difficult to determine the identity and credibility of a *client*, both at the start of a *business relationship* and during its course.

4.10.3 For example, delivery channel risk could be increased where services/products are provided to *client*s who have not been met face-to-face, or where a *business relationship* with a *client* is conducted through an intermediary.

4.10.4 *Firms* should consider the risks posed by a given delivery channel when determining the risk profile of a *client*, and whether an increased level of *CDD* needs to be performed.

4.11 Why is documentation important?

4.11.1 *Accountancy firms* must be able to demonstrate to their relevant *competent authority* how they assess and seek to mitigate *MLTF* risks. This *firm* risk assessment must be documented, and made available to the relevant *competent authority* on request. The documentation should demonstrate how the *accountancy firm's* risk assessment informs their policies and procedures. *Accountancy firms'* risk assessments must also be approved by *senior management* and kept up to date in accordance with internal policies, controls and procedures.

5 *CUSTOMER DUE DILIGENCE (CDD)*

- What is the purpose of *CDD*?
- When should *CDD* be carried out?
- How should *CDD* be applied?
- What happens if *CDD* cannot be performed?

5.1 What is the purpose of *CDD*?

5.1.1 Criminals often seek to mask their true identity by using complex and opaque ownership structures. The purpose of *CDD* is to know and understand a *client*'s identity and business activities so that any *MLTF* risks can be properly managed. Effective *CDD* is, therefore, a key part of AML defences. By knowing the identity of a *client*, including who owns and controls it, a *firm* not only fulfils its legal and regulatory requirements it equips itself to make informed decisions about the *client*'s standing and acceptability.

5.1.2 *Customer due diligence* measures are a key part of the anti-*money laundering* requirements. They ensure that *accountancy firms* know who their *clients* are, ensure that they do not accept *clients* unknowingly which are outside their normal risk tolerance, or whose business they will not understand with sufficient clarity to be able to form *money laundering* suspicions when appropriate. If an *accountancy firm* does not understand its *client's* regular business pattern of activity it will be very difficult to identify any abnormal business patterns or activities. In addition, *accountancy firms* must be in a position to supply the *client's* identity in the event that the *accountancy firm* is required to submit an *external report* to *FIU Ireland* and the Revenue Commissioners.

5.1.3 Many *accountancy firms* will have other procedures for *client* acceptance, for example to ensure compliance with professional requirements for independence and to avoid conflicts of interest. The requirements of the *2010 Act,* may either be integrated with those procedures or addressed separately. In either case, initial *customer due diligence* information not only assists in acceptance decisions, but also enables the *accountancy firm* to form well-grounded expectations of the *client*'s behaviour which provides some assistance in detecting potentially suspicious behaviour during the *business relationship.*

5.1.4 The processes required for compliance with anti-money laundering initial *customer due diligence* requirements contribute vitally to the overall picture of potential *clients* and appropriate risk assessment of them. However a lack of concern raised during *customer due diligence* does not mean that the *client* and engagement will remain in their initial risk category. Continued alertness for changes in the nature or ownership of the *client*, its business model, or its susceptibility to money laundering – or actual evidence of the latter – must be maintained.

CDD principles

5.1.5 Sections 33 through 39 of the *2010 Act4* the required components of *CDD*. *Accountancy firms* must apply them, (a) at the start of a new *business relationship* (including a company formation), (b) at appropriate points during the lifetime of the relationship and (c) when an *occasional transaction* is to be undertaken. The required components are:

- Identifying the *client* (i.e., knowing who the *client* is) and then verifying their identity (i.e., confirming that identity is valid by obtaining documents or other information from sources which are independent and reliable) (see Appendix B);
- Identifying beneficial owner(s) so that the ownership and control structure can be understood and the identities of any individuals who are the owners or controllers can be known and, on a risk sensitive basis, reasonable measures should be taken to verify their identity; and
- Gathering information, reasonably warranted by the risk of money laundering or *terrorist financing* on the intended purpose and nature of the *business relationship*.

5.1.6 When determining the degree of *CDD* to apply, the *firm* must adopt a risk based approach, taking into account the type of *client*, *business relationship*, product or *transaction*, and ensuring that the appropriate emphasis is given to those areas that pose a higher level of risk (see Section 4 of this guidance). For this reason it is important that risks are assessed at the outset of a *business relationship* so that a proportionate degree of *CDD* can be brought to bear.

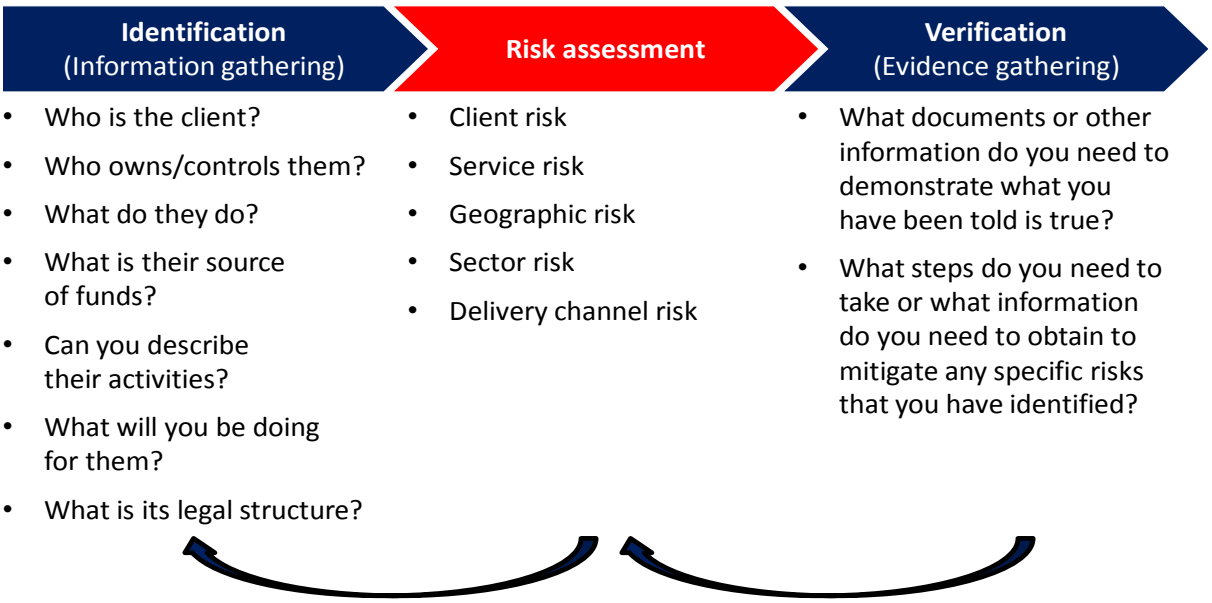
5.1.7 Where the work to be performed falls within the scope of *defined services*, the *firm* must ensure that *CDD* is applied to new and existing *clients* alike. For existing *clients*, *CDD* information gathered previously should be reviewed and updated where it is necessary, timely and risk-appropriate to do so.

5.1.8 The *2010 Act* stipulates that *CDD* must also be performed where there is either a suspicion of *MLTF*, or any doubts about the reliability of the identity information, or documents obtained previously for verification purposes.

5.1.9 Where there is such knowledge or suspicion the *firm* needs to consider not only whether the existing *CDD* information is sufficient and up-to-date, but also whether an external *STR* should be made to *FIU Ireland* and the Revenue Commissioners.

5.1.10 While the *2010 Act* prescribes the level of *CDD* that should be applied in certain situations (i.e. simplified or enhanced – for more on this see section 5.3 of this guidance), it does not describe how to do this on a risk-sensitive basis. Nonetheless, a *firm* is expected to be able to demonstrate to the relevant *competent authority* that the measures it applied were appropriate in accordance with its own risk assessment. Section 4 of this guidance outlines broadly the key areas to be considered when developing a risk based approach including (amongst other factors) the purpose, regularity and duration of the *business relationship*.

Stages of CDD



5.1.11 The arrows in the diagram above represent feedback loops by which an initial risk assessment or verification may highlight a need for more information to be gathered or a fresh risk assessment performed.

5.1.12 The identification phase requires the gathering of information about a *client's* identity and the purpose of the intended *business relationship* before entering into a *business relationship*. This applies to single *transactions* or a series of linked *transactions* valued in excess of €15,000. 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 correspondence file. 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 , and further detail on how to deal with them can be found in 5.1.16 onwards of this guidance. *A* designated person shall also verify any person purporting to act on behalf of a customer and verify the identity of that person.

5.1.13 The next stage of *CDD* is risk assessment. This should be performed in accordance with the risk based approach guidance contained in Section four of this guidance, and must reflect the purpose, regularity and duration of the *business relationship,* as well as the size of *transactions* to be undertaken by the *client* and the *firm's* own risk assessment. An initial risk assessment is based on the information gathered during stage one (identification), but this may prompt the gathering of additional information as indicated by the left-hand feedback loop. The right-hand feedback loop shows that additional risk assessment may be required in the light of stage three (verification).

5.1.14 Once an initial risk assessment has been carried out, evidence is required to verify the identity information gathered during the first stage. This is called *client* verification. Verification involves validating (with an independent, authoritative source), that the identity is genuine and belongs to the claimed individual or entity. For an individual, verification may require sight of a passport (with a photocopy taken). For corporates and others, in addition to the *client* itself, reasonable verification measures for any individual beneficial owners must also be considered on a risk sensitive basis.

5.1.15 Further guidance on the type of information that should be gathered and the documents that can be used to verify it, can be found in paragraph 5.3.34 onwards..

Beneficial ownership

Definition

5.1.16 A beneficial owner can only be a natural person i.e., an individual (other than in the case of a trust, see below).

5.1.17 Sections 26 through 30 set out in some detail the meaning of beneficial owner in terms of bodies corporate, partnerships, trusts, estates of deceased persons and a catch all provision that, where not otherwise specified, defines the beneficial owner as the person who ultimately owns or controls the *client* or on whose behalf a service or *transaction* is being conducted. The table below gives a summary of how beneficial ownership could be established for a variety of entities:

***Client* type**	**Voting Rights**	**Shares**	**Capital or profits**	**Other means of ownership/control**
Companies whose securities are listed on a *EEA* regulated investment market or equivalent				No requirement to establish beneficial ownership
Bodies corporate	>25%	>25%		Any individual who ultimately owns or controls whether through direct or indirect ownership or control (including through bearer shareholdings) more than 25% of the shares or voting rights in the body, or who otherwise exercises control over the management of the body
Partnerships	entitled to or controls >25%		entitled to or controls >25%	Any individual who ultimately is entitled to or controls (whether entitlement or control is direct or indirect), more than 25% of the capital or profits of the partnership or more than 25% of the voting rights in the partnership, or who otherwise exercises control over the management of the partnership
Trusts				The beneficiaries (or where some/all have not yet been determined, the class of persons in whose main interest the trust is set up or

Client type	Voting Rights	Shares	Capital or profits	Other means of ownership/control
				operates) The settlor , the trustee, the protector 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
Estates of deceased individuals				The executor or administrator of the estate
All other cases Where all possible means of identifying the beneficial owner of a body corporate have been exhausted and recorded				The individual who ultimately owns or controls the *client*, or on whose behalf a *transaction* is being conducted, 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*).

5.1.18 *Accountancy firms*, in accordance with their legal obligations, need to be diligent in their enquiries about beneficial ownership, taking into account that the information they need may not always be readily available from public sources. A flexible approach to information gathering will be needed as it will often involve direct enquiries with *clients* and their advisers as well as searches of public records in Ireland and overseas. 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%.

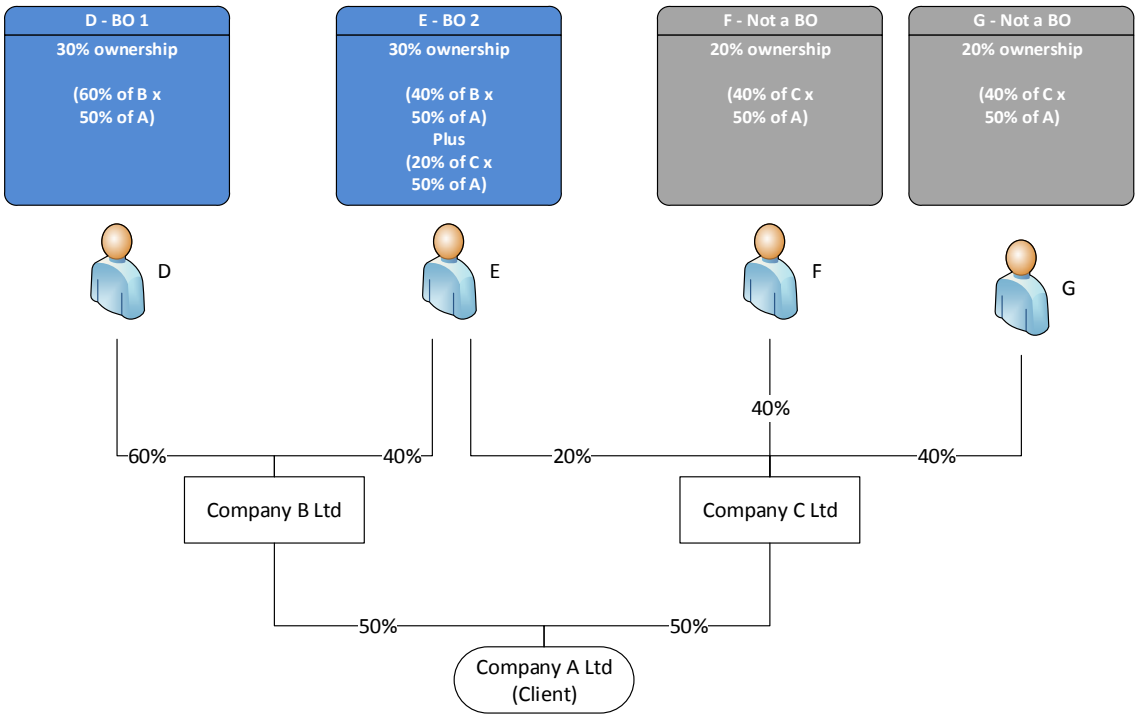
5.1.19 Some possible options of verifying the identity of beneficial owners include:

- Requesting from the customer documentary evidence from an independent source detailing the beneficial owners;
- Searches of the relevant company registry;
- Electronic searches either direct or via a commercial agency for electronic agency for electronic verification;
- The beneficial ownership register maintained by the company.

Determining beneficial owners in respect of complex structures

5.1.20 In many situations determining beneficial ownership is a straightforward matter. Cases in which the *client* is part of a complex structure will need to be looked at more closely. The diagrams below illustrate types of structures, including indirect ownership and aggregation, which should be taken into account when determining beneficial ownership.

EXAMPLE 1



The *client* is Company A Ltd, a private company. Unless persons F or G exercise the relevant control through other means (such as through 25% voting rights or other means of control) and based on a 25% ownership threshold, the beneficial owners are person D and person E.

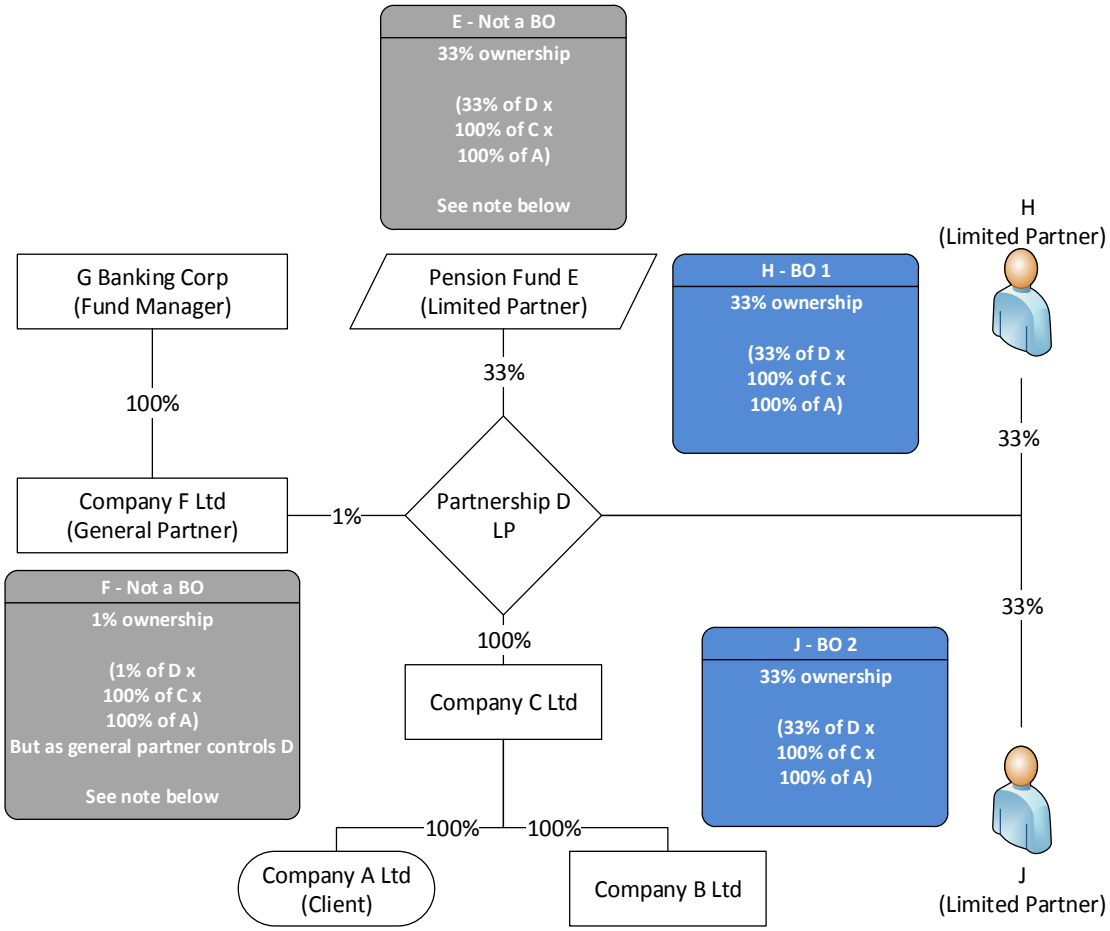
In determining the beneficial owner position, we would need to understand the ownership of Companies B & C (also private companies), but they themselves do not meet the definition of a BO as they are not natural persons.

Person D: is a beneficial owner due to their indirect shareholding of 30% via Company B.

Person E: is a beneficial owner due to their indirect shareholding of 30% via Company B and C.

Persons F & G are not beneficial owners as they only own 20% each via Company C.

EXAMPLE 2



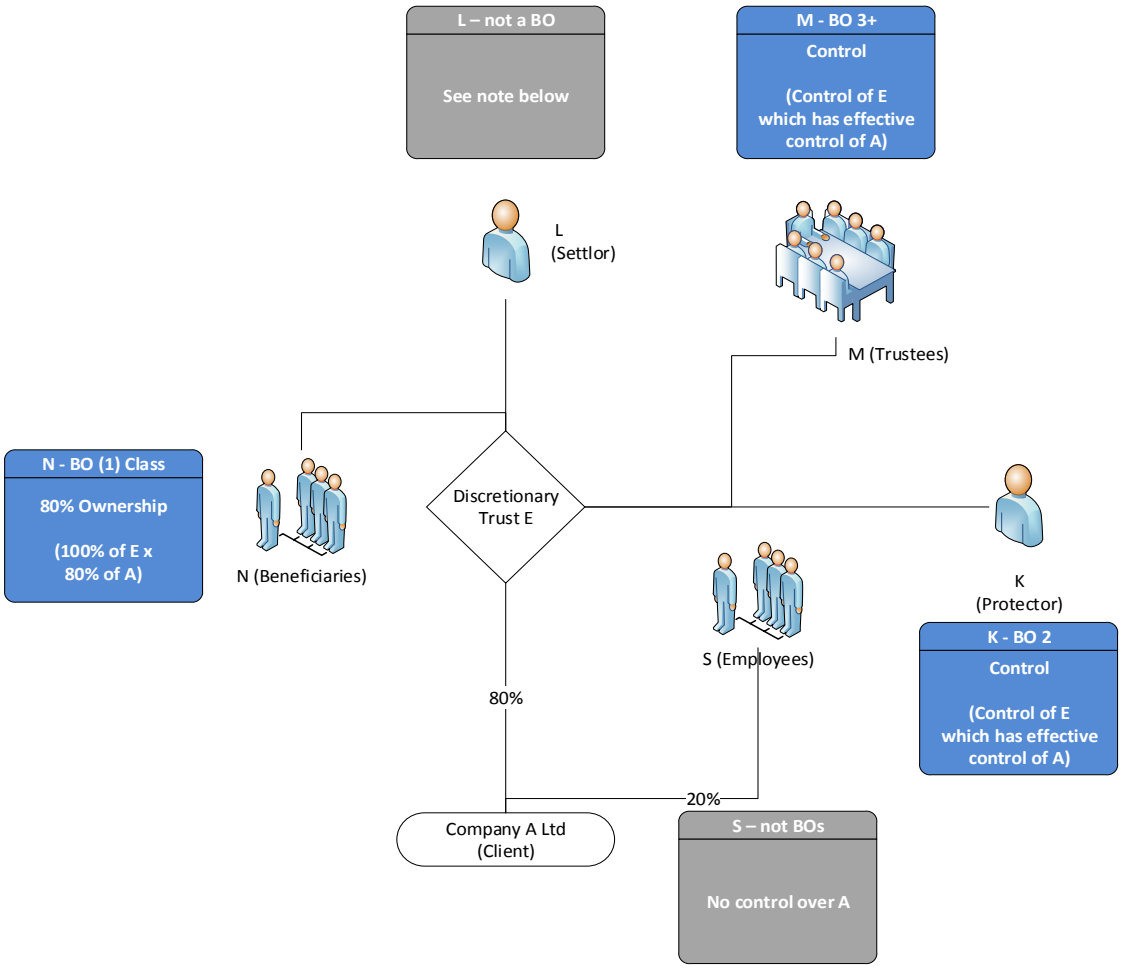
The *client* is Company A Ltd, a private company. Unless E or F control through other means (such as through 25% voting rights or other means of control) and based on a 25% threshold, the beneficial owners are person H and person J.

In determining the beneficial owner position, we would need to understand the structure of Company C, Partnership D, Pension Fund E, Company F and G Banking Corp but they themselves do not meet the definition of a beneficial owner as they are not natural persons.

Persons H & J: are beneficial owners based on a 25% threshold due to their indirect shareholding of 33% each via Partnership D.

Whilst not beneficial owners in their own right, Pension Fund E and Company F present avenues of ownership and control which should be considered further. Pension Fund E has a 33% ownership interest in Company A. Company F, as General Partner, controls the operations of Partnership D (which owns 100% of Company A). Company F is ultimately owned by G Banking Corp. In some situations, if risk is low, pension schemes and banks may qualify for Simplified Due Diligence (SDD), in which case consideration will stop at the point that we can confirm they are eligible for such treatment. Depending on the risk assessment we may need to further investigate the ownership and control structure to ensure there are no further beneficial owners.

EXAMPLE 3



The *client* (Company A Ltd) is a body corporate, therefore:

- Its beneficial owners are the natural persons who: (a) is entitled to a *vested interest* in possession, remainder or reversion, whether or not the interest is defeasible; (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; (c) any individual who has control over the trust; or (d) the settlor; (e) the trustee; (f) the protector.
- There is no need to use the beneficial owner rules related to other types of *client*, such as trusts.

In our case, all of the shares in Company A have equal voting rights. 80% of them are owned by Discretionary Trust E, which allows Discretionary trust E to control the activities of Company A. The remaining shares are owned by employees of Company A, none of whom have any connection to anyone else in the ownership and control structure.

Discretionary trust E is not a natural person, so it cannot be a beneficial owner.

The activities of Discretionary trust E are controlled by its trustees (M). Thus, each trustee is a beneficial owner of Company A.

In our case the trust's protector (K) acts as a check on the powers of the trustees and is also responsible for appointing new trustees. They are therefore regarded as having

significant influence and control over E. Protector K is a beneficial owner of Company A.

In our case the settlor (L) has no involvement following settlement of assets into the trust, nor do they exercise significant influence or control over the trustees or the protector. L has no other connection to A. L is not a beneficial owner of Company A, since they will not be exercising significant influence or control over E.

The employee-shareholders do not have enough votes, acting either individually or together, to control Company A, none of them is a beneficial owner of Company A.

Although the trustees and the protector must act in the interest of the beneficiaries, they (N) have no authority over the trustees or protector. Thus, the beneficiaries will not be beneficial owners of Company A, unless they exercise significant influence or control over E or A.

Notes:

- There may be situations where it is appropriate to know the identity of person L, for example to understand the source of Company A's capital. The *MLRO* should make the decision to seek such information as a risk-sensitive response to a particular set of circumstances.
- There may be situations where it is appropriate to identify the class of beneficiaries of trust E or even individuals receiving distributions from the trust, for example where distributions from Company A appear excessive it may be appropriate to establish that the beneficiary or beneficiaries require substantial funds. This may occur where a beneficiary is paying for a wedding or for large medical bills. The *MLRO* should make the decision to seek such information as a risk-sensitive response to a particular set of circumstances.
- If the trust E becomes a *client*, the settlor and the class of beneficiaries will need to be identified, in line with the rules for a discretionary trust.

5.2 When should *CDD* be carried out?

When establishing a business relationship

5.2.1 *CDD* should normally be completed before entering into a *business relationship* or undertaking an *occasional transaction*. For guidance on the situation when *CDD* cannot be performed before the commencement of a *business relationship*, see 5.4 of this guidance.

5.2.2 A *business relationship* is defined by Section 24 of the *2010 Act* as:

'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.'

Thus generic advice, provided with no expectation of any *client* follow-up or continuing relationship (such as generic reports provided free of charge or available for purchase by anyone), is unlikely to constitute a *business relationship*, although may potentially be an *occasional transaction*.

5.2.3 Under Section 24 of the *2010 Act*, for a *transaction* to be 'occasional' it must occur outside of a *business relationship* and have a value more than €10,000. Such a thing is not common in *accountancy services*, but should it occur then the *firm* must,

(a) understand why the *client* requires the service,

(b) consider any other parties involved, and

(c) establish whether or not there is any potential for *MLTF*. If the *client* returns for another *transaction* the *firm* should consider whether this establishes an ongoing relationship.

5.2.4 In addition, section 33A of the *2010 Act* provides for an *electronic money* derogation, provided certain criteria are met (including that the payment instrument concerned is not reloadable and has a maximum monthly payment *transaction* limit not exceeding €250).

5.2.5 *CDD* procedures must also be carried out at certain other times, such as when there is a suspicion of *MLTF*, or where there are doubts about the available identity information, perhaps following a change in ownership/control or through the participation of a *PEP* (see section 5.3.11 of this guidance).

Ongoing monitoring of the client relationship

5.2.6 Established *business relationships* should be subject to *CDD* procedures throughout their duration. This ongoing *monitoring* involves the scrutiny of *client* activities (including enquiries into sources of funds if necessary) to make sure they are consistent with the *firm's* knowledge and understanding of the *client* and its operations, and the associated risks.

Event-driven reviews

5.2.7 *Accountancy firms* need to make sure that documentation, data and information obtained for *CDD* purposes is kept up-to-date. Events prompting a *CDD* information update must include:

- a change in the *client's* identity
- a change in beneficial ownership of the *client*

- a change in the service provided to the *client*
- information that is inconsistent with the *firm's* knowledge of the *client*

An event driven review may also be triggered by:

- the start of a new engagement;
- planning for recurring engagements;
- a previously stalled engagement restarting;
- a significant change to key office holders;
- the participation of a *PEP* (see section 5.3.12 of this guidance)
- a significant change in the *client's* business activity (this would include new operations in new countries); and
- there is knowledge, suspicion or cause for concern (for example where you doubt the veracity of information provided). If a *STR* has been made, care must also be taken to avoid making any disclosures which could constitute *tipping off*.

Periodic reviews

5.2.8 *Accountancy firms* should use routine periodic reviews to update their *CDD*. The frequency of up-dating should be risk based, making use of the *firm's* risk assessment covered in Section 4 of this guidance, and reflecting the *firm's* knowledge of the *client* and any changes in its circumstances or the services it requires.

Ongoing procedures

5.2.9 The *CDD* procedures required for either event-driven or periodic reviews may not be the same as when first establishing a new *business relationship*. Given how much existing information could already be held, ongoing *CDD* may require the collection of less new information than was required at the very outset.

5.3 How should *CDD* be applied?

Applying CDD by taking a risk based approach

5.3.1 Sections 33 and 35 of the *2010 Act* require *customer due diligence* measures to be carried out on a risk-sensitive basis. This means that *accountancy firms* need to consider how their risk assessment and management procedures (see Section 4 of this guidance) flow through into their *client* acceptance and ID procedures, to give sufficient information and evidence, in the way most appropriate to the business concerned. In addition, there are certain circumstances where Sections 33 through 39 of the *2010 Act* lay down categories where simplified due diligence or *enhanced due diligence* is appropriate, according to national and international assessments of the risk of money laundering. A non-exhaustive list of risk factors can be found in APPENDIX D.

5.3.2 For information on client verification documents for the more frequently encountered entity types see APPENDIX B.

Simplified due diligence (SDD)

5.3.3 'Simplified due diligence', whilst not being explicitly referred to as such in the *2010 Act*, is covered in Sections 34 and 36 of the *2010 Act*. It is a phrase which means that an *accountancy firm* is not required to apply the *customer due diligence* measures laid out in Sections 33 (both in relation to a customer and to beneficial owners) and 35 of the *2010 Act*, where the accountancy firm has reasonable grounds for believing that *client* falls into the relevant categories.

5.3.4 *Accountancy firms* who may be permitted to apply the simplified due diligence exemptions but who perceive other than a low risk of money laundering in a specific case, should consider applying their standard or *enhanced due diligence* processes. In any case, where a *client* or potential *client* has been subject to simplified due diligence and a suspicion or money laundering or *terrorist financing* arises in relation to that *client*, the simplified due diligence provisions may no longer be applicable and the *customer due diligence* requirements of Sections 33 and 35 of the *2010 Act* may need to be applied, subject to any issues regarding the potential to prejudice an investigation through a prohibited disclosure under Section 49.

5.3.5 The *firm's* 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 risk factors in APPENDIX D (taken from Schedule 3 of the *2010 Act*) and relevant information made available by its *competent authority*. Where a firm applies CDD measures, 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 firm to detect unusual or suspicious *transactions*.

5.3.6 In any case, when a *client* or potential *client* has been subjected to SDD, and a suspicion of *MLTF* arises nonetheless, the SDD provisions must be set aside and the appropriate due diligence procedures applied instead (with due regard given to any risk of *tipping off*).

Enhanced due diligence (EDD)

5.3.7 A risk based approach to *CDD* will identify situations in which there is a higher risk of *MLTF*. Section 38A of the *2010 Act* specifies that 'enhanced' due diligence must be applied to manage and mitigate the risk of money laundering and *terrorist financing*....when dealing with a customer established or residing in a *high-risk third country*.

5.3.8 Examples of scenarios requiring the application of *enhanced due diligence* might include:

- where there is a high risk of *MLTF*;
- in any *occasional transaction* or *business relationship* with a person established in a *high-risk third country*;
- if a *firm* has determined that a *client* or potential *client* is a *PEP*, or *an immediate family member* or *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;
- in any other case which by its nature can present a higher risk of *MLTF.*

5.3.9 The *firm's* internal procedures should set out clearly what constitutes reasonable grounds for a *client* to qualify for EDD and must take into account at least the high risk factors in APPENDIX D (taken from Schedule 4 of the *2010 Act*).

5.3.10 EDD procedures must include:

- as far as reasonably possible, examining the background and purpose of the engagement; and
- Increasing the degree and nature of *monitoring* of the *business relationship* in which the *transaction* is made to determine whether that *transaction* or that relationship appear to be suspicious.

5.3.11 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 *firm*;
- taking additional measures to understand better the background, ownership and financial situation of the *client*, and other parties relevant to the engagement concerned;
- taking further steps to be satisfied that the *transaction* is consistent with the purpose and intended nature of the *business relationship*;
- Increasing the *monitoring* of the *business relationship*, including greater scrutiny of *transactions*.

Politically exposed person (PEP)

5.3.12 As set out above, section 37 of the *2010 Act* specifies that *PEPs* (as well as certain *immediate family members* and *close associates*) must undergo EDD. The nature, and extent of, such EDD measures will need to vary depending on the extent of any heightened *MLTF* risk associated with individual *PEPs* (including domestics *PEPs*). *Accountancy firms* must treat *PEPs* on a case-by-case basis, and apply EDD on the basis of their assessment of the *MLTF* risk associated with any individual *PEPs*.

5.3.13 Section 37 defines a *PEP* as an individual '…who is or has, at any time in the preceding 12 months, been entrusted with a prominent public function', including either a "specified official" or a member of the administrative, management or supervisory body of a state-owned enterprise or an *immediate family member* or *close associate* of such a person. Specified official is defined as any of the following officials (including any such officials in an institution of the European Communities or an international body):

- a head of state, head of government, government minister or deputy or assistant government minister;
- a member of parliament or of a similar legislative body;
- 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;

- a member of a court of auditors or of the board of a central bank;
- an ambassador, charge d'affairs or high ranking officer in the armed forces; or
- a director, deputy director or member of the board of, or person performing the equivalent function in relation to, an international organisation.

For risk management and reputational risk reasons, *accountancy firms* may wish to treat as *PEPs* persons who held such positions more than a year ago.

'*Immediate family member*' of a *PEP* includes: parents, spouses and equivalent, children, spouses of children and equivalent, and any other family member of a class prescribed by the Minister (none at the time of publication). '*Close associate*' includes any person who

(i) has joint beneficial ownership of a legal entity or arrangement, or any other close business relations with a *PEP* or

(ii) has sole beneficial ownership of a legal entity or arrangement set up for the actual benefit of a *PEP*.

5.3.14 An individual identified as a *PEP* solely because of their public function must still be treated as a *PEP*. However if the *firm* 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*. The risk factors guidance produced by the European Supervisory Authorities set out factors that might point to potential higher risk. Such factors might also include, for example:

- known involvement in publicised scandals e.g., regarding expenses;
- undeclared business interests;
- previous prosecution for criminal offences;
- the acceptance of inducements to influence policy.

5.3.15 In lower-risk situations a *firm* should apply less onerous EDD requirements (such as, for example, making fewer enquiries of a *PEP's immediate family members* or *close associates;* and taking less intrusive and less exhaustive steps to establish the sources of wealth/funds of *PEPs*). Conversely, and in higher-risk situations, *firms* should apply more stringent EDD measures. This represents part of the risk based approach that *firm's* should take to *MLTF* compliance, as described more fully elsewhere in this section.

5.3.16 *Accountancy firms* must treat individuals as *PEPs* for at least 12 months after they cease to hold a prominent public function. This requirement does not apply to *immediate family members* or *close associates. Immediate family members* and *close associates* of *PEPs* should be treated as ordinary *clients* (and subject only to *CDD* obligations) from the point that the *PEP* ceases to discharge a prominent public function. *Firms* need only apply EDD measures to *PEPs* for more than 12 months after they have ceased to hold a prominent public function when the *firm* has determined that they present a higher risk of *MLTF*.

5.3.17 An *accountancy firm* is deemed to know or have reasonable grounds to know that a person is a *PEP*, an immediate *family member* of a *PEP* or a *close associate* of a *PEP* on the basis of information in the possession of the *accountancy firm* or in the public domain. The *2010 Act* provides that the definition of immediate *family member* must include the spouses/civil partners of *PEPs*, the children of *PEPs* (and their spouse or

civil partner) and the parents of *PEPs*. This is not an exhaustive list – in determining whether other immediate *family members* should be subject to EDD, *accountancy firms* should consider the levels of *MLTF* risk associated with the relevant *PEP*. In lower-risk situations, a *firm* should not apply EDD to additional immediate *family members* other than those contained within the definition set out in the *2010 Act*.

5.3.18 As regards international organisations, the *2010 Act* states that only directors, deputy directors and board members (or equivalent) should be treated as *PEPs*. Middle-ranking and junior officials do not fall within the definition of a *PEP*.

5.3.19 'International organisation' is not defined, and due consideration should be given to the type, reputation and constitution of the body before excluding it or its representatives from *enhanced due diligence*. However, bodies such as the United Nations, NATO and *FATF* may reasonably be included within the definition of an international body for this purpose. The context of the *engagement* and role of the *PEP* in respect of it should also be considered.

5.3.20 *Accountancy firms* are required to have risk sensitive measures in place to recognise *PEPs* (Sections 37(1) to 37(3)). This can be a simple check conducted by enquiring of the *client* and perhaps using an internet search engine. *Accountancy firms* that are likely to regularly undertake services for *PEPs* may need to subscribe to a specialist database. *Firms* that use such databases must understand how they are populated and will need to ensure that those flagged by the database fall within the definition of a *PEP*, *immediate family member* or *close associate* as set out in Section 37 of the *2010 Act*. During the life of a relationship, and to the extent that it is practical, attempts should be made to keep abreast of developments that could transform an existing *client* into a *PEP*.

5.3.21 *Firms* wanting to enter into, or continue, a *business relationship* with a *PEP* must carry out EDD, which includes:

- *senior management* approval for the relationship;
- adequate measures to establish sources of wealth and funds; and
- enhanced *monitoring* of the ongoing relationship.

As set out above, the nature and extent of EDD measures must vary depending on the levels of *MLTF* risk associated with individual *PEPs*.

5.3.22 The Anti Money Laundering Compliance Unit (AMLCU) of the Department of Justice has published guidance on how businesses that it supervises for MLTF purposes should identify and treat *PEPs*. *Accountancy firms* may find this guidance useful in determining the approach that they should take to identifying and applying EDD to *PEPs*.

5.3.23 The preamble to the *EU Directive* (which the *2018 Act* brought into Irish law makes it clear that refusing a *business relationship* with a person solely on the basis that they are a *PEP* is contrary to the spirit and letter of the *EU Directive*, and of the *FATF* standards. *Firms* should instead mitigate and manage any identified *MLTF* risks, and should refuse *business relationships* only when such risk assessments indicate that they cannot effectively mitigate and manage these risks.

Financial sanctions and other prohibited relationships

5.3.24 The *2010 Act* sets out circumstances which constitute prohibited relationships. In Section 59, correspondent banking relationships with *shell banks*, or a bank known to

permit use of its accounts by a *shell bank* are prohibited. In addition, Section 58 prohibits the setting up of anonymous accounts, and *customer due diligence* must be applied to any existing accounts continuing in existence after commencement of the *2010 Act* before such an account is used. In addition, *accountancy firms* must comply with any prohibition issued by the Department of Finance in respect of any person, or State to which financial sanctions apply. These are published regularly in Iris Oifiguil.

5.3.25 Financial sanctions can be a complex and changeable area. Detailed discussion of it is beyond the scope of this guidance. *Accountancy firms* should refer to the Department of Finance. *Firms* unsure of their legal obligations should seek legal advice.

Reliance on other parties

5.3.26 Section 40 of the *2010 Act* provides that *accountancy firms* may rely on certain third parties, referred to as 'relevant third parties', to complete all or part of *customer due diligence*, subject to there being an arrangement between the *firm* and the relevant third party. The *firm* proposing to rely on a relevant third party must satisfy themselves that, on the basis of the arrangement in place, the relevant third party will forward any documents or information relating to the *client* in question that has been obtained by the relevant third party in identifying that *client*, as soon as practicable after the *firm* makes the request. *Accountancy firms* should, however, be cautious in relying on third parties as the firm will remain liable for any failure to comply with *customer due diligence* measures notwithstanding their reliance on a third party (Section 40(5)). *Accountancy firms* should consider requiring copies of relevant information and documentation from the third parties, in order that they may satisfy themselves the information is sufficient. 'Relevant third parties' on whom reliance may be placed are:

- *credit* or *financial institutions* (excluding undertakings solely providing foreign exchange or money services)
  - in Ireland; or
  - authorised to operate under the laws of another Member State or of a designated place (under Section 31)
- *external accountants*, auditors, *tax advisers* and *relevant independent legal professionals*
  - who are members of a Designated Accountancy Body, the Irish Taxation Institute or the Law Society of Ireland respectively; or
  - who are subject to mandatory professional registration or mandatory professional supervision under the laws of another Member State or in a designated place (under Section 31);
- *trust or company service providers*
  - who are members of a Designated Accountancy Body, or the Law Society of Ireland, or are authorised to carry on business by the Central Bank of Ireland; or
  - who are subject to mandatory professional registration or mandatory professional supervision under the laws of another Member State or in a designated place (under Section 31);

The relevant third parties in the abovementioned 'designated place' under Section 31 must be supervised or monitored in the place for compliance with requirements equivalent to those specified in the Fourth Money Laundering Directive. *Accountancy firms* may outsource their *customer due diligence* measures but remain liable for any failure in the *customer due diligence*.

5.3.27 Outsourcing is permitted only if the other party is required to apply the requirements of the Directive (eg a *designated person* in Ireland) or subject, in an *EEA* or non-*EEA* state, to an equivalent regulatory regime which includes compliance supervision requirements equivalent to the *EU Directive.*

5.3.28 *Firms* should note that where one party places reliance on another they should enter into an agreement (that should be in writing) to ensure that the other party will provide the *CDD* documentation as soon as practicable after a request. An arrangement of this kind can be useful and efficient when the two parties are able to build a relationship of trust, but it should not be entered into lightly. Liability for inadequate *CDD* remains with the relying party. *Firms* placing reliance on another should satisfy themselves with the level of *CDD* being undertaken.

Parties seeking reliance

5.3.29 A *firm* relying on a third party in this way is not required to apply standard *CDD*, but it must still carry out a risk assessment and perform ongoing *monitoring*. That means it should still obtain a sufficient quantity and quality of *CDD* information to enable it to meet its *monitoring* obligations.

5.3.30 If relying on a third party, *firms* should obtain from that party copies of all relevant information to satisfy *CDD* requirements. They should also enter into a written arrangement that confirms that the party being relied on will provide copies of identification and verification documentation as soon as practicable after a request.

Parties granting reliance

5.3.31 An *accountancy firm* is not obliged to act as a relevant third party for another *designated person*. *Accountancy firms* agreeing an arrangement to act as a relevant third party in relation to the *customer due diligence* obligations of another *designated person* should take great care to ensure they have adequate systems in place to keep proper records and to respond to any request for these. Where an *accountancy firm* agrees to be part of an arrangement whereby another *designated person* relies on him in meeting their obligations under the *2010 Act* with regard to *customer due diligence* must, if requested, make available to the person relying as soon as is reasonably practicable:

- any information obtained about the *client* (and any beneficial owner) when applying *customer due diligence* measures; and/or;
- copies of any identification and verification data and other documents on the identity of the *client* (and any beneficial owner) obtained when applying *customer due diligence* measures.

Other *designated persons* who rely on an *accountancy firm* to carry out *customer due diligence* measures, as part of an arrangement between both parties, remain ultimately responsible under the *2010 Act* for any failure to apply the measures

Subcontracting

5.3.32 Where a relevant *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.

5.3.33 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. In this situation, A may wish to take into account information provided by B and the relationship it has with C when determining what *CDD* is required under its risk based approach. It should be noted that the same considerations are relevant in networked arrangements, where work is referred between member firms.

Evidence gathering

5.3.34 The purpose of verification of identity is to confirm and prove the information collected in so far as it relates to the identity of the *client*. Recourse to documents from independent sources is important. The amount of reliance that can be placed upon, and thus the strength of, particular forms of evidence varies. The following are illustrative of a different of strength of various forms of documentary evidence starting with the highest:

- documents issued by a government department or agency or a Court (including documents filed at the Companies Registration Office or overseas equivalent);
- documents issued by other public-sector bodies or local authorities;
- documents issued by *designated persons* regulated by the Central Bank of Ireland or overseas equivalent;
- documents issued by *relevant professional advisers* and *relevant independent legal professionals* regulated for anti-money laundering purposes by the Designated Accountancy Bodies or the Law Society of Ireland and overseas equivalents;
- documents issued by other bodies.

In the case of *clients* who are persons, documents from highly rated sources that contain photo identification as well as written details are a particularly strong source of verification of identity. Consideration should also be given to conducting a general internet search of the company and the directors and beneficial owners.

5.3.35 In higher risk cases *firms* must consider whether they need to take extra steps to increase the depth of their *CDD* knowledge. These might include more extensive internet and media searches covering the *client*, key counterparties, the business sectors and countries and requests for additional identity evidence. Subscription databases can be a quick way to access this kind of public domain information, and they will often reveal links to known associates (companies and individuals) as well.

5.3.36 *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.

5.3.37 It is important that verification procedures are undertaken on a risk-sensitive basis.

Refer to APPENDIX B for a non-exhaustive list of documents that can be used for verification purposes.

Validation of documents

Certification of documents by a third party

5.3.38 *Accountancy firms* may consider it appropriate, in the case of documents originating from or provided by a third party, to request certification as to their accuracy. In such cases, *firms* are advised to have regard to the standing of the person certifying and may wish to consider specifying from whom certification may be accepted. For instance, *firms* may decide to accept those documents certified by a person in the permitted categories for reliance (Section 40) which are broadly a *credit* or *financial institution* authorised by the Central Bank of Ireland, a professionally qualified auditor, *external accountant*, insolvency practitioner or *tax adviser*, or *relevant independent legal professional*, or their equivalent in other Member States or other designated places under Section 31, which have equivalent law and provided in all cases that the person is subject to supervision as to his compliance with those requirements.

Annotation of sources of validation

5.3.39 This should be used when the document is as good as an original but is not the original itself. This particularly applies to printouts from the Internet, such as downloads from the Companies Registration Office, regulator, stock exchange or government websites, or similar trustworthy business information sources. Each document so obtained should bear written evidence showing who printed it, when, from where and should be signed by the relevant person. Where necessary and taking a risk based approach, such documents (whether downloaded or otherwise) should be validated with an authoritative source such as a government agency.

Use of electronic data

5.3.40 There are now a number of subscription services that give access to databases of information on identity. Many of these services can be accessed on-line and are often used by *accountancy firms* to replace or supplement paper verification checks. This means *firms* may use on-line verification as a substitute for paper verification checks for *clients* considered normal risk, supplemented by additional paper verification checks for higher risk *clients*, or vice versa.

5.3.41 Before using electronic databases, however, *firms* should question whether the information supplied is sufficiently reliable, comprehensive and accurate. Consider the following points:

- **Does the system draw on multiple sources?** A single source (e.g., the Electoral Register) is usually not sufficient. A system which uses negative and positive data sources is generally more robust than one that does not.
- **Are the sources checked and reviewed regularly?** Systems that do not regularly update their data regularly are generally prone to more inaccuracies than those that do.
- **Are there control mechanisms to ensure data quality and reliability?** Systems should have built-in data integrity checks which, ideally, are sufficiently transparent to prove their effectiveness.
- **Is the information accessible?** Systems need to allow a *firm* either to download and store the results of searches in appropriate electronic form, or

to print off a hardcopy record containing all necessary details as to name of provider, source, date etc.

- **Does the system provide adequate evidence that the *client* is who they claim to be?** Consideration should be given as to whether the evidence provided by the system has been obtained from an official source, e.g., certificate of incorporation from the official company registry.

5.4 What happens if *CDD* cannot be performed?

When delays occur

5.4.1 In forming new *business relationships*, there are some cases where delay **may** be acceptable, such as in urgent insolvency appointments, and urgent appointments that involve ascertaining the legal position of a *client* or defending the *client* in legal proceedings.

5.4.2 In such cases, *accountancy firms* should still gather enough information to allow them to at least form a basic assessment of the identity of the *client* and money laundering risk and to complete other acceptance formalities such as considering the potential for conflicts of interest.

5.4.3 In other cases, where the majority of information required has been collected before entering a *business relationship*, short time extensions to complete collection of remaining information may be acceptable, provided this is caused only by administrative or logistical issues, and not by any reluctance of the *client* to provide the information and is necessary not to interrupt the normal course of business. Such extensions should be exceptional, rather than the norm. It is recommended that such extensions of time are considered and agreed by a member of *senior management* or the *MLRO*, where appointed in accordance with the *firm's* procedures, to ensure the reasons for the extension are valid and do not give rise to concern over the risk category of the *client* or the potential for money laundering suspicion.

5.4.4 Provided that *CDD* is completed as soon as practicable, verification procedures may be completed during the establishment of a *business relationship* if it is necessary not to interrupt the normal course of business and there is little risk of *MLTF*. In some situations it may be necessary to carry out *CDD* while commencing work because it is urgent. Such situations could include:

- some insolvency appointments;
- appointments that involve ascertaining the *client's* legal position or defending them in legal proceedings;
- response to an urgent cyber incident; or
- when it is critically important to preserve or extract data or other assets without delay.

5.4.5 If evidence is delayed (rather than refused), *accountancy firms* should consider;

- the credibility of the *client's* explanation;
- the length of delay;
- whether the delay is in itself reasonable grounds for suspicion of a *money laundering* offence requiring a report to *FIU Ireland* and the Revenue

Commissioners and/or a factor indicating against acceptance of the *client* and engagement; and

- documenting the reasons for delay and steps taken.

5.4.6 No client engagement (including transfers of *client* money or assets) should be completed until *CDD* has been completed in accordance with the *firm's* own procedures.

Cessation of work and suspicious transactions reporting

5.4.7 If a prospective *client* refuses to provide evidence of identity or other information properly requested as part of *customer due diligence*, the *business relationship* should be discontinued and/or the *transaction*/series of linked *transactions* amounting to in excess of €10,000 sought by the *client* must not be provided, for so long as the failure continues (but see paragraphs 5.4.10 to 5.4.12 below regarding particular circumstances affecting insolvency cases). Consideration must be given as to whether a report needs to be made to *FIU Ireland* and the Revenue Commissioners, in accordance with Section 42(4).

5.4.8 Where the appointment is of either a lawyer or *relevant professional advisor* in the course of ascertaining the legal position for the *client*, or performing the task of defending or representing the *client* in or concerning legal proceedings (including advice on instigating or avoiding proceedings) the requirement to cease acting and consider reporting to the FIU Ireland and the Revenue Commissioners does not apply although *customer due diligence* information will still need to be collected within the time constraints in Sections 33 and 35 of the *2010 Act*. *Accountancy firms* are advised to consider the position very carefully before applying this exception to ensure that the type of work and their professional status fall within the definition of *relevant professional adviser* set out in Section 24 of the *2010 Act*.

Insolvency cases

5.4.9 An insolvency practitioner should obtain verification of the identity of the person or entity over which he is appointed. Acceptable evidence of verification may include a court order, a court endorsed appointment, or an appointment made by a debenture holder or creditors meeting supported by a company search or similar. It is not always possible or necessary to obtain identification evidence direct from persons or individual shareholders or directors in an appointment in respect of a company as their co-operation may not be forthcoming.

5.4.10 It is important for an officeholder to be sure about the identity of the person or entity over which he is taking appointment given the urgency of the situation and the necessity not to delay when this might risk dissipation of assets and erosion of value. Initial contact with the company would include, for example accepting instructions from directors to take steps to place a company into liquidation or to accept appointment as independent expert under section 504 of the Companies Act 2014. . However, completion of other elements of customer due diligence may not be possible prior to appointment and should be completed as soon as practicable after appointment (if possible, usually within 5 working days).

5.4.11 Insolvency practitioners post appointment have a very different relationship with the insolvent client than that with an audit or advisory client and have access to a very

wide range of information which alters the need for traditional pre-appointment CDD. However, particular focus is needed before, and immediately after, appointment on considering the way the business has been operated and assessing the risk of assets being tainted by crime. In such cases it may well be necessary, but not as a matter of routine in every case, to make an external report prior to performing the normal range of duties of collection, realisation and distribution of assets.

5.4.12 Where the insolvency practitioner is appointed by Court order without any prior involvement with the insolvent company, reliance on the order of appointment or winding-up order is considered to be sufficient evidence of identity. This would apply in the following cases:

• Appointment as provisional liquidator by order of the Court;

• Appointment as liquidator in a winding up by the Court (including by order following an examination); or

• Appointment as examiner by order of the Court.

An insolvency practitioner appointed to a company which is itself a *designated person* under the *2010 Act*, and becoming responsible for the company's operation, will need to be satisfied that the company has appropriate procedures in place to ensure its compliance with the requirements of the *2010 Act* and that the procedures continue to function during the term of the his appointment.

6 SUSPICIOUS TRANSACTION REPORTING (*STR*)

- What must be reported?
- Offences
- When and how should a report be made?
- Reporting and the privileged circumstances exception?
- Determining whether to proceed with or withdraw from a *transaction* or service
- Requests for further information
- What should happen after an external *STR* has been made?

6.1 What must be reported?

The reporting regime

6.1.1 The obligation to make a Suspicious Transaction Report (*STR*) is set out in section 42 of the *2010 Act* and arises when:

- an *accountancy firm* or an *individual* connected with the firm knows or suspects, or has reasonable grounds to suspect, that another person has been, or is, engaged in money laundering or *terrorist financing (*see below*);*
- the information on which the above is based came to the *firm* or the *individual* in the course of carrying on the business of an *accountancy firm* or accountant;
- the *firm* or *individual* has scrutinised the information in the course of reasonable business practice.

Money laundering

6.1.2 Section 2 of the guidance defines the *money laundering offences* (see paragraph 2.2.1). A person commits a *money laundering offence* if he, knowing or believing that property is or 'probably comprises' the *proceeds of criminal conduct* or being reckless as to whether the property is or 'probably comprises' such proceeds, engages in any of the following acts in relation to the property:

- concealing or disguising the true nature, source, location, disposition, movement or ownership or the property, or any rights relating to the property;
- converting, transferring, handling, acquiring, possessing or using the property;
- removing the property from, or bringing the property into, the State.

6.1.3 Money laundering can be carried out in respect of the proceeds of both conduct that is an offence in Ireland and, in certain circumstances, conduct occurring elsewhere. These circumstances are set out in section 8 of the *2010 Act* and include actions by an Irish citizen in another jurisdiction or that take place on an Irish ship or an aircraft registered in Ireland.

6.1.4 For a matter to be money laundering, there must not only be *criminal conduct*, but also *proceeds of criminal conduct*.

Terrorist financing

6.1.5 '*Terrorist financing'* means an offence under Section 13 of the Criminal Justice (Terrorist Offences) Act 2005 and involves the provision, collection or receipt of funds with the intent or knowledge they will be used to carry out an act of terrorism or any act intended to cause death or serious injury.

6.1.6 The offence is committed by any person, in or outside the State, who directly or indirectly, unlawfully and wilfully, provides, collects or receives funds intending that they will be used or knowing that they will be used to carry out an act of terrorism. Terrorism is taken to be the use or threat of action designed to influence government, or to intimidate any section of the public, or to advance a political, religious or ideological cause where the action would involve violence, threats to health and safety, damage to property or disruption of electronic systems.

6.1.7 **Materiality or 'de minimis' exceptions do not exist in relation to either *money laundering* or *terrorist financing* offences**

6.1.8 In relation to reporting obligations, references to *accountancy firms* are to be read as including references to a director or other officer, employee or (in the case of a partnership) principal of the *accountancy firm*. Section 41 also captures agents of the *accountancy firm* or other persons 'engaged under a contract for services' within the definition of *designated persons* for the purposes of the reporting obligation.

6.1.9 Disclosure is ordinarily made internally to the *MLRO* or other nominated person in accordance with procedures established by the *accountancy firm* in accordance with s54(3)(g) or, if appropriate in the circumstances, may be made directly to *FIU Ireland* and the Revenue Commissioners.

6.1.10 The procedures implemented by the *accountancy firm* should also provide a mechanism to ensure that the *STR* to *FIU Ireland* and Revenue Commissioners is made where there is knowledge, suspicion or reasonable grounds to suspect money laundering or *terrorist financing* as a consequence of the *internal report*.

6.1.11 The key elements required for a *STR* (knowledge, suspicion, crime, proceeds) are set out below.

Knowledge and Suspicion

6.1.12 An *accountancy firm* or *individual* is required to make an *STR* where that *firm* or *individual* has knowledge, suspicion or reasonable grounds for suspicion of money laundering or *terrorist financing* arising from the *firm's/individual's* normal course of business.

6.1.13 Having knowledge means actually knowing that something is the case. There is very little guidance on what constitutes 'suspicion' so the concept remains subjective. Some pointers can be found in case law, where the following observations have been made. Suspicion is:

- a state of mind more definite than speculation but falling short of evidence-based knowledge;
- a positive feeling of actual apprehension or mistrust;
- an opinion, based on indicative but not conclusive evidence.

Suspicion is not

- a mere idle wondering;

- a vague feeling of unease.

6.1.14 An *STR* must be made where there is knowledge or suspicion of money laundering *terrorist financing*, but there is no requirement to make speculative *STRs*. If, for example, a suspicion is formed that someone has failed to declare all of their income for the last tax year, to assume that they had done the same thing in previous years would be speculation in the absence of specific supporting information. Similarly, the purchase of a brand new Ferrari by a *client's* financial controller is not, in itself, a suspicious *transaction*. However, inconsistencies in accounts for which the financial controller is responsible could raise speculation to the level of suspicion.

6.1.15 An *STR* is also required when there are 'reasonable grounds' to suspect money laundering or *terrorist financing (*section *42(3) of the 2010 Act)*. While suspicion is, by its nature, subjective, the term "reasonable grounds to suspect" is an objective test i.e., the standard of behaviour expected of a reasonable person in the same position. Claims of ignorance or naivety are no defence.

6.1.16 'Reasonable grounds' should not be confused with the existence of higher than normal risk factors which may affect certain sectors or classes of persons. For example, cash-based businesses or complex overseas trust and company structures may be capable of being used to launder money, but this capability of itself is not considered to constitute ''reasonable grounds'.

6.1.17 Existence of higher than normal risk factors require increased attention to gathering and evaluation of *CDD* information, and heightened awareness of the risk of money laundering in performing professional work, but do not of themselves require a report of suspicion to be made. For 'reasonable grounds' to come into existence, there needs to be sufficient information to advance beyond speculation that it is merely possible someone is laundering money, or a higher than normal incidence of some types of crime in particular sectors.

6.1.18 It is important for *individuals* to make enquiries that would reasonably be expected of someone with their qualifications, experience and expertise, and such enquiries fall within the normal scope of the engagement or *business relationship*. In other words, they should exercise a healthy level of professional scepticism and judgement and, if unsure about what to do, consult their *MLRO* or other nominated officer (or similar) in accordance with the *firm's* own procedures. If in doubt, it is advisable to err on the side of caution and report to the *MLRO*.

6.1.19 The information or knowledge that gave rise to the suspicions must have come to the *individual* in the course of business a as *designated person* (section 42 of the *2010 Act*). .

Crime and proceeds

6.1.20 *Criminal conduct* is behaviour which constitutes an offence in Ireland or, in certain circumstances, occurring elsewhere (see Section 2 above). *Criminal conduct* is defined under Section 6 in terms of the commission of "an offence". This definition captures not only criminal offences, but all other offences which result in proceeds. As such, *criminal conduct* is defined very broadly. It goes beyond the common understanding of money laundering, being the conversion and concealment of funds derived from illegal activity, to incorporate the mere possession, acquisition or use of the illicit proceeds. Any offence, therefore, whether indictable or otherwise, which results in proceeds, represents a *money laundering offence* and falls to be reported under the legislation.

6.1.21 Since Irish law defines *money laundering offences* so widely, any *criminal conduct* which has resulted in any form of *proceeds of criminal conduct* will also constitute *money laundering*. It is not expected that *individuals* will become expert in the very wide range of underlying or predicate criminal offences which lead to *money laundering* but they will be expected to recognise those that fall within the professional competence of their role and should use professional scepticism, judgement and independence as appropriate to identify offences.

6.1.22 The *2010 Act*'s definition of *money laundering offences* (section 2 of the Act) requires that an offender must know or suspect, or be reckless as to whether or not, that property is the *proceeds of criminal conduct*. An innocent error or mistake would not normally give rise to criminal proceeds (unless a strict liability offence).

6.1.23 If an *accountancy firm* or *individual* knows or believes that a *client* is acting in error, the *individual* may approach the *client* and explain the situation and legal risks to him. However, once the criminality of the conduct is explained to the *client*, that *client* must bring the conduct (including past conduct) promptly within the law to avoid a *money laundering offence* being committed. Where there is uncertainty about the legal issues, outside the competence of the *accountancy firm, clients* should be referred to an appropriate specialist or professional legal adviser.

6.1.24 As noted above, the reporting obligations arise where offences are committed which give rise to proceeds. These *predicate offences* may be under any legislation – for example, including inducements offered in contravention of the Criminal Justice (Corruption Offences) Act 2018. *Accountancy firms* are most likely to encounter possible offences under the Companies Acts, the Criminal Justice (Theft and Fraud Offences) Act 2001 and tax legislation. However, they should be aware that if they receive information during the normal course of their work which gives rise to knowledge, suspicion or reasonable grounds for suspicion that an offence has been, or is being, committed under other legislation, they have a reporting obligation in such circumstances (except where the *professional privilege reporting exemption* applies – see section 6.4 below). *CCAB-I* / professional guidance has been issued dealing with indictable offences under the Companies Acts which are reportable to the Office of the Director of Corporate Enforcement, and reporting of theft and fraud offences, which at date of issue are as follows:

- Technical Release 04/2015 – Companies Act 2014 A *statutory auditor's* duty to report to the Director of Corporate Enforcement;
- Technical Release 03/2016 – Companies Act 2014 Reporting Company Law Offences: Information for *Statutory Auditors*;
- *CCAB-I* memo – Section 59 Criminal Justice (Theft and Fraud Offences) Act 2001;
- Information Sheet 01/2013 – Criminal Justice Act 2011, Reporting implications for Members in Practice and in Business.

6.1.25 In most cases of suspicious *transactions* the reporter will have a particular type of *criminal conduct* in mind, but this is not always the case. Some *transactions* or activities so lack a commercial rationale or business purpose that they give rise to a general suspicion of *MLTF*. As noted in paragraph 6.1.21, Irish law defines money laundering widely: *individuals* are not required to become experts in the wide range of criminal offences that lead to money laundering, but they are expected to recognise any that fall within the scope of their work. Exercise professional scepticism and judgement at all times.

Proceeds

6.1.26 *Proceeds of criminal conduct* means any property that is derived from or obtained through *criminal conduct*, directly or indirectly, in whole or in part. Criminal proceeds can take many forms. Cost savings (as a result of tax evasion or ignoring legal requirements) and other less obvious benefits can be proceeds of crime. Where criminal property is used to acquire more assets, these too become criminal property. It is important to note that there is no question of a de minimis value.

6.1.27 If someone knowingly engages in criminal activity with no benefit, then they may have committed some offence other than money laundering (it will often be fraud) and there is no obligation to make an *STR*. However, the duty to report under other legislation (including company law and the Criminal Justice (Theft and Fraud Offences) Act 2001) should be assessed and where appropriate a report made as required by that legislation.

6.1.28 Examples of unlawful behaviour which may be observed, and may well result in advice to a *client* to correct an issue, but which are not reportable as *money laundering offences* are given below:

- offences where no proceeds or benefit results, such as the late filing of company accounts. However, *accountancy firms* and *individuals* should be alert to the possibility that persistent failure to file accounts could represent part of a larger offence with proceeds, such as fraudulent trading or credit fraud involving the concealment of a poor financial position.
- misstatements in tax returns, for whatever cause, but which are corrected before the date when the tax becomes due.
- attempted frauds where the attempt has failed and so no benefit has accrued (although this may still be reportable under other legislation.

A checklist for the *STR* reporting process can be found in APPENDIX C.

Examples of reportable matters

Example 1 – Overpaid invoices	
Some customers of your *client* have overpaid their invoices. The *client* retains overpayments and credits them to the profit and loss account.	
Report	If you: • know or suspect that the *client* intends to dishonestly retain the overpayments. Reasons for such a belief may include: ○ The *client* omits overpayments from statements of account. ○ The *client* credits the profit and loss account without making any attempt to contact the overpaying party.

Example 1 – Overpaid invoices	
Do not report	If you: • believe that the *client* has no dishonest intent to permanently deprive the overpaying party. Reasons for such a belief may include: ○ Systems operated by the *client* to notify the customer of overpayments. ○ Evidence that requested repayments are processed promptly. ○ Evidence that the *client* has attempted to contact the overpaying party. ○ The *client* has sought and is following legal advice in respect of the overpayments.

Example 2 – Illegal dividends	
Your *client* has paid a dividend based on draft accounts. Subsequent adjustments reduce distributable reserves to the extent that the dividend is now illegal.	
Report	If there is suspicion of fraud.
Do not report	If there is no such suspicion. The payment of an illegal dividend is not a criminal offence under the Companies Act.

Example 3 – Invoices lacking commercial rationale	
Your *client* plans to expand its operations into a new country of operation. They have engaged a consultancy firm to oversee the implementation although it is not clear what the firm's role is. Payments made to the consultancy firm are large in comparison to the services provided and some of the expenses claimed are for significant sums to meet government officials' expenses. The country is one where corruption and facilitation payments are known to be widespread. You ask the Finance Director about the matter and he thought that such payments were acceptable in the country in question.	
Report	If you suspect that bribes have been paid.
Do not report	If you do not suspect illegal payments.
Money laundering offences include, in certain circumstances, conduct occurring overseas which would constitute an offence if it had occurred in Ireland.	

Example 4 – Concerted price rises
Your *client's* overseas subsidiary is one of three key suppliers of goods to a particular market in Europe. The subsidiary has recently significantly increased its prices and margins and its principal competitors have done the same. There has been press speculation that the suppliers acted in concert, but publicly they have cited increased costs of production as driving the increase. Whilst this explains part of the reason for the increase, it is not the only reason

because of the increase in margins. On reviewing the accounting records, you see significant payments for consultancy services and seek an explanation. Apparently, they relate to an assessment of the impact of the price increase on the market as well as some compensation for any losses the competitors suffered on their business outside of Europe. Some of the increased profits have flowed back to the Irish parent company. There is not a criminal cartel offence under local law but there is under Irish law.	
Report	If you suspect a price fixing cartel.
Do not report	If you do not suspect criminal activity.

6.2 Offences relating to reporting

Failure to disclose

6.2.1 Persons involved in the conduct of the designated activity e.g. employees of an accountancy firm ("relevant employees") should make sure that any information in their possession which is part of the required disclosure is passed to the MLRO as soon as practicably possible.

6.2.2 Where, as a result of an *internal report*, or otherwise, the MLRO obtains knowledge or forms a suspicion of *MLTF*, they must as soon as practicable make an external *STR* to *FIU Ireland* and the Revenue Commissioners. The *MLRO* may commit an offence if they fail to do so.

Defences and exemptions

6.2.3 There are defences to the offence of failing to report as follows:

- the *professional privilege reporting exemption* (see section 6.4 below) applies; or
- the *relevant employee* did not actually know or suspect *money laundering* has occurred and had not been provided by his employer with the training required by the *2010 Act*. If the employer has failed to provide the training, this is an offence on the part of the employer. In these circumstances, it may not be reasonable for relevant employees to be held liable for failing to make a report; or
- it is known, or believed on reasonable grounds, that the *money laundering* is occurring outside Ireland, and is not unlawful under the criminal law of the country where it is occurring.

6.2.2.1 In determining whether a failure to disclose offence has been committed under Section 42(9), the Courts may have regard to the content of this Guidance when applied to an *individual,* delivering *defined services,* or to an *MLRO* or other nominated officer, where one is appointed under the *accountancy firm's* procedures.

Prejudicing an investigation ('tipping off')

6.2.4 A 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 concerning money laundering or terrorist financing has been, or is required to be made, commits an

offence if they make any disclosure that is likely to prejudice an investigation that may be conducted following the making of the report (section 49 of the *2010 Act*).

6.2.5 This offence is committed when an *individual* in the *designated sector* discloses that:

- an *STR* has been, or is required to be, made and this disclosure is likely to prejudice any subsequent investigation; or
- an investigation into allegations of *MLTF* is underway (or being contemplated) and this disclosure is likely to prejudice that investigation.

6.2.6 Considerable care must be taken when communicating with *client*s or third parties if any form of *STR* has been made or is required to be made. Before disclosing any of the matters reported, or to be reported, it is important to consider carefully whether to do so is likely to constitute an offence of *prejudicing an investigation*. It is suggested that *accountancy firms* keep records of these deliberations and the conclusions reached.

6.2.7 No *tipping off* offence is committed under Section 53(1)(c) of the *2010 Act*, if the person did not know or suspect that their disclosure was likely to prejudice any subsequent investigation.

Permitted Disclosures

6.2.8 There are a number of exceptions to this prohibition on revealing the existence of or requirement to make a report or an actual or contemplated investigation which are as follows:

- **Section 50 - Disclosure to customer in case of direction or order to suspend service or *transaction***: it is a defence for *accountancy firms* to prove that the disclosure was to a customer/*client*, who was the subject of an order or direction given to the *accountancy firm* not to carry out any specified service or *transaction* (by a member of *FIU Ireland* of the rank of superintendent or above and/or on application by the Garda Síochána to the District Court), in accordance with Section 17, and the disclosure made was solely that the effect that the *accountancy firm* had been so ordered/directed.
- **Section 51(1) - Disclosures within an undertaking:** it is a defence to prove that the disclosures in question were between agents, employees, partners, directors or other officers of the same undertaking.
- **Section 51(2) - Disclosures between *credit* or *financial institutions, or a* majority owned subsidiary or branch of such institution, belonging to the same group**: a person does not commit an offence where disclosure is made between two or more institutions, belonging to the same *group* (as defined in Section 52(2) of the *2010 Act*, and the institution receiving the disclosure is from a Member State or from a country other than a *high-risk third country*.
- **Section 51(3) - Disclosures between legal advisers or *relevant professional advisers* within different undertakings that share common ownership, management or control**: it is a defence for a legal adviser or a *relevant professional adviser* to prove that the disclosure was made to another legal adviser or a *relevant professional adviser* where both the person making the disclosure and the person to whom it was made are in either a Member State or from a country, other than a *high-risk third country*, as imposing equivalent anti-*money laundering* requirements and both undertakings share common ownership, management or control.

- **Section 52 - Other permitted disclosures between institutions or professionals**: it a defence for a *credit institution*, a *financial institution*, a legal adviser or a *relevant professional adviser* to prove that the disclosure was
    - to another institution of the same type (e.g. one *credit institution* to another) or professional of the same kind from a different undertaking but of the same professional standing (including being subject to equivalent duties of professional confidentiality and the protection of personal data within the meaning of the Data Protection Legislation);
    - related to the same *client* or former *client* of both institutions or advisers or involves a *transaction* or provision of a service that involved them both;
    - was made only for the purpose of preventing a *money laundering* or *terrorist financing* offence; and
    - was made to a person in an EU Member State or a State imposing an equivalent anti-money laundering requirements.

    This means that, for example, an accountant may only disclose to another accountant, and not to a lawyer or another kind of *relevant professional advisor*.

- **Section 53 - Other permitted disclosures (general)**: a defence is available if the accountancy firm or individual is able to prove that disclosure is made:
    - to a *competent authority* by virtue of the *2010 Act*, or
    - for the purpose of the detection, investigation or prosecution of a criminal offence in the Ireland or elsewhere, or
    - because the person did not know or suspect, at the time of the disclosure, that the disclosure was likely to prejudice an investigation into whether a *money laundering* or *terrorist financing offence* had been committed, or
    - by an *accountancy firm* ('a *relevant professional adviser*' per the legislation) to its *client* solely to the effect that the *accountancy firm* would no longer provide the particular service in question to the *client*, provided that the *accountancy firm* ceased providing the service thereafter and made any *external report* required in accordance with the *2010 Act.*

- Agents of, and other persons 'engaged under a contract for services' with, *accountancy firms* are required, under sections 41 and 42 of the *2010 Act*, to make a report to *FIU Ireland* and the Revenue Commissioners where they have knowledge, suspicion or reasonable grounds for suspicion that another person "has been or is engaged in an offence of *money laundering* or *terrorist financing"*. Such reporting is required, independently of the *accountancy firm* and unlike the approach of the *2010 Act* with regard to employees being permitted to report by way of an internal reporting procedure, agents do not fulfil their obligations by reporting up to the *accountancy firm* to which they are contracted by way of an agreed reporting procedure. Section 52 would, however, permit agents, who are themselves *external accountants*, to report their knowledge and suspicions also to the *accountancy firm* to which they are

contracted without committing the offence of prejudicing an investigation if such disclosure was for the purpose of preventing money laundering or terrorist financing.

6.2.9 A prohibited disclosure under section 49 of the *2010 Act (tipping off)* may be made in writing or verbally, and either directly or indirectly – including through inclusion of relevant information in published information. Considerable care is required in carrying out any communications with *clients* or third parties whilst considering whether to make a report as well as following any such report. Before any disclosure is made relating to matters referred to in an *internal report* or *an external report*, it is important to consider carefully whether or not it is likely to constitute an offence of *prejudicing an investigation*. It is suggested that *accountancy firms* keep records of these deliberations and the conclusions reached.

6.2.10 However, *individuals* and *accountancy firms* will frequently need to continue to deliver their professional services and a way needs to be found to achieve this without falling foul of the offence of *prejudicing an investigation*. More guidance on acting for a *client* after a *money laundering* suspicion has been formed is given in paragraph 6.5.3.

6.2.11 *Accountancy firms* should ensure they have sufficient document retention policies in place to meet their needs in this regard and in meeting their obligations under the *2010 Act*, as well as their legal and professional obligations more generally.

6.2.12 Falsification, concealment or destruction of documents relevant to an investigation (or causing the same) can also fall within this offence. Again, there is a defence if it was not known or suspected that the documents were relevant, or there was no intention to conceal facts.

6.3 When and how should a report be made?

Is a report required?

6.3.1 There are no hard and fast rules for recognising *MLTF*. It is important for everyone to remain alert to the risks and to apply their professional judgement, experience and scepticism.

6.3.2 All *individuals* involved in the conduct of the *accountancy firm's* business must, where concerned that criminal conduct may have occurred, ask themselves whether something they have observed in the course of business has the characteristics of *MLTF* and, therefore, warrants a *STR*. Most *firms* include in their standard anti-money laundering systems and controls arrangements to enable such individuals to discuss, with suitable people, whether their concerns amount to reportable knowledge or reasonable grounds for suspicion. *Individuals* should take advantage of these arrangements, where appropriate, to clarify reporting responsibilities

6.3.3 Once there is the requisite knowledge or suspicion, or reasonable grounds for either, then the staff member concerned must submit an *internal report* to their *MLRO* promptly. In exceptional circumstances, a report straight to *FIU Ireland and the Revenue Commissioners* may be appropriate. Sole practitioners make a report directly to *FIU Ireland* and the Revenue Commissioners.

6.3.4 There are no legal or other external requirements for the format of an *internal report* and accountancy firms may design their systems for internal reporting as they wish. *Internal reports* may be made orally or in writing, and may refer to *client* files or contain all the requisite information in a standard form, provided that all the

information as required by Section 42(6) of the *2010 Act* and other information which the accountancy firm requires under its procedures for the reporting of money laundering are reliably provided and recorded.

6.3.5 Deciding whether or not something is suspicious may require further enquiries to be made with the *client* or their records (all within the normal scope of the assignment or *business relationship*). The Irish anti-money laundering regime does not prohibit normal commercial enquiries to fulfil *client* duties, and these may help establish whether or not something is properly a cause for suspicion.

6.3.6 Investigations into suspected *MLTF* should not be conducted unless to do so would be within the scope of the *engagement*. Any information sought should be in keeping with the normal conduct of business. Normal business activities should continue (subject to the *firm's* consideration of the risks involved), with any relevant information or other matters that flow from those activities included in an *STR*. To perform additional investigations is not only unnecessary, it is undesirable since it would risk *tipping off* a money launderer.

6.3.7 *Individuals* may wish to consider the following questions to assist their decision:

Step	Question
1	• Do I have knowledge or suspicion, or reasonable grounds for suspicion, of criminal activity? Or • Am I aware of an activity so unusual or lacking in normal commercial rationale that it causes a suspicion or reasonable grounds for suspicion of *MLTF*?
2	• Do I know or suspect, or have reasonable grounds to suspect, that a benefit arose from the activity in 1?
3	• Do I think that someone involved in the activity, or in possession of the proceeds of that activity, knew or suspected that it was criminal?
4	• Can I identify the person (or persons) in possession of the benefit? Or • Do I know the location of the benefit? Or • Do I have information that will help identify the person (or persons)? Or • Do I have information that will help locate the benefits?

6.3.8 Note that the reporting requirement may relate to any information coming to an *accountancy firm* in the course of carrying on business as an *accountancy firm*, and not just information relating to *clients* and their affairs. This means that reports may be required on the basis of information not only about *clients*, but about potential *clients*, associates and counterparties of *clients*, acquisition targets and even employees of *accountancy firms.*

6.3.9 If in doubt, always report concerns to the *MLRO*.

***Internal reports to the MLRO or other* nominated officer**

6.3.10 Only sole practitioners, who employ no employees, or who themselves undertake the role of the *MLRO* (see section 3.2 of this guidance)*,.*have a duty to submit *STRs* straight to *FIU Ireland* and the Revenue Commissioners.

6.3.11 Section 44 of *the 2010 Act* provides for *individuals* undertaking work for an *accountancy firm* to make an *internal report* to their *MLRO* in accordance with an internal reporting procedure – reporting to a line manager or colleague is not enough to comply with the legislation. In making an *internal report* to their *MLRO,* the *individual* has a defence against accusations of failing to report under Sections 42 and 43 of the *2010 Act*. It is vital that all principals and staff of an *accountancy firm* clearly understand the communication lines for reporting suspicions of money laundering with the *accountancy firm's* procedures, and the importance of complying with those procedures in meeting the obligation both of *individuals* and of the *accountancy firm* under the legislation. Someone seeking reassurance that their conclusions are reasonable can discuss their suspicions with managers or other colleagues, in line with the *firm's* procedures.

6.3.12 When more than one member of staff is aware of the same reportable matter a single *internal report* can be submitted to the *MLRO*, but it should contain the names of all those making the report. No *internal report* should be made in the name of an individual who is unaware of the existence of the *internal report*. There is no prescribed format for internal *STRs* to be made to an *MLRO* or other nominated person.

6.3.13 The role of the *MLRO* should be undertaken by an appropriately experienced *individual*. One of the principals of an accountancy firm, or similar in other *accountancy firms*, is likely to be suitable, or another senior and skilled person with sufficient authority to enable decisions to be taken independently. Fulfilling that role in relation to STRs involves:

- considering *internal reports* of money laundering;
- deciding if there are sufficient grounds for suspicion to pass those reports on to *FIU Ireland* and the Revenue Commissioners in the form of an *external report*, and, if so, to make that report;
- acting as the key liaison point with *FIU Ireland* and the Revenue Commissioners;
- advising on how to proceed with work once an *internal report* and/or *external report* has been made in order to guard against risks of *prejudicing an investigation.*

6.3.14 If these responsibilities are not undertaken by the *MLRO*), they should be taken on by another sufficiently senior and skilled person within the *accountancy firm*. This person should work closely with the MRLO.

6.3.15 Depending on the size and complexity of an *accountancy firm*, it may establish procedures such that the functions of an *MLRO* can be delegated, although it would be advisable that the *MLRO* maintain close supervision of such delegated functions. It would also be advisable for *accountancy firms* to have contingency arrangements for discharging the duties of a *MLRO*, where appointed, during periods of absence or unavailability. *Accountancy firms* may consider appointing an alternate or deputy *MLRO* for these situations and ensure that the reporting channels are well known to all relevant employees.

6.3.16 Like all *individuals*, *MLROs*, where appointed, can commit the money laundering and *terrorist financing* offences as well as the related offences of failure to disclose and *prejudicing an investigation*.

Onward reports by the MLRO to FIU Ireland and the Revenue Commissioners

6.3.17 It is the *MLRO's* responsibility to decide whether the information reported internally needs to be reported to *FIU Ireland* and the Revenue Commissioners. When an *internal report* is submitted, there are two matters which need to be dealt with immediately. Rapid consideration of the *internal report* is needed as section 42(7) of the *2010 Act* requires, with only limited exceptions, that where a report is deemed necessary, it must be submitted before the *accountancy firm* proceeds with the *transaction* or service in question (see section 6.5). In addition, the *accountancy firm* should first establish by discussion and review whether or not the *professional privilege reporting exemption* may apply, as this exemption significantly affects not only whether an *external report* must be made under the legislation, but also whether it may be made.

6.3.18 External STRs to *FIU Ireland* are required to be made using the GoAML Online System. Guidance on registration and use of the system has been issued by the Department of Justice and Equality, and is available at *GoAML*.

6.3.19 Following acceptance of a report to *FIU Ireland* via GoAML*, a* printed copy of the online report should be forwarded to the Revenue Commissioners.

6.3.20 The *accountancy firm's* procedures should also address the process for considering whether or not to proceed with a *transaction* or service in circumstances where a report is deemed necessary but has not yet been submitted.

6.3.21 *MLROs* should approach external reporting with caution. When deciding what to do they should consider the following questions:

Step	Question
1	• Do I know or suspect (or have reasonable grounds for either) that someone is engaged in MLTF?
2	• Do I think that someone involved in the activity, or in possession of the proceeds of that activity, knew or suspected that it was criminal?
3	• From the contents of the internal *STR,* can I identify the suspect or the whereabouts of any laundered property if this information is available through normal conduct of business?
4	• Can I provide the information essential to an external *STR* without disclosing information acquired in privileged circumstances? The professional privilege reporting exemption is limits to *relevant professional advisers* as defined by the *2010 Act*. Further guidance on the privilege reporting exemption can be found in section 6.4 of this guidance.

6.3.22 The MLRO may want to make reasonable enquiries of within the *firm*. These may confirm the suspicion, but they may also eliminate it, enabling the matter to be closed without the need for an external *STR.*

6.3.23 The disclosure of information in accordance with the requirements of the *2010 Act* shall not be treated, for any purpose, as a breach of any other enactment or rule of law e.g. Data Protection Legislation (Section 47 of the *2010 Act*) or the *accounting firm*'s duty of client confidentiality

Timing of Reporting

6.3.24 Knowledge, suspicions or reasonable grounds for suspicion are deemed only to arise where the *accountancy firm* has scrutinised the information "in the course of reasonable business practice" (Section 42(3) of the *2010 Act*). *CCAB-I* understands this provision to emphasise that the information must come to the *accountancy firm* "in the course of carrying on business" of an *accountancy firm* (Section 42(1) of the *2010 Act*) and there is no obligation to complete an assessment of that information on a timescale which is different to that on which the *firm* normally conducts its business.

6.3.25 Care is advised in applying this provision, however, as information might come to an *accountancy firm* in circumstances where normal business practice might be that such information would typically not be scrutinised until a later date, which might be some time after the information is received. Section 42(2) requires a report "as soon as practicable after acquiring that knowledge or forming that suspicion". For example, audit conclusions are made at the end of the audit process and this may have an impact on the timing of the auditor's judgement that an issue is reportable under Section 42. In certain circumstances, an auditor may only be able to conclude at audit completion and sign off that he has reasonable grounds for suspecting that an offence resulting in proceeds has taken place. Also, information may be received during the course of an interim audit, which may take place some months before the planned audit completion and sign off, and such information might not normally be considered until a much later stage in the audit process.

6.3.26 An *accountancy firm* which does not deal with information for an extended period of time after receiving the information or forming the suspicion could expose itself to an accusation of a breach of Section 42(2) on timely reporting. Where doubt exists, it would be advisable to seek legal advice.

What information should be included in an external STR?

6.3.27 An *external report* to *FIU Ireland* is made by completing an *STR* on the GoAML website. Following the acceptance of that report by *FIU Ireland*, a copy of the accepted *STR* is sent to the Revenue Commissioners. Guidance can be found at http://www.antimoneylaundering.gov.ie/en/AMLCU/Pages/GoAML_and_Suspicious_Transaction_Reports_STRs. The following details are required by the *STR* report to be completed should be regarded as essential information:

- Name of reporter;
- Date of report;
- The name of the suspect or information that may help identify them, if this information is available. As many details as possible should be provided to *FIU Ireland* to assist with the identification of the suspect;

- Details of who else is involved, associated, and how, if this information is available;
- Clarification of the role of each subject/person, as far as it is known, in the matter, clearly identifying whether or not each subject/person is suspected of being involved in the commission of the alleged money laundering or *terrorist financing* offence;
- Information regarding bank account/*transaction* details, where available and relevant;
- The facts regarding what is suspected or the grounds for suspicion and why. The 'why' should be explained clearly so that it can be understood without professional or specialist knowledge;
- The whereabouts of any criminal property, or information that may help locate it, if this information is available;
- Section 42(6) requires that the *accountancy firm* include "any relevant information" in the *external report*. This could, for example, include the names of victims or other persons associated with the activity. If such persons are not suspected by the *accountancy firm* to be involved in the alleged *money laundering* of *terrorist financing* offence, the report should clearly state this.

6.3.28 All external *STRs* should be free of jargon and written in plain English.

6.3.29 It is recommended that in making an external STR the reporters:

- do not include confidential information not required by AML legislation;
- show the name of the *accountancy firm*, *individual* or *MLRO* submitting the report only once, in the source ID field and nowhere else;
- do not include the names of those who made the internal *STRs* to the *MLRO*;
- include other parties as 'subjects' only when the information is necessary for an understanding of the external *STR* or to meet *required disclosure* standards; and
- highlight clearly any particular concerns the reporter might have about safety (whether physical, reputational or other). This information should be included in the 'reasons for suspicion/disclosure' field.

Confidentiality

6.3.30 A correctly made external *STR* provides full immunity from action for any form of breach of confidentiality, whether it arises out of professional ethical requirements or a legal duty created by contract (e.g., a non-disclosure agreement).

6.3.31 There will be no such immunity if the external *STR* is not based on knowledge or suspicion or reasonable grounds for suspicion, or if it is intended to be 'defensive' i.e., for the purposes of regulatory compliance rather than because of a genuine suspicion.

Documenting reporting decisions

6.3.32 In order to control legal risks it is important that adequate records of internal *STRs* are kept. This is usually done by the *MLRO* or person nominated by the *MLRO* and would normally include details of:

- all internal *STRs* made;
- how the *MLRO* handled matters, including any requests for further information;
- assessments of the information provided, along with any subsequent decisions about whether or not to await developments or seek extra information;
- the rationale for deciding whether or not to make an external *STR*;
- any advice given to engagement teams about continued working.

These records can be simple or sophisticated, depending on the size of the *firm* and the volume of reporting, but they always need to contain broadly the same information and be supported by the relevant working papers. They are important because they may be needed later if the *MLRO* is required to justify and defend their actions.

6.3.33 For the *MLRO's* efficiency and ease of reference, a reporting index may be kept and each internal *STR* given a unique reference number.

6.4 Reporting and the privileged circumstances exemption

6.4.1 Section 46(1) of the *2010 Act* states that disclosure of information which is subject to legal privilege is not required. *Accountancy firms* and *individuals* may, in the course of their work, receive information documentation subject to legal privilege, for example when engaged by a legal professional to carry out work on behalf of a *client*.

6.4.2 Apart from legal privilege, Section 46(2) of the 2010 Act, as quoted below, also establishes that *relevant professional advisers* are not required to submit an *external report* in certain circumstances.

> "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."

6.4.3 *Relevant professional advisers* who know about or suspect *MLTF* (or have reasonable grounds for either) are not required to submit an external *STR* if the information came to them in privileged circumstances, defined in section 46(2) as being when ascertaining the legal position of the *client*. In these circumstances, and as long as the information was not provided with the intention of advancing a crime, then the information need not be reported. The *privileged reporting exemption* only covers *STRs* and should not be confused with legal professional privilege (see paragraph 6.4.2 above), which also extends to other documentation and advice.

6.4.4 In Section 24 of the *2010 Act*, *relevant professional adviser* is defined as an accountant, auditor or *tax adviser* who is a member of a designated accountancy body or of the Irish Institute of Taxation.

6.4.5 Whether or not the privilege reporting exemption applies to a given situation is a matter for careful consideration. The *firm* may have been providing the *client* with a variety of services, not all of which would create the circumstances required for the exemption. Consequently, it is strongly recommended that careful records are kept about the provenance of the information under consideration when decisions of this kind are being made. Legal advice may be needed.

6.4.6 Audit work, book-keeping, preparation of accounts or tax compliance assignments are unlikely to take place in privileged circumstances.

Discussion with the MLRO

6.4.7 Given the complexity of these matters – as well as the need for a considered and consistent approach to all decisions, supported by adequate documentation – it is recommended that they are always discussed with the *MLRO*.

6.4.8 Where the purpose of these discussions is to obtain advice on making a disclosure under Section 43 of the *2010 Act* they do not affect the applicability of the privilege reporting exemption.

The crime/fraud exception

6.4.9 Information received from or obtained in relation to a client that would otherwise qualify for the privilege reporting exemption are excluded from it when they are intended to facilitate or guide anyone in the furtherance of a criminal purpose. An example of this might be where tax advice was sought ostensibly to enable the affairs of a tax evader to be regularised but in reality was sought to aid continued evasion by improving the evader's understanding of the relevant issues. This is usually the *client* but could be a third party.

6.4.10 The criminal purpose exception does not apply where the adviser is approached to advise on the consequences of a crime or fraud or similar conduct that has already taken place and where the *client* has no intention, in seeking advice, to further that crime or fraud. This means that a person who is concerned that he may be guilty of tax evasion can approach a *tax adviser* for legal advice in this regard without fear of the exception being invoked. This remains the case even if the potential *client* declines a *client* relationship having received the advice, and the adviser does not know whether the person will proceed to rectify his affairs. However, if the person behaves in a way that makes the adviser suspicious that the intended use of the advice is to further continued evasion, then an *external report* could be required.

6.4.11 In summary, the following issues need to be considered before deciding whether to apply the professional privilege reporting exemption:

(a) Are those who received the information or other matter which gave rise to knowledge or suspicion of *money laundering or terrorist financing offences relevant professional advisers* (Section 24 of the *2010 Act*)?

(b) Was the information or other matter which gave rise to knowledge or suspicion of money laundering/*terrorist financing* received by the *relevant professional adviser* in privileged circumstances (Section 46(2) of the *2010 Act*) and not in some other communication or situation?

(c) Was the information or other matter received or communicated with the intention of furthering a criminal purpose (ie, does the criminal purpose exception apply (Section 46(3) of the *2010 Act*)?

If the answers to (a) and (b) are yes, and the answer to (c) is no, the professional privilege reporting exemption must be applied. If the answer to (a) and (b) are yes and the answer to (c) is yes, the criminal purpose exception applies and an *external report* must be made. Further advice should be sought from the relevant

professional body or a lawyer in cases of doubt. This issue may be vital in balancing legal and professional requirements for confidentiality and for serving the public interest and the interests of *clients*. If doubts cannot be resolved through internal discussion, through access to normal sources of professional advice, *accountancy firms* are strongly recommended to seek advice from a professional legal adviser with experience of these matters.

6.5 Determining whether to proceed with or withdraw from a *transaction* or service

6.5.1 As noted above, *external reports* must be made as soon as practicable. Section 42(7) of the *2010 Act* requires an *accountancy firm*, obliged to make an *external STR,* to do so before proceeding with any suspicious *transaction* or service that is connected with, or the subject of, the report. There are two exceptions to this requirement, namely:

- where it is not practicable to delay or stop the *transaction* or service from proceeding; or
- where the *accountancy firm* reasonably believes that a failure to proceed with the *transaction* would alert the other person to the possibility that a report may have been or will be made, or that an investigation is being contemplated or is on-going.

6.5.2 These exceptions do not apply to situations where the *accountancy firm* has received a valid direction from the Garda Síochána or an order from a judge of the District Court not to proceed with the *transaction* or service (see section 42(8) of the *2010 Act*).

6.5.3 When preparing to make an external *STR* the *MLRO* must consider carefully whether the *firm* would commit a *money laundering offence* if it continued to act as it intends (usually as instructed by the *client*).

Proceeding with a transaction or service

6.5.4 Examples of scenarios which may constitute a "*transaction* or service connected with, or the subject of, the report", requiring the *external STR* to be made prior to proceeding might include:

- acting as an insolvency officeholder when there is knowledge or a suspicion that either:
  - all or some assets in the insolvency are criminal property; or
  - the insolvent entity may enter into, or become concerned in, an arrangement which facilitates the “converting, transferring, handling, acquiring, possessing or using” the *proceeds of criminal conduct* (under section 7 of the *2010 Act*);
- designing and implementing trust or company structures (including acting as trustee or company officer) when there is knowledge or suspicion arises that the *client* is, or will, or may be about to, use these to launder money or finance terrorism;
- acting as an agent of a *client* in the negotiation or implementation of a *transaction* (such as a corporate acquisition) in which there is an element of criminal property being bought or sold by the *client*;

- handling through *client* accounts money that is suspected of being criminal in origin;
- providing outsourced business processing services to *client*s when the money is suspected of having criminal origins.

Typically, the issuing of an opinion on whether a set of financial statements give a true and fair view of the performance and financial position of the reporting entity is unlikely to be relevant to, or connected with, an *external STR* to *FIU Ireland* and the Revenue Commissioners regarding knowledge or suspicions of the commission of a *money laundering* or *terrorist financing offence*. However, if the auditor suspects that the audit report is necessary in order for financial statements to be issued in connection with a *transaction* involving the proceeds of crime, or if the auditor is due to sign off an auditor's report on financial statements for a company that he suspects to be a front for illegal activity, the auditor might be involved in an arrangement which facilitates the "converting, transferring, handing, acquiring possessing or using" the *proceeds of criminal conduct*.

Instructions not to proceed with a transaction or service

6.5.5 Under Section 17(1), a member of the Garda Síochána, who has a rank "not below the rank of superintendent", may direct a person, in writing, not to proceed with a particular service or *transaction* for the period specified in the direction, not to exceed seven days. A District Court Judge may also issue and order not to proceed with a specified service or transaction. For further details, see Appendix F.

6.6 What should happen after an external *STR* has been made?

Client relationships

6.6.1 *Accountancy firms* do not have to stop working after submission of an *external STR* unless a direction of an appropriate member of the Garda Síochána (rank of superintendent or above) or an order from a judge of the District Court is received (Appendix E), in which case all or part of *client* work may well need to be suspended until the relevant period of the direction/order lapses or notice is received in writing that the direction/order ceases to have effect.

6.6.2 Where an *external STR* involves a *client* as a suspect, *accountancy firms* may wish to consider whether the behaviour observed is such that for professional reasons the *accountancy firm* no longer wishes to act.

6.6.3 Generally, if following a report of suspicion, an *accountancy firm* wishes for its own commercial or ethical reasons to exit a relationship, there is nothing to prevent this provided the way the exit is communicated does not constitute an offence of *prejudicing an investigation* under section 49 of the *2010 Act*.

6.6.4 If a decision is made to terminate a *client* relationship, an *accountancy firm* should follow its normal procedures in this regard, whilst always bearing in mind the need to avoid *prejudicing an investigation*. Section 53(2) of the *2010 Act* provides a defence for a legal adviser or *relevant professional adviser* (see Section 24 of the *2010 Act*) in exiting a *client* relationship, as long as:

- the disclosure was solely to the effect that the legal adviser or *relevant professional adviser* would no longer provide the particular service concerned to the *client;*

- the service duly ceases once the *client* has been informed; and
- the *relevant professional adviser* made any report required in accordance with *the 2010 Act*.

Balancing professional work and the requirements of the 2010 Act

6.6.5 Normal commercial enquiries to understand a *transaction* carried out in the course of an engagement will not generally lead to *prejudicing an investigation*, although care should be exercised to avoid either making a disclosure prohibited under section 49 of the *2010 Act* (see paragraphs 6.2.4 to 6.2.12) or making accusations or suggesting that any person is guilty of an offence. It is important to confine enquiries to those required in the ordinary course of business and not attempt to investigate a matter unless that is within the scope of the professional work commissioned.

6.6.6 Continuation of work may require discussion with *client senior management* of matters relating to suspicions formed. This may be of particular importance in audit relationships. Care must be taken to select appropriate, and non-complicit, members of *senior management* for such discussion whilst always bearing in mind the need to avoid *prejudicing an investigation.*

6.6.7 In more complex circumstances, consultation with the Garda Síochána may be necessary before enquiries are continued, but in most cases a common sense approach will resolve the issue.

6.6.8 *Accountancy firms* may wish to consult the *MLRO*, where appointed, or other *individual(s)* in accordance with the *accountancy firm's* procedures, or other suitable specialist (for example a solicitor) regularly if there are concerns with regard to *prejudicing an investigation*, and, in particular, it is important that before any document referring to the subject matter of a report is released to a third party the *MLRO,* if appointed, is consulted and, in extreme cases, the Garda Síochána. Some typical examples of documents released to third parties are shown below as an aide memoire:

- public audit or other attest reports;
- public record reports to regulators;
- confidential reports to regulators (e.g. to the Central Bank of Ireland);
- provision of information to sponsors or other statements in connection with the Irish Stock Exchange Listing Rules;
- reports by a liquidator to the Director of Corporate Enforcement on the conduct of directors under Section 682 of the Companies Act 2014;
- statements on resignation as auditors in accordance with Section 400 and 403 of the Companies Act 2014;
- professional clearance/etiquette letters;
- communications to *clients* of intention to resign.

6.6.9 In particular, Section 400 of the Companies Act 2014 ('2014 Act') requires notice of auditor resignations to be filed at the Companies Registration Office and such notice to include statements of any circumstances "connected with the resignation to which it relates that the auditor concerned considers should be brought to the notice of the members or creditors of the company". Furthermore, Section 403 of the 2014 Act requires notification to the Irish Auditing and Accounting Supervisory Authority ('IAASA') where an auditor resigns in accordance with Section 400 of the 2014 Act, or

is removed in accordance with Section 399 of the 2014 Act, during the period between the conclusion of the last annual general meeting and the conclusion of the next annual general meeting. Notice of resignation to IAASA is to be accompanied by the resignation notice served under Section 400(3) of the 2014 Act (or, in the case of removal, by a copy of any representations made by the auditor to the company in accordance with Section 399(3) of the 2014 Act – except where they were not sent out to the members in accordance with Section 399(4)). The contents of such statements require careful consideration to ensure that statutory and professional duties are met, without including such information as may constitute an offence of *prejudicing an investigation*. There are no provisions in the *2010 Act* in this regard. However, *accountancy firms* may well wish, in cases of complexity, to discuss the matter with the Garda Síochána in order to understand their perspective and document such discussion.

6.6.10 Such a discussion with the Garda Síochána may well be valuable, but *accountancy firms* and *individuals* should bear in mind these authorities are not able to advise, and nor are they entitled to dictate how professional relationships should be conducted. It may be possible to arrive at an agreed wording, such that the *firm's* obligations are adequately addressed whilst the relevant law enforcement agency is satisfied that the wording would not *prejudice an investigation*. In such circumstances, it is unlikely that the *firm* will know or suspect that the report will *prejudice an investigation*. If the wording cannot be agreed, the *firm* or *individual* should seek legal advice and potentially the directions of the Court to protect itself.

6.6.11 *Accountancy firms* may on occasion need advice to assist them in considering such reporting issues. Legal advice may be sought from a suitably skilled and knowledgeable professional legal adviser, and recourse may also be had to helplines and support services provided by professional bodies.

6.7 Requests for further information

Requests from FIU Ireland and/or the Revenue Commissioners

6.7.1 *FIU Ireland* is responsible for receiving and analysing *STRs* and other information for the purpose of prevention, detection and investigation of possible MLTF offences. According to section 40C(3) of the *2010 Act* a member of the Garda Síochána, who is a member of *FIU Ireland*, may request, in writing, a *designated person* to provide any financial, administrative or law enforcement information that *FIU Ireland* requires to assist it in its functions. Additionally s42(6A) of the *2010 Act* requires a *designated person* who is required to make a *STR* to respond to any request for additional information by *FIU Ireland* or the Revenue Commissioners as soon as practicable after receiving the request and to take all reasonable steps to provide any information specified in the request.

6.7.2 Before responding, it is recommended that a verification process is undertaken to ensure the person making contact is a bona fide member of the Garda Síochána / the Revenue Commissioners. This may be most simply achieved by taking a caller's name and organisation details, and then calling the main switchboard of the organisation to be put through to the person.

6.7.3 To the extent that the request is simply aimed at clarifying the content of an *external report*, *accountancy firms/individuals* may respond without the need for any further process.

6.7.4 However, if the request is for production of documents or provision of information additional to the *external report*, it is recommended that *accountancy firms/individuals* require the relevant agency to use its powers of compulsion before they respond to requests by *FIU Ireland* or the Revenue Commissioners. This is not intended to be non co-operative, and indeed *accountancy firms/individuals* are recommended to engage in constructive dialogue with *FIU Ireland* / Revenue Commissioners, including as to the content and drafting of the request, but is intended to protect *accountancy firms/individuals* from allegations that they breached confidentiality. *Client* or other third party consent is not required in cases of compulsion, and nor should it be sought due to the risk of *prejudicing an investigation.*

6.7.5 Before providing information to a member of *FIU Ireland* or the Revenue Commissioners, *accountancy firms/individuals* should require evidence of the person's identity, for example, by showing official identification and a copy of the relevant order, or *accountancy firms* may attend the premises of the relevant agency to hand over the information.

6.7.6 Before responding to requests for further information, *accountancy firms/individuals* should ensure they understand

- the authority under which the request is made;
- the extent of the information requested;
- the required timing and manner of the production of information; and
- what information should be excluded *eg,* that subject to legal privilege.

If in any doubt, *accountancy firms/individuals* should seek legal advice. *Accountancyfirms* should document their consideration of the issues.

6.7.7 Information or documentation that is subject to legal privilege or legal professional reporting privilege should not be provided. If *individuals* or *accountancy firms* are unsure as to whether certain documents fall within the privileged category or not, they should not include these documents in response to enquiries and seek legal advice.

Requests arising from a change of professional appointment (professional enquiries)

Requests regarding client identification or information regarding suspicious transactions

6.7.8 In general, it is recommended that such requests are declined as the offence of *prejudicing an investigation* greatly restricts the ability to make such disclosures. It is recommended that *accountancy firms* do not respond to questions in professional enquiry letters concerning either their satisfaction as to the identity of an entity or natural person or as to whether any *external report* has been made or contemplated. *Accountancy firms* may wish to consider a standard wording in such responses to the effect that the legislation precludes them from responding to such queries.

Data protection - including subject access requests

6.7.9 Under the Data Protection Legislation *accountancy firms* need not comply with data subject access requests that are likely to prejudice the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties. Similarly, personal data that relates to knowledge or suspicion of *MLTF* (i.e., data that has been processed to help prevent or detect crime) should not be disclosed

under a subject access request especially as to do so could constitute *tipping off*. Both of these exceptions apply to the personal data likely to be contained in records relating to internal *MLTF* reports and *STRs*.

6.7.10 Personal data exempt from one subject access request may no longer be exempt at the time of a subsequent request (perhaps because the original suspicion has by then been proved false). When a *firm* receives a data subject access request covering personal data in its possession, it should always consider whether the exception applies to that specific request regardless of any history of previous requests relating to the same data. These deliberations will usually involve the *MLRO,* or other designated person, and the data protection officer. It is recommended that the thinking behind any decision to grant or refuse access is documented.

7 RECORD KEEPING

- Why may existing document retention policies need to be changed?
- What should be considered regarding retention policies?
- What considerations apply to *STRs* and directions, orders and authorisations relating to investigations?
- What considerations apply to training records?
- Where should reporting records be located?
- What do *accountancy firms* need to do regarding third-party arrangements?
- What are the requirements regarding the deletion of personal data?

7.1 Why may existing document retention policies need to be changed?

7.1.1 Records relating to *CDD*, the *business relationship* and *occasional transactions* must be kept for five years from the end of the *client* relationship. More specifically, records must be kept of *clients'* identity, the supporting evidence of verification of identity (in each case including the original and any updated records), the firm's *business relationships* with them (i.e. including any non- engagement related documents relating to the *client* relationship) and details of any *occasional transactions* and details of *monitoring* of the relationship.

7.1.2 All records related to an *occasional transaction* must be retained for five years after the date of the *transaction*.

7.1.3 The *2010 Act* does not specify the medium in which records should be kept, but they must be readily retrievable.

7.2 What should be considered regarding retention policies?

7.2.1 *Accountancy firms* must be aware of the interaction between of *MLTF* laws with the requirements of the GDPR. The Data Protection Regime 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.

7.3 What considerations apply to *STRs* and directions, orders and authorisations relating to investigations?

7.3.1 No retention period is officially specified for records relating to:

- *internal reports*;
- the *MLRO's* consideration of *internal reports*;
- any subsequent reporting decisions;
- issues connected to directions, orders and authorisations relating to investigations (sections 17-23 of the *2010 Act*), production of documents and similar matters;
- suspicious transaction reports;

- requests received for additional information in accordance with Section 42(6A) of the *2010 Act* sent to the Garda Síochána and Revenue Commissioners, or its responses to such requests;
- Copies of requests received from *FIU Ireland* or Revenue Commissioners in accordance with Section 41(1) of the *2010 Act*, copies of the relevant orders, evidence of agent's identity and resulting consideration of the matter by the firm;
- Requests from "relevant third parties" in accordance with Section 40 of the *2010 Act* and related considerations and responses.

7.3.2 Since these records can form the basis of a defence against accusations of MLTF and related offences, *firms* will determine an appropriate retention period for them, taking into account the Statute of Limitations and potential gravity of the underlying matter.

7.4 Where should reporting records be located?

7.4.1 Records related to internal and external *STRs* of suspicious *transactions* are not part of the working papers relating to *client* assignments. They should be stored separately and securely as a safeguard against *tipping off* and inadvertent disclosure to someone making routine use of *client* working papers.

7.5 What considerations apply to training records?

7.5.1 *Accountancy firms* must demonstrate their compliance with *2010 Act* that place a legal obligation on them to make sure that certain of their relevant employees are

(a) aware of the law relating to *MLTF*, and

(b) trained regularly in how to recognise and deal with *transactions* and other events which may be related to *MLTF*.

7.5.2 These records should show the training that was given, the dates on which it was given, which *individuals* received the training and the results from any assessments.

7.6 What do *accountancy firms* need to do regarding third-party arrangements?

7.6.1 An *accountancy firm* may arrange for another organisation to perform some of its AML related activities – *CDD* or training, for example. In which case, it must also ensure that the other party's record keeping procedures are good enough to demonstrate compliance with the *MLTF* obligations, or else it must obtain and store copies of the records for itself. It must also consider how it would obtain its records from the other party should they be needed, as well as what would happen to them if the other party ceased trading.

8 TRAINING AND AWARENESS

- Who should be trained and who is responsible for it?
- What should be included in the training?
- When should training be completed?

8.1 Who should be trained and who is responsible for it?

8.1.1 The *2010 Act* requires that all *individuals* involved in providing *defined services* (including partners are made aware of MLTF law and trained regularly to recognise and deal with activities which may be related to MLTF, as well as to identify and report anything that gives grounds for suspicion (see Section 6 of this guidance).

8.1.2 Thought should also be given to who else might need AML training. When identifying which staff may be considered relevant, *accountancy firms* should consider not only those who have involvement in *client* work, but also, where appropriate, those who deal with the *firm's* finances, and those who deal with procuring services on behalf of the *firm* and who manage those services. Accordingly, it is likely that all client-facing staff will be considered relevant and at least the senior support staff. *Firms* may decide to provide comprehensive training to all relevant staff members, or may choose to tailor their provision to match more closely the role of the employees concerned. In particular, *MLROs*, where appointed, or other individual(s) given significant responsibilities in relation to compliance with the firm's obligations under the *2010 Act,* may require supplementary training, and members of *senior management* may also benefit from a customised approach or some supplementary training.

8.1.3 The *MLRO* (or another member of senior management) should be made responsible for ensuring that appropriate AML training is delivered. There should be a mechanism to ensure that *individuals* complete their AML training promptly.

8.1.4 Someone accused of a failure-to-disclose offence has a defence if:

- they did not know or suspect that someone was engaged in money laundering even though they should have; but
- their employer had failed to provide them with the appropriate training.

8.1.5 This defence – that an*individual* did not receive the required AML training – is likely to put the *accountancy firm* at risk of prosecution for a regulatory breach.

8.2 What should be included in the training?

8.2.1 Training can be delivered in several different ways: face-to-face, self-study, e-learning, video presentations, or a combination of all of them.

8.2.2 The programme itself should include:

- an explanation of the law within the context of the *firm's* own commercial activities;
- so-called 'red flags' of which *individuals* should be aware when conducting business, which would cover all aspects of the MLTF procedures, including CDD (for example those that might prompt doubts over the veracity of evidence provided) and *STRs* (for example what might prompt suspicion); and

- how to deal with activities that might be related to *MLTF* (including how to use internal reporting systems), the *firm's* expectations of confidentiality, and how to avoid *tipping off* (see Section six of this guidance).

8.2.3 Training programmes should be tailored to each business area and cover the *firm's* procedures so that *individuals* understand the *MLTF* 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. Furthermore, *firm's* should aim to create an AML culture in which employees are always alert to the risks of *MLTF* and habitually adopt a risk based approach to *CDD*.

8.2.4 Records should be kept showing who has received training, the training received and when training took place (see 7.4 of this guidance). These records should be used so as to inform when additional training is needed – e.g. when the *MLTF* risk of a specific business area changes, or when the role of an *individual* changes.

8.2.5 The effectiveness of the training, should be considered on an ongoing basis.

8.2.6 The overall objective of training is not for employees and partners to develop a specialist knowledge of criminal law. However, they should be able to apply a level of legal and business knowledge that would reasonably be expected of someone in their role and with their experience, particularly when deciding whether to make an internal *STR* to the *MLRO* or other designated person.

8.3 When should training be completed?

8.3.1 *Accountancy firms* need to make sure that new employees are trained promptly.

8.3.2 The frequency of training events can be influenced by changes in legislation, regulation, professional guidance, case law and judicial findings (both domestic and international), the *firm's* risk profile, procedures, and service lines.

8.3.3 It may not be necessary to repeat a complete training programme regularly, but it may be appropriate to provide employees and partners with concise updates to help refresh and expand their knowledge and to remind them how important effective anti-money laundering work is.

8.3.4 In addition to training, *firms* are encouraged to mount periodic *MLTF* awareness campaigns to maintain alertness to individual and firm-wide responsibilities.

GLOSSARY

2005 Act Criminal Justice (Terrorist Offences) Act 2005

2010 Act Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 as amended by Criminal Justice Act 2013 and the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018.

2018 Act Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018.

Accountancy firm(s)/Firm(s) A firm, sole practitioner, company, partnership or other organisation undertaking *defined services*. This includes accountancy practices, whether structured as partnerships, sole practitioners or corporate practices.

Accountancy services For the purpose of this guidance this includes any service provided under a contract for services (i.e. not under a contract of employment) which pertains to the recording, review, analysis, calculation or reporting of financial information.

Business relationship a business, professional or commercial relationship between a *designated person* and a customer, which is expected by the *designated person*, at the time when contact is established, to have an element of duration.

Business risk assessment has the meaning given by section 30A of the *2010 Act* and shall take into account

- the type of clients that the firm has;
- the products and services that the designated person provides;
- the countries or geographical areas in which the firm or its clients operate (taking into account those jurisdictions identified as high risk by FATF and the EU);
- the type of services that the firm provides;
- the delivery channels used for those service;
- other prescribed additional risk factors.

Capital Requirements Regulations means Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for *credit institutions* and investment firms and amending Regulation (EU) No 648/2012.

CCAB-I the Consultative Committee of Accountancy Bodies in Ireland, which represents Chartered Accountants Ireland, the Association of Chartered Certified Accountants, the Chartered Institute of Management Accountants; and the Institute of Certified Public Accountants in Ireland.

CDD Client due diligence.

Client A person or entity in a *business relationship*, or carrying out an *occasional transaction*, with an *accountancy firm*.

Close associate of a *politically exposed person* means any individual has joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a *politically exposed person*; any individual who has sole beneficial ownership of a legal entity or a legal arrangement set up for the actual benefit of a *politically exposed person* (Section 37(10) of the *2010 Act*).

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 bodies identified by Sections 60 and 61 of the *2010 Act* as being empowered to supervise the compliance of *individuals* and *accountancy firms* with the *2010 Act*. [or in the case of an *Accountancy firm* the relevant designated accountancy body (eg the Association of Chartered Certified Accountants)].

Correspondent relationship (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 (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).

Criminal conduct conduct that constitutes an offence in Ireland as well as, in certain circumstances, conduct occurring elsewhere that (a) constitutes an offence under the law of that place and would have been an offence if it had taken place in Ireland or (b) 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 Ireland and the person or official concerned doing the act, or making the omission, concerned in relation to their office, employment, position or business is a foreign official within the meaning of that Act (Section 6 of the *2010 Act*).

Customer Due Diligence (CDD) The process by which information regarding the *or* is gathered, and the identity of a *client* is established and verified, for both new and existing *clients*.

Data Protection Legislation Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) as implemented in Ireland by the Data Protection Act 2018.

Defined services Activities carried on, in the course of business carried on by *accountancy firms firms* or *individuals* as an auditor, *external accountant*, insolvency practitioner or *tax adviser* or as *trust or company service providers* (eg company secretarial services).

Designated person has the meaning given by section 25 of the *2010 Act* as amended by the *2018 Act*.

EEA European Economic Area. Countries which form the combined membership of the European Union (EU) and the European Free Trade Association (EFTA).

Electronic money means electronic money within the meaning of the European Communities (Electronic Money) Regulations 2011 (S.I. No. 183 of 2011).

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* and in a number of specific situations (Sections 37 and 39 of the *2010 Act*).

EU Directive Refers in this document to the Forth Money Laundering Directive.

External accountant Means a person (an *accountancy 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 (Section 24 of the *2010 Act*).

External report Report made under Section 42 or 43 of the *2010 Act* to the *FIU Ireland* and the Revenue Commissioners.

FATF Financial Action Task Force. Created by G7 nations to fight money laundering.

Financial institution has the meaning given by Section 24 of the *2010 Act* as amended by Section 4 of the *2018 Act*.

FIU Ireland means those members of the Garda Síochána, or members of the civilian staff of the Garda Síochána, appointed by the Commissioners of the Garda Síochána who may carry out all the functions of an EU Financial Intelligence Unit under the Fourth Money Laundering Directive (Section 40A of the *2010 Act*).

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 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.

High-risk third country those jurisdictions identified by FATF, EU law or by other authoritative sources. Such jurisdictions identified by the EU as at February 2019 consist of the following:

- Afghanistan
- American Samoa
- The Bahamas
- Botswana
- Democratic People's Republic of Korea
- Ethiopia
- Ghana
- Guam
- Iran
- Iraq
- Libya
- Nigeria
- Pakistan
- Panama
- Puerto Rico
- Samoa
- Saudi Arabia

- Sri Lanka
- Syria
- Trinidad and Tobago
- Tunisia
- US Virgin Islands
- Yemen

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.

Individuals Includes the partners, directors, subcontractors, consultants and employees of *accountancy firms*.

Internal report A report made internally by an *individual* in accordance with procedures established by the *accountancy firm*.

Money laundering offences As defined in Section 7 of the *2010 Act,* 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 (Section 8), attempts outside the State to commit offences in the State (Section 9) and aiding, abetting, counselling or procuring outside the State commission of offence in the State (Section 10).

Irish AML Regime Irish anti-money laundering and *terrorist financing* regime.

MLRO *Money laundering reporting officer*: an individual designated as having responsibility for oversight of an *accountancy firm's* anti-money laundering and reporting procedures.

MLTF (money laundering and terrorist financing) Defined for the purposes of this document to include those offences relating to terrorist financing as defined under section 13 of the Criminal Justice (Terrorist Offences) Act 2005 as well as the money laundering offences defined by sections 6 to 11 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010.

Money laundering reporting officer See *MLRO*, above.

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.

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 €1,000,

(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) that the amount of money to be transferred is in aggregate not less than €1,000,

(bb) in a case where the *designated person* concerned is a person referred to in section 25(l)(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 (a), (b), or (bb), that the amount or aggregate of amounts concerned is not less than €10,000.

PEPs Politically exposed persons. As defined in section 37 of the *2010 Act* as amended by the *2018 Act* to include domestic PEPs and immediate family members of a PEP.

Predicate offence means the underlying offence or any offence as a result of which *criminal property* has been generated.

Prejudicing an investigation A 'related' *money laundering offence*, defined under section 49 of the *2010 Act*. 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 (section 6 of *2010 Act*).

Professional privilege reporting exemption an exemption from reporting suspicions formed on the basis of information received in privileged circumstances (see section 6.4 of this Guidance).

Public body means an FOI body within the meaning of the Freedom of Information Act 2014.

Regulated market (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 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 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 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 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).

Relevant independent legal professional 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).

Relevant professional adviser Defined in Section 24 of the *2010 Act* as an accountant, auditor or *tax adviser* who is a member of a designated accountancy body or of the Irish Taxation Institute.

Required disclosures The requirement under Section 42(6) of the *2010 Act* to disclose (a) information on which the knowledge, suspicion or reasonable grounds are based; (b) 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*; (c) the whereabouts, if known, of the criminal property; and (d) any other relevant information. Section 42(6A) requires a *designated person* who is required to make a report under this section to respond to any request for additional information by *FIU Ireland* or the Revenue Commissioners as soon as practicable after receiving the request and to take all reasonable steps to provide any information specified in the request.

STR Suspicious transaction report (see below).

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 partner of the firm concerned or a member of the management board.

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.

Suspicious transaction report: a report concerning suspicions of moneylaundering or terrorist financina made in accordance with section 42 of the *2010 Act* (also referred to as a *STR* (see above).

Statutory Auditor means an individual or firm who is approved in accordance with the Companies Act 2014, as amended by the Companies (Amendment) Act 2018.

Tax adviser means a person who by way of business provides advice about the tax affairs of other persons (Section 24 of *2010 Act*).

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 is listed in the annex to the Terrorist Financing Convention, or

(b) An act (other than one referred to in paragraph (a) —

i. 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

ii. 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 an act that is committed in or, in certain circumstances, outside the State and that (a) if committed in the State, would constitute an offence specified in Part 1 of Schedule 2 [of the 2005 Act], and (b) is committed with the intention of (i) seriously intimidating a population, (ii) unduly compelling a government or an international organisation to perform or abstain from performing an act, or (iii) seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a state or an international organisation); and

- terrorist-linked activity (defined as (a) an act that is committed in or, in certain circumstances, outside the State and that (i) if committed in the State, would constitute an offence specified in Part 2 of Schedule 2, and (ii) is committed with a view to engaging in a terrorist activity, (b) an act that is committed in or, in certain circumstances, outside the State and that (i) if committed in the State, would constitute an offence specified in Part 3 of Schedule 2, and (ii) is committed with a view to engaging in a terrorist activity or with a view to committing an act that, if committed in the State, would constitute an offence under section 21 or 21A of the Act of 1939, (c) public provocation to commit a *terrorist offence*, (d) recruitment for terrorism, or (e) training for terrorism.

Tipping off See *prejudicing an investigation.*

Transaction The provision of any service by an *accountancy firm* or *individual* to a *client* by way of business, or the handling of *client's* finances by way of business. Section 24 of the *2010 Act* defines transactions in the context of different '*designated persons*', including:

"(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."

Trust or company service provider means any person whose business it is to provide any of the following services as defined under Section 24 of *2010 Act*.

Vested interest Is an interest to which an entitlement already exists (whether immediately – 'in possession'; or in the future, following the ending of another interest – 'in remainder' or 'in reversion'). It is in contrast to an interest which is merely 'contingent'; a contingent interest is an interest which will only arise on the happening of a particular event, such as surviving to a particular date or surviving a particular person. Determining whether an interest is vested or contingent requires careful analysis. For example, if a trust provides that A has a life interest, and that B has an interest which takes effect on A's death, both A and B will have vested interests and, if B does not survive A, B's interest will devolve as part of B's estate; however, if B's interest is expressed to take effect on A's death only if he (B) is then living, B's interest (which will fail if he predeceases A) is merely contingent.

A *defeasible interest* is one which may be defeated, generally by the exercise of a power under the trust deed; an indefeasible interest is one which cannot be defeated. In the examples given above, A and B both have indefeasible interests. It is important that a defeasible vested interest is not mistaken for contingent interest. A defeasible vested interest will take effect unless and until it is defeated; a contingent interest on the other hand will not take effect unless and until the event on which it is contingent arises.

APPENDIX A: OUTSOURCING, SUBCONTRACTING AND SECONDMENTS

A.1 Outsourcing and subcontracting arrangements *later paragraph numbers to be conformed*

A.1.1 Where an *accountancy firm* chooses to outsource or subcontract work to a third party it is still obliged to maintain appropriate risk management procedures to prevent *MLTF*. This also requires the *firm* to consider whether the outsourcing or subcontracting increases the risk that it will be involved in, or used for, *MLTF*, in which case appropriate controls to address that risk should be put in place.

A.1.2 Where a *firm* contracts with a *client*, it remains responsible for ensuring that it undertakes *CDD* to Irish standards, including maintaining the appropriate records even if execution of all or part of the *client* work is outsourced or sub-contracted out. Some aspects of *CDD,* such as collecting documentary evidence, can also be delegated to an outsourcer or sub-contractor, but the *firm* remains responsible for compliance with Irish legislation.

A.1.3 Regardless of any outsourcing or subcontracting arrangement, a *firm* remains responsible for reporting any knowledge or suspicion of *MLTF* that comes to it in the course of its own activities. However a *firm* is not responsible for reporting knowledge or suspicion that comes to the attention of the outsourcer or sub-contractor, where such knowledge or suspicion has not been passed on to the *firm*. Subcontractors are subject to the reporting requirements of the *2010 Act* by virtue of section 41: however there is no legal obligation for an outsourcer or subcontractor to report knowledge or suspicion of *MLTF* to a *firm. Firms* may wish to establish a *MLTF* reporting protocol in the terms of engagement agreed with the subcontractor concerned. If an *STR* is made by the sub-contractor, the *firm* should consider its own reporting obligations. When a sub-contractor is integrated into an Irish business it may be appropriate for its staff to be trained in the *MLTF* procedures adopted by that *firm* so that common standards can be observed.

A.2 Secondees and those temporarily working outside of Ireland

A.2.1 A secondee is an individual legally employed by one organisation (the seconder) but acting as an employee of another. The formal terms of all secondments should make clear to all concerned how the secondee's legal obligations will be applied.

A.2.2 The position of a secondee working temporarily outside of Ireland or on foreign secondments but still within an Irish *firm* is difficult. For example the duty to report *MLTF* suspicions may be influenced by the terms of the secondment. Issues to consider include:

- If the work outside of Ireland is part of an Irish *defined service* then in some circumstances the *MLTF* suspicion will be reportable;
- an *individual* should be particularly cautious about any decision not to make a *STR* in accordance with the secondee's legal employer's procedures if the information relates to work that they are undertaking in Ireland or to an entity incorporated, or an individual resident, in Ireland.

A.2.3 Arrangements must be considered on their own facts to determine which policies and procedures the secondee should follow. *Accountancy firms* may wish to take legal advice in relation to the need for their relevant employees to comply with the Ireland's money laundering reporting regime as well as any local legal requirements, and in relation to the drafting of appropriate secondment agreements.

A.3 Reporting requirements for subcontractors

A.3.1 Where all or part of a piece of work is contracted-out to a subcontractor there is no legal requirement for the subcontractor to report suspicious *transactions* to the referring *firm's MLRO*, although this may be addressed in the engagement terms agreed by the *firm* with the subcontractor concerned. Whether or not such reporting is agreed between the parties, where the subcontractor notifies the referring *firm* of information which gives rise to a *MLTF* suspicion, the referring *firm* must consider its own reporting obligations.

APPENDIX B: *CLIENT* VERIFICATION

As discussed in section 5 of this guidance, documentation purporting to offer evidence of identity may emanate from a number of sources. These documents differ in their integrity, reliability and independence. Some are issued after due diligence on an individual's identity has been undertaken; others are issued on request, without any such checks being carried out. There is a broad hierarchy of documents:

- certain documents issued by government departments and agencies, or by a court; then
- certain documents issued by other public sector bodies or local authorities; then
- certain documents issued by regulated firms in the financial services sector; then
- those issued by other firms subject to the *2010 Act*, or to equivalent legislation; then
- those issued by other organisations.

B.1 Individuals

***Client* identification:**

B.1.1 The full name, date of birth and residential address should be obtained.

***Client* Verification:**

B.1.2 A document issued by an official (e.g., government) body is deemed to be independent and reliable source even if provided by the *client*. Documents should be valid and recent. Documents sourced online should not be accepted if there is any suspicion regarding the provenance of the documents. The following is a suggested non-exhaustive list of sources of evidence.

Risk profile	Verification
Normal risk	The original, or an acceptably certified copy, of one of the following documents or similar should be seen and a copy retained: • valid passport • valid photo card driving licence • national Identity card
Higher risk	The original of a second document should be seen and a copy retained. This should be one of the following: • Recent evidence of entitlement to a state- or local authority-funded benefit (including housing benefit, council tax benefit, tax credits, state pension, educational or other grant). • Instrument of a court appointment (such as a grant of probate). • Documents issued by the Revenue Commissioners, such as PAYE coding notices and statements of account (NB: employer issued documents such as P60s are not acceptable). • End of year tax deduction certificates. • Current (within last 3 months) bank statements or credit/debit card statements issued by a regulated financial sector firm in Ireland, EU or designated place under Section 31. • Current utility bills. • An electoral register search showing residence in the current or

Risk profile	Verification
	most recent electoral year (can be done via http://www.checktheregister.ie/. • A solicitor's letter confirming recent house purchase or land registry confirmation (you should also verify the previous address).

Source of wealth and source of funds

B.1.3 Where appropriate, evidence can be obtained from searching public information sources like the internet, company registers and land registers.

B.1.4 If the *client*'s funds/wealth have been derived from, say, employment, property sales, investment sales, inheritance or divorce settlements, then it may be appropriate to obtain documentary proof.

B.2 Private companies

***Client* identification**

B.2.1 The following information must be obtained and verified:

- full name of company
- registered number
- registered office address and, if different, principal place of business
- any shareholders/members who ultimately own or control more than 25% of the shares or voting rights (directly or indirectly including bearer shares), or any individual who otherwise exercises control over management must be identified (and verified on a risk sensitive basis).
- The identity of any agent or intermediary purporting to act on behalf of the entity and their authorisation to act e.g., where a lawyer engages on behalf of an underlying *client*.

Unless the entity is listed on a *regulated market*, reasonable steps should be taken to determine and verify:

- the law to which it is subject
- its constitution (for example via governing documents)
- the full names of all directors (or equivalent) and senior persons responsible for the operations of the company.

Company registers of beneficial ownership may be used but not solely relied upon.

B.3 Listed or regulated entity

***Client* identification**

B.3.1 The following information should be gathered:

- full name
- membership or registration number
- address

***Client* verification**

Risk Profile	Recommended verification
Normal/ high risk	One of the following documents should be seen and a copy retained: • a printout from the web-site of the relevant regulator or exchange (which should be annotated); • written confirmation of the entity's regulatory or listing status from the regulator or exchange.

B4. Government or similar bodies

Client identification

B.4.1 The following information should be gathered:

- full name of the body
- main place of operation
- government or supra-national agency which controls it

Client verification

Risk Profile	Recommended verification
Normal/ high risk	The following information should be obtained and reviewed, and a copy retained: • a printout from the web-site of the relevant body (which should be annotated). Additionally for housing associations: • the printout must contain its registered number, registered company number (where appropriate) and registered address.

APPENDIX C: *STR* REPORTING PROCESS CHECKLIST

Should I report to the MLRO?		**As the MLRO, should I report externally?**
• Do I have knowledge or suspicion of criminal activity resulting in someone benefitting? • Am I aware of an activity so unusual or lacking in normal commercial rationale that it causes a suspicion of money laundering? • Do I know or suspect a person or persons of being involved in crime? • Do I think that the person(s) involved in the activity knew or suspected that the activity was criminal? • Can I explain my suspicions coherently? In making a report to the MLRO, consider whether you are aware of information as to who might have received the benefit of the criminal activity, or where the criminal property might be located, based on information obtained in the conduct of firm's business.		• Do I know, suspect or have reasonable grounds to know or suspect that another person is or was engaged in money laundering; **and** • Did the information or other matter giving rise to the knowledge or suspicion come to me in an internal STR? • Was the information scrutinised in the course of reasonable business practice? • Does the privileged circumstances exemption apply (see section 6.4)?

CHECKLIST: Essential elements of an external SAR – to be submitted using GoAML and copied to the Revenue Commissioners in hard copy

- Name of reporter;
- Date of report;
- Who is suspected or any information available to the *accountancy firm* or individual making the report that may assist in ascertaining the identity of the suspect (which may simply be details of the victim and the fact that the victim knows the identity but this is not information to which the firm is privy in the ordinary course of its work). The reporter should provide as many details as possible to allow *FIU Ireland* to identify the main subject; together with

(*continued overleaf)*

- Who is otherwise involved in or
- The facts;
- What is suspected and why;
- Any information available to the *accountancy firm* or individual regarding the whereabouts of any criminal property or information that may assist in ascertaining it.
- Reports should generally be jargon free and written in plain English.

associated with the matter and in what way.

APPENDIX D: RISK FACTORS

High risk factors

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 the EU as having strategic deficiencies in their regime for countering money-laundering and terrorist financing. As of 13 February 2019, 23 jurisdictions had been identified by the EU process, which takes into account *FATF* assessments: the list and commentary is available on the Europeans Commission website here

(b) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to combat *MLTF*;

(c) countries identified by credible sources as having significant levels of corruption or other criminal activity;

(d) countries subject to sanctions, embargos or similar measures issued by organisations such as, for example, the European Union or the United Nations;

(e) countries (or geographical areas) providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country."

Low risk factors

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).

APPENDIX E: DIRECTIONS FROM GARDA SIOCHAN OR COURT REGARDING PROCEEDING WITH A TRANSACTION OR SERVICE

E1 Directions not to proceed

E1.1 Under Section 17(1), a member of the Garda Síochána, who has a rank "not below the rank of superintendent", may direct a person, in writing, not to proceed with a particular service or *transaction* for the period specified in the direction, not to exceed seven days.

E1.2 An order to proceed may also be made by the District Court. Details of relevant circumstances and processes to be followed in relation to such orders are set out in

E1.3 The direction:

- may, but is not required to be, issued on foot of a report made by an *accountancy firm* under Section 42 of the *2010 Act*;
- is made on the basis that the member of the Garda Síochána is satisfied that the direction is reasonably necessary to allow preliminary investigations to be carried out to establish whether or not there are reasonable grounds to suspect that the service or *transaction* would comprise or assist in money laundering or *terrorist financing.*

E2 Order from a judge of the District Court not to proceed

E2.1 Section 17(2) of the *2010 Act* also provides for an order from a District Court Judge not to proceed with a specified service or *transaction* for the period specified in the order, not to exceed 28 days. However, such orders may be made on more than one occasion, in accordance with Section 17(3) of the *2010 Act*.

E.2.2 In making such an order, the District Court Judge is satisfied by information provided on oath by a member of the Garda Síochána that:

- There are reasonable grounds to suspect that the service or *transaction* would comprise or assist *money laundering* or *terrorist financing*, and
- An investigation of a person for that *money laundering* or *terrorist financing* is taking place.

E.2.3 Applications for an order by a District Court Judge are made to a judge of the District Court in the district where the order is to be served (Section 17(4) of the *2010 Act*).

E3 Directions and orders - compliance; notice

E.3.1 Failure to comply with a direction of the Garda Síochána or an order from a judge of the District Court is an offence. Any person acting in compliance with a direction or order will not be treated as having breached any requirement or restriction imposed by any other enactment or rule of law.

E.3.2 Section 18(1) of the *2010 Act* obliges the member of the Garda Síochána, who issues the direction or applies to the District Court for the order, to give notice in writing to any person, whom he knows to be affected by the direction or order, as soon as practicable after the direction is given or order is made, unless:

- it is not reasonably practicable to ascertain the whereabouts of the person; or

- there are reasonable grounds for believing that disclosure would prejudice the investigation.

E3.3 If the member of the Garda Síochána becomes aware that a person who is affected by the direction or order is aware of the direction or order, then the member of the Garda Síochána is obliged to inform him in writing as soon as practicable thereafter of the direction or order, notwithstanding the above provision about *prejudicing the investigation* (Section 18(2)) of the *2010 Act*.

E3.4 The notice in writing shall include the reasons for the direction or order and advise the person of their rights to apply the District Court:

- (under Section 19 of the *2010 Act*) for a revocation of the direction or order; or
- (under Section 20of the *2010 Act*) for an order to in relation to any of the property concerned (a) to discharge reasonable living expenses and other necessary expenses of the person and/or the person's dependents or (b) to carry on a business, trade, profession or other occupation to which any of the property relates.

E3.5 Under Section 19 of the *2010 Act*, a judge of the District Court may revoke a direction or order on application by a person affected by the direction/order, if satisfied that the grounds for the direction/order do not, or no longer, apply.

E3.6 The direction or order ceases to have effect on the cessation of the investigation. As soon as practicable thereafter, a member of Garda Síochána is obliged to inform, in writing, both the person who received the direction or order and any other person whom the member is aware is affected by the direction or order.

E4 Authorisation from the Garda Síochána to proceed

E4.1 A member of the Garda Síochána, not below rank of superintendent, may authorise, in writing, a person to proceed with a service or *transaction*, which would otherwise comprise or assist *money laundering*, if the member is satisfied that to do so is necessary for the purposes of the investigation (Section 23 of the *2010 Act*).

E5 Suspension of Activity

E5.1 Once a direction or order has been received, the process must be adhered to and the activity that would otherwise be a *money laundering* or *terrorist financing* offence refrained from until the notice period has expired or notice in writing has been received that the direction or order has ceased to have effect. Failure to do so risks prosecution either for a *money laundering* or *terrorist financing* offence, which is punishable by imprisonment and/or a fine.

E5.2 Section 50 of the *2010 Act* provides a defence against the offence of making a disclosure which prejudices an investigation where disclosure is made to a *client* that the defendant (the *accountancy firm*) was directed by the Garda Síochána or ordered by a judge of the District Court not to carry out any specified service or *transaction* in respect of the *client*. Disclosure must be made only to the *client* and must be solely to the effect that the *accountancy firm* has been so directed / ordered.