An Roinn Dlí agus Cirt
Department of Justice

Anti-Money Laundering & Countering the Financing of Terrorism

Guidelines for Designated Persons supervised by the Anti-Money Laundering Compliance Unit (AMCLU)

(Published 28th March 2024)

Version Control

Version	Author	Comments	Date
1.0	Anti-Money Laundering Compliance Unit, Department of Justice	Initial Publication	28th March 2024

The AMLCU will update or amend the Guidelines from time to time, as appropriate. Following initial publication, a first review process shall be completed within one year.

Table of Contents

1 Glossary

AGS	An Garda Síochána
AML	Anti-Money Laundering
AML/CTF	Anti-Money Laundering and Countering the Finance of Terrorism
AMLCU	Anti-Money Laundering Compliance Unit
Beneficial Ownership Register	Central register of the beneficial owners of Certain Financial Vehicles (CFV)
BRA	Business Risk Assessment
CDD	Customer Due Diligence
Central Bank	The Central Bank of Ireland
CJA 2005	Criminal Justice (Terrorist Offences) Act 2005
CJA 2010 as amended	Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 as amended
CRA	Customer/Transaction Risk Assessment
CRBOT	Central Register of Beneficial Ownership
CRO	Companies Registration Office
DABs	Designated Accountancy Bodies
Designated Person	Defined under Section 25 of the Act
DNFBP	Designated Non-Financial Businesses and Professions
EDD	Enhanced Due Diligence
EFT	Electronic Funds Transfer
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
HVGD	High Value Goods dealers
KYC	Know Your Customer
ML	Money Laundering
ML/TF	Money Laundering and Terrorist Financing
MLRO	Money Laundering Reporting Officer
NFTs	Non-Fungible Tokens (digital assets)
NRA	National Risk Assessment
NRA	National Risk Assessment
CEA	Corporate Enforcement Authority
PEPs	Politically Exposed Persons
PMC	Private Members Club
RBO	Registration of Beneficial Ownership
Relevant Third Party	Those persons identified in Section 40 of the Act
ROS	Revenue Online Services
SI 487 of 2018	Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (Section 25) (Prescribed Class of Designated Person) Regulations 2018

SOF/SOW	Source of Funds/Source of Wealth
SNRA	EU's Supranational Risk Assessment
STR	Suspicious Transaction Report
TCSP	Trust or Company Service Provider
TF	Terrorist Financing
The Act	Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 as amended
VASP	Virtual Asset Service Provider

Section 1

General Guidelines for Designated Persons Supervised by the AMLCU

2 Introduction

2.1 Purpose of guidance

The purpose of the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Guidelines (the Guidelines) is to assist those Designated Persons* supervised by the Department of Justice Anti-Money Laundering Compliance Unit (AMLCU) in understanding and meeting their AML/CFT obligations under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 as amended** and related Statutory Instruments.

The Act provides for the supervision of Designated Persons i.e. designated financial and non-financial businesses and professions to ensure compliance with their statutory obligations. Under Section 60 of the Act, a number of separate competent authorities are prescribed as supervisors of Designated Persons, depending on the business type.

These are non-statutory Guidelines. Designated Persons must always refer to the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 as amended when ascertaining their statutory obligations. These Guidelines are not exhaustive nor to be considered as legal advice or legal interpretation. It remains solely the responsibility of the Designated Person to ensure that they meet their statutory obligations under the CJA 2010 as amended. It is a matter for Designated Persons to seek legal advice if they are unsure regarding the application of the CJA 2010 to their particular set of circumstances.

Where there is any discrepancy between these Guidelines and the CJA 2010 as amended, the CJA 2010 as amended will apply.

* See Table 1, p12.
** Also referred to as 'CJA 2010 as amended' / the 'Act' in this publication.

2.2 Introduction to the legislation (the Act)

Irish anti-money laundering legislation is largely contained within the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended. This Act and the legislation which has amended it gives effect to the European Union's Anti-Money Laundering Directives, the latest of which is Directive (EU) 2018/843, commonly referred to as the "Fifth Anti-Money Laundering Directive".

The Act provides an AML/CTF framework that requires Designated Persons to adopt an effective risk-based approach to managing their businesses. This includes a risk-based approach to Customer Due Diligence, assessment of risk, AML/CTF training, record keeping, internal controls and the reporting of suspicious transactions - all of which are required to combat the crime of money laundering and the financing of terrorism.

The Act places a number of obligations on Designated Persons to ensure they safeguard their business from being used to facilitate money laundering (ML) or terrorist financing (TF).

The obligations on Designated Persons include, inter alia, requirements to:

- Understand risks and threats potentially facing their business;
- Carry out an AML/CFT risk assessment of their business, risk assess customers and transactions and adopt a risk-based approach to ensuring their business is not used for ML/TF;
- Demonstrably implement appropriate AML/CFT policies and procedures and ensure all staff involved in the business are instructed on the law relating to ML/TF;
- Identify and verify the identity of relevant customers and beneficial owners and apply the appropriate level of Customer Due Diligence (CDD) depending on the risk associated with the customer;
- Monitor transactions and be alert to unusual transactions or transaction patterns not in line with expectations of the customer and their source of funds;
- Report suspicious activity to the Financial Investigation Unit (FIU) and the Revenue Commissioners using the GoAML and ROS systems;
- Retain records evidencing the procedures applied, and information obtained, in respect of each customer, where required.

The Minister for Justice is recognised as a 'Competent Authority' under Section 60 of the CJA 2010 as amended. Under Section 108 of the Act, the Minister has delegated the Minister's Competent Authority functions to the Anti-Money Laundering Compliance Unit (AMLCU) of the Department of Justice. Section 60 of the Act also sets out which competent authorities are responsible for supervising the various categories of Designated Persons under the Act.

The AMCLU supervises the following categories of non-financial businesses and professions, as provided for under the Act:

- High Value Goods Dealers (HVGDs);
- Trust or Company Service Providers (TCSPs) not otherwise supervised;
- Notaries not otherwise supervised;
- Tax Advisers not otherwise supervised;
- External Accountants (not supervised by the prescribed accountancy bodies);
- Gambling Service Providers (private members' clubs, retail bookmakers, on course bookmakers and online gambling providers);
- High Value Art Traders and Art Intermediaries.

Under the Act's framework, in principle, existing regulators will be designated as the Competent Authority for AML/CFT supervision of their regulated populations. The AMLCU is responsible for supervising those Designated Persons not subject to supervision by another Competent Authority.

2.3 International Context

The Financial Action Task Force (FATF) is the global standard setting body in the area of AML/CFT. It is an inter-governmental body founded in 1989 which sets standards to assist its 39 members (37 jurisdictions and 2 regional organisations) in preventing, detecting and investigating ML/TF. It publishes guidance on the risk-based approach to AML/CFT, including sector specific guidance. FATF's 40 Recommendations are widely considered the global standard for combating ML/TF. The FATF website[1] is a useful source of guidance for Designated Persons. The FATF monitors countries' progress in implementing the FATF Recommendations[2]; reviews money laundering and terrorist financing methods and counter-measures; and, promotes the adoption and implementation of the FATF Recommendations globally as a means of combatting ML and TF. These periodic reviews are known as Mutual Evaluation Reviews (MERs).

The European Union (EU) is also active in seeking to prevent ML and TF and proposes AML/CFT legislation, which Member States (and EEA members) either transpose or which is directly effective. To date, Ireland has transposed EU legislation through the Act and related statutory instruments. The EU has produced a supranational risk assessment[3] examining the risks of ML and TF within the EU across various business types, which Designated Persons may find to be a useful source of information.

2.4 What is Money Laundering?

Money Laundering is the process by which criminals attempt to conceal the illicit origin and ownership of the proceeds of their unlawful activities. This process may involve the use of legitimate businesses and service providers, often without their knowledge or consent. The AML/CFT framework introduced in Ireland by the Act is aimed at preventing this from occurring.

[1] https://www.fatf-gafi.org
[2] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html
[3] https://commission.europa.eu/system/files/2019-07/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union_-_annex.pdf

The offence of Money Laundering is set out in Section 7(1) of the CJA 2010 as amended:

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.

Section 6 of the CJA 2010 as amended defines the "proceeds of criminal conduct" as:

"… any property that is derived from or obtained through criminal conduct, whether directly or indirectly, or in whole or in part…"

2.5 What is Terrorist Financing?

Terrorist financing is commonly defined as the provision, collection or receipt of funds with the intent or knowledge that the funds will be used to carry out an act of terrorism or any act intended to cause death or serious bodily injury.

"Terrorist financing" is defined in the Act, as an offence under Section 13 of the Criminal Justice (Terrorist Offences) Act 2005 ("CJA 2005").

Section 13(1) of CJA 2005 provides that a person is guilty of a terrorist financing offence if:

> *13(1) "…in or outside the State, the person by any means, directly or indirectly, unlawfully and wilfully provides, collect 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 that 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) This 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."*

Section 13(2) of CJA 2005 provides that a person who attempts to commit an offence under subsection (1) is guilty of an offence.

IMPORTANT NOTE: It is the ultimate responsibility of all Designated Persons to ensure that they are compliant with their obligations under the CJA (Money Laundering and Terrorist Financing) 2010 as amended. These guidelines are intended as an aid to achieving understanding of and compliance with those obligations.

3 Legislation

3.1 Scope of obligations under the Act

The Act applies to all Designated Persons.

3.2 Meaning of Designated Person and whether a business is a Designated Person under the Act

Section 25 of the CJA 2010 as amended sets out the meaning of a 'Designated Person'.

Section 25 of Act can be found on the Law Reform website, here: **https://revisedacts.lawreform.ie/eli/2010/act/6/revised/en/html#SEC25**.

The below table sets out the various Designated Persons and their Competent Authority with responsibility for their supervision for compliance with the Act.

Table 1: Designated Persons and competent authorities under the Act

Designated Person	Competent Authority
Regulated Credit and Financial Institutions (including some TCSPs which are subsidiaries of regulated entities)	Central Bank of Ireland
Solicitors	Law Society of Ireland
Barristers	Legal Services Regulatory Authority (LSRA)
Accountants, Auditors, Tax Advisers and some TCSPs in specific circumstances	6 Designated Accounting Bodies (DABs)
Property Service Providers	Property Services Regulatory Authority (PSRA)
Any Designated Person who is not subject to supervision by another regulator: - Dealers in High Value Goods (HVGDs) - Trust or Company Service Providers (TCSPs) not otherwise supervised; - Notaries not otherwise supervised; - High Value Art Traders and Art Intermediaries; - Tax Advisers not otherwise supervised; - External Accountants (not within the remit of the DABs); - Gambling Service Providers (private members clubs, retail bookmakers, on-course bookmakers and online gambling providers).	Minister for Justice (delegated to the AMLCU under Section 108 of the Act)

3.3 Designated Persons supervised by the AMLCU

As set out in Table 1, the AMLCU supervises those entities:

- Trust or Company Service Providers, Tax Advisers, External Accountants and Notaries where they are not otherwise supervised by another Competent Authority; and
- High Value Goods Dealers, High Value Art Traders and Art Intermediaries and Gambling Service Providers.

3.4 Definitions

The definitions for those 'Designated Persons' supervised by the AMLCU are as follows:

Section 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—*

Tax Advisers and External Accountants

…(c) an auditor, external accountant, tax adviser or any other person whose principal business or professional activity is to provide, directly or by means of other persons to which that other person is related, material aid, assistance or advice on tax matters.

These are defined in Section 24. – (1) as follows:

… *"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 the person holds accountancy qualifications or is a member of a designated accountancy body.*

(Note: Designated Accountancy Body under s.24 means a prescribed accountancy body, within the meaning of Part 2 of the Companies (Auditing and Accounting) Act 2003).

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

Trust or Company Service Providers (TCSPs)

… (e)"trust or company service provider"

This is defined in Section 24. – (1) as follows:

… "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.

Gambling service providers

… (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.

Under *S.I. 487 of 2018*, providers of gambling services became a class of Designated Person for the purpose of Section 25(1)(j) of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 as amended.

"Gambling services" in the SI has the same meaning as Directive 2015/849. Under article 3 of the Directive:

> *'gambling services' means a service which involves wagering a stake with monetary value in games of chance, including those with an element of skill such as lotteries, casino games, poker games and betting transactions that are provided at a physical location, or by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services.*

Note: Where providers of gambling services are operating remotely but providing gambling services in the State; then irrespective of the jurisdiction given as their registered address, per the definition above, they constitute Designated Persons under the Act, with all the obligations that entails.

Under *S.I. 487 of 2018*, the following are <u>not</u> included in the definition:
(*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.

High Value Goods Dealers

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

Art traders and art intermediaries

… (ib) a person trading or acting as an intermediary in the trade of works of art (including when carried out by an art gallery or an auction house) but only in respect of transactions of a total value of at least €10,000 (whether in one transaction or in a series of transactions that are or appear to be linked to each other);

… (ic) a person storing, trading or acting as an intermediary in the trade of works of art when this is carried out in a free port but only in respect of transactions of a total value of at least €10,000 (whether in one transaction or as a series of transactions that are or appear to be linked to each other).

Notaries

Section 25. – (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).*

This is defined in Section 24. – 1 as follows:
… "relevant independent legal professional" means a barrister, solicitor or notary who carries out any of the following services:
(a) the provision of assistance in the planning or execution of transactions for clients concerning any of the following:

(i) buying or selling land or business entities;
(ii) managing the money, securities or other assets of clients;
(iii) opening or managing bank, savings or securities accounts;
(iv) organising contributions necessary for the creation, operation or management of companies;
(v) creating, operating or managing trusts, companies or similar structures or arrangements;

(b) acting for or on behalf of clients in financial transactions or transactions relating to land.

3.5 The Anti Money Laundering Compliance Unit

The Minister for Justice has delegated the Minister's Competent Authority functions under Section 108 of the Act to the Anti-Money Laundering Compliance Unit (AMLCU) in the Department. The AMLCU is recognised as a Competent Authority under Section 60 of the Act and a State Competent Authority under Section 62.

The AMLCU supervises certain designated non-financial businesses and professions that are required to take measures to ensure their businesses aren't being used for money laundering and/or terrorist financing. There are multiple competent authorities under the Act as already set out in Table 1. The AMLCU is the supervisor by default where there is no existing regulator for a particular category of Designated Person in Ireland. As a result of being the supervisor by default, the cohorts supervised by the AMLCU are not fixed and may change from time to time e.g. FATF and the EU may decide that particular categories of non-financial businesses or professions are at greater risk of being used for ML/TF and should become obliged entities (Designated Persons). Alternatively, the Minister may prescribe additional categories of business based on the national AML/CFT risk assessment.

Currently, the AMLCU supervises a wide variety of Designated Persons including High Value Goods Dealers (car and boat dealers, jewellers, gold bullion dealers, antique dealers etc.), High Value Art Traders and Art Intermediaries, Trust or Company Service Providers (not supervised by the Central Bank or a designated accountancy body), Gambling Service Providers (retail bookmakers, online gambling, on-course and Private Members' Clubs at which gambling is carried on), Notaries (not otherwise supervised e.g.: who are not practising barristers or solicitors), and Tax Advisers and External Accountants not otherwise supervised.

As a Competent Authority, under Section 63 of the CJA 2010 as amended, the AMLCU is required to:

- 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 their obligations under the Act;
- Consider whether a Designated Person has been able to demonstrate that the requirements of the Act have been met;
- Report to the FIU and Revenue Commissioners any knowledge or suspicion that a Designated Person or any other person has been or is engaged in ML or TF;
- Adopt a risk-based approach to the exercise of its supervisory functions;
- Ensure the AMLCU team have relevant information on the domestic and international risks of ML and TF which affect the business categories it supervises;
- Base the frequency and intensity of onsite and offsite supervision on the profile of the Designated Persons it supervises and on the risks of ML and TF in the State;
- Review both periodically and when there are major events or developments in their management and operations, their assessment of ML and TF risk profile of

Designated Persons, including the risks of non-compliance with the provisions of the Act;

- Where a Designated Person operates establishments in the State which has head offices in another Member State or vice versa, take the necessary steps to cooperate with other Member States competent authorities in relation to the development and implementation of policies to counter ML and TF, to coordinate activities with them and to cooperate with them to ensure the effective supervision of such Designated Persons;
- Establish effective and reliable mechanisms to encourage the reporting of potential and actual breaches of the Act;
- Provide a communication channel for persons reporting potential and actual breaches of the Act (the AMLCU provides the following channel: antimoneylaundering@justice.ie);
- Include in each annual report published by the AMLCU an account of the activities that it has carried out in performing its functions during the year to which the annual report relates. The AMLCU's annual reports are available at www.amlcompliance.ie.

In addition to supervising those Designated Persons as already mentioned, other responsibilities of the AMLCU also include:

- Dealing with applications for authorisation (or renewals of authorisation) to carry on business as a Trust or Company Service Provider (TCSPs) where the TCSP is not supervised by either the Central Bank or a DAB. This involves conducting a fit and proper assessment of all principal officers and beneficial owners in the TCSP;
- Publishing annually in Iris Oifigiúil details of TCSPs authorised by the AMLCU;
- Registering Private Member Clubs (PMCs) where gambling activities are carried on. Conducting a fit and proper assessment of all relevant personnel and beneficial owners of PMCs where they are non-residents and ensuring An Garda Síochána (AGS) have vetted all relevant personnel and beneficial owners who are resident in the State prior to registration;
- Liaising with AGS on the initiation of enforcement proceedings against Designated Persons found to be in breach of their obligations under the Act;
- Communicating with Designated Persons under the supervision of the AMLCU through a variety of means (Note the AMLCU, inter alia, maintains a website www.amlcompliance.ie);
- Engaging on an ongoing basis with various stakeholders in the area of ML/TF. For example, the Department of Finance, other Government Departments, other supervisory bodies, FIU, Revenue, CEA, CRO, State agencies, international and supranational organisations.

3.6 Compliance monitoring

The monitoring process involves regulatory investigators of the AMLCU carrying out inspections of Designated Persons to ensure that they are meeting their obligations under the Act. Regulatory investigators in the AMLCU are appointed as 'authorised officers' by the Minister for Justice under Section 72 of the Act.

The purpose of an inspection by a regulatory investigator of the AMLCU is, inter alia, to:

- Establish the extent to which the business appears to be complying with its obligations under the Act and consider whether the business has been able, inter alia, to demonstrate that the requirements of the Act have been met;
- Review the business's customer list and record of transactions to assess whether the business has adopted a risk-based approach to ML/TF, that a documented Business Risk Assessment is prepared and that the business has risk assessed its customers and transactions appropriately;
- Assess the adequacy of anti-money laundering/terrorist financing policies and procedures, including, inter alia, examination and background of certain transactions, CDD, EDD in relation to PEPs, cases of heightened risk and high risk third countries, staff training and record keeping, that have been put in place by the business;
- Consider whether the business has made any suspicious transaction reports and whether it is registered on GoAML and ROS;
- Report to the State Competent Authority (i.e. senior management of the AMLCU) on the level of compliance by the business.

Regulatory investigators may conduct announced or unannounced inspections. As set out above, the AMLCU adopts a risk-based approach and the frequency of inspections of designated businesses varies.

In the case of announced inspections, the regulatory investigator contacts the Designated Person in advance to notify them of the time and date for the appointment and issues a formal inspection appointment letter. That letter, in addition to setting out the time and date for the inspection, will advise the Designated Person, inter alia, who is required to be in attendance and the level of documentation that should be available on the day of the inspection.

The inspection itself consists of a meeting between the Designated Person and the regulatory investigator during which the regulatory investigator will ask a series of questions relating to various sections of the Act. The inspection process also includes a review of the business's AML, CDD and transactional documentation. Once the regulatory investigator has completed their compliance inspection of the business, they submit a report to the Competent Authority (i.e. a senior official in the AMLCU) to consider the report findings and issue an 'inspection follow up' letter to the Designated Person. This letter will detail the findings and outcome of the inspection.

In some cases, the business will be directed to refrain from engaging in specific conduct and/or to take specific actions reasonably necessary to ensure compliance with the Act. This letter will also include any specific follow-on remedial actions to be completed by the Designated Person within a specified timeframe. Except in cases where there has been a serious breach that requires immediate action, a reasonable period of time will be allowed to take whatever action or actions are required to ensure compliance. After a direction is issued by the AMLCU, the regulatory investigator may decide to carry out an early follow-up inspection to assess compliance in practice, particularly on areas of concern identified during the initial inspection.

Under Section 80 of the Act, a person commits an offence where they obstruct or interfere with an 'authorised officer' in the exercise of their powers, or if they fail to comply with a requirement or request made by an 'authorised officer' under Section 77 of the Act. This could result in a liability, on summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both).

Further information regarding the inspection process specific to particular cohorts of Designated Persons can be found in the relevant chapter of this guide.

4 Overview of Obligations

4.1 When do your obligations apply?

The obligations required of those Designated Persons supervised by the AMLCU under the Act are set out in Part 4 of the Act. The obligations apply when any Designated Person, defined in Section 25 of the Act (previously set out in Chapter 3), is acting in the course of business carried out by that person and meets the definition for their specific business cohort.

Example: Notaries

Their definition as a Designated Person is:
Section *25 (1): 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).*

Section 24 (1)
"relevant independent legal professional" means a barrister, solicitor or notary who carries out any of the following services:
(a) the provision of assistance in the planning or execution of transactions for clients concerning any of the following:
(i) buying or selling land or business entities;
(ii) managing the money, securities or other assets of clients;
(iii) opening or managing bank, savings or securities accounts;
(iv) organising contributions necessary for the creation, operation or management of companies;
(v) creating, operating or managing trusts, companies or similar structures or arrangements;

(b) acting for or on behalf of clients in financial transactions or transactions relating to land;

In this instance, the obligations apply to notaries but only in relation to the carrying out of services set out in 24(1)(a) (i) to (v) and (b).

The obligations for each cohort of Designated Persons are detailed in the relevant chapters of this guide.

4.2 Key AML Obligations

4.2.1 Section 30A Business Risk Assessment

A Designated Person shall carry out 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. This exercise should be appropriately documented and take account of the money laundering and terrorist financing risks involved in carrying out the business of a Designated Person.

This exercise should be repeated yearly, record the name of the author of the exercise and the management level at which it has been approved. A record of the Business Risk Assessments (both current and historical) must be made available to the relevant Competent Authority upon request.

In preparing your Business Risk Assessment, you should consider at a minimum, the risk factors listed under Section 30A of the Act as follows:

- The type of customer;
- The products and services provided by the Designated Person;
- The countries or geographical areas in which the Designated Person operates;
- The type of transactions carried out by the Designated Person;
- The delivery channels used by the Designated Person;
- Other prescribed additional risk factors.

A Business Risk Assessment is a tool that assists in identifying where there is a risk in your business that could be exploited for money laundering and terrorist financing purposes. **The assessment exercise should be an accurate appraisal of the risks specific to your business as a Designated Person.** The exercise will allow you to assess the risks identified and to put in place appropriate internal controls to manage and mitigate these risks to an acceptable level.

It is important to note that for terrorist financing to occur, the source of the funds (SOF) is irrelevant, i.e. the funds can be from a legitimate or illegitimate source, rather it is the intended usage of the funds that is important, e.g. funds raised through charitable donations then used for financing of terrorism.

To conduct a Business Risk Assessment that adequately appraises the risks of ML/TF to their business, the Designated Person requires an understanding of what money laundering is.

The below box provides an overview of the stages of money laundering and terrorist financing.

The stages of the money laundering process:

1. **Placement**
   Placing proceeds of crime money into the legitimate financial system.

2. **Layering**
   A technique that disguises the source of money and the ultimate beneficial owner by hiding them behind “layers” of transactions.

3. **Integration**
   The return of the money from seemingly legitimate sources to be used by the criminal.

The stages of Terrorist Financing:

1. **Raising/collecting funds**

2. **Moving funds**

3. **Using funds**

4.2.2 Customer Risk Assessment

A Designated Person shall identify and assess the risk of money laundering and terrorist financing in relation *to each relevant customer or transaction concerned.*

In accordance with Section 30B of the Act, a Designated Person shall identify and assess the risk of money laundering and terrorist financing in relation to each customer or transaction concerned, having regard to at least the following:

- The relevant Business Risk Assessment;
- The matters specified in Section 30A(2);
- Any relevant risk variables, including at least the following:
    - The purpose of an account or relationship;
    - The level of assets to be deposited by a customer or the size of transactions undertaken;
    - The regularity of transactions or duration of the business relationship;
    - Any additional prescribed risk variable;
- The presence of any factor specified in Schedule 3 or prescribed under Section 34A suggesting potentially lower risk;
- The presence of any factor specified in Schedule 4; and
- Any additional prescribed factor suggesting potentially higher risk.

The Customer Risk Assessment should result in each customer having their own individual risk assessment rating assigned to them e.g. low, low-medium, medium, medium-high or high risk. *Knowing your customers (KYC) and rating them in this fashion mitigates against the risk of money laundering and terrorist financing.*

A Customer Risk Assessment is a tool that aids you in identifying where there is a risk that a particular client could exploit your products or services for money laundering and terrorist financing. This tool allows you to assess the identified risks so that you can determine the level of Customer Due Diligence to apply to the customer:

- Simplified Due Diligence;
- Standard Due Diligence;
- Enhanced Due Diligence.

The factors outlined in the business risk assessment may be used for the Customer Risk Assessment.

Schedule 3 (Non-exhaustive list of factors suggesting potentially lower risk) and **Schedule 4** (Non-exhaustive list of factors suggesting potentially higher risk) of the Act may be consulted to assist you in identifying and assessing the risks.

4.2.3 Customer Due Diligence

Customer Due Diligence (CDD) is a key part of the anti-money laundering requirements for Designated Persons to comply with under the Act. CDD refers to the range of measures used by Designated Persons to:

(i) identify and verify the identity of the customer;

(ii) to identify and verify the identity of the beneficial owner if not the customer;

(iii) obtaining information on the purpose and intended nature of the business relationship;

(iv) conducting ongoing monitoring including scrutinising transactions carried out during the business relationship.

The purpose of these measures is to know and understand a customer's identity and intentions so that the money laundering and terrorist financing risks associated with this customer are managed as appropriate. *Know your customer.*

Sections 33 to 39 of the Act provide the CDD measures that a Designated Person must take in order to comply with obligations in respect of identifying and verifying customers, persons purporting to act on behalf of customers and beneficial owners.

Evidence of identification and verification of the customer's identity is based on documents and information that the Designated Person has reasonable grounds to rely on. For instance, documents from a government source or any prescribed class of documents. You should set out in your policies and procedures what level of documentation or information you are willing to accept and the circumstances under which you are willing to accept them in order to identify and verify the identity of a customer.

You must keep these documents on file and make them available for examination by regulatory investigators of the Anti-Money Laundering Compliance Unit (AMLCU) at all AML compliance inspections.

Requirements for and benefits of effective KYC:

1. **Collect Basic Information**: Names, address, date of birth, SOF/SOW, etc.;
2. **Verify Customer Information**: Collect appropriate up-to-date documentation to verify information collected;
3. **Assign a risk rating to your customer:** Effective KYC measures allow you to rate the riskiness of your customer and to decide whether more stringent AML/CFT measures are required or whether you should continue the business relationship;
4. **Ongoing review:** Effective KYC requires regular review of information held on customers to ensure it is up-to-date and accurate. This will assist you in identifying changes in behaviour, facilitate accurate risk rating of your customers and ultimately help you to *protect your business and brand.*

4.2.4 Registers of Beneficial Ownership

Prior to the establishment of a business relationship with a customer that is a relevant entity, a Designated Person shall check that information concerning the beneficial ownership of the customer is entered in the relevant central Register.

Where the beneficial owner recorded in the RBO is the senior managing official, a Designated Person shall take the necessary measures to verify the identity of that person and shall keep records of the actions taken to verify the person's identity including any difficulties encountered in the verification process.

Checking Registers of Beneficial Ownership

- The procedures for accessing Central Register of Beneficial Ownership of Companies and Industrial and Provident Societies (RBO) data and purchasing RBO Reports are set out in the FAQ section of the RBO website: www.rbo.gov.ie
- The procedures for accessing Central Register of Beneficial Ownership of Trusts (CRBOT) data is available on Revenue.ie: https://www.revenue.ie/en/crbot/inspecting-the-crbot/index.aspx
- The procedures for accessing the Beneficial Ownership Register data are set out on the Central Bank of Ireland Website: https://www.centralbank.ie/regulation/anti-money-laundering-and-countering-the-financing-of-terrorism/beneficial-ownership-register/access-the-register

4.2.5 Ongoing Monitoring

Under Section 35(3) of the Act, 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.

In its simplest terms, monitoring your customer activity and transactions is for the purpose of identifying unusual transactions or customer behaviour that may be linked to money laundering or terrorist financing activity.

Under Section 36 of the Act, and in accordance with a Designated Person's own policies and procedures, they shall 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. Where necessary, additional Customer Due Diligence may be required from the customer by the Designated Person before proceeding with a transaction. These transactions may also require the Designated Person to submit a Suspicious Transaction Report (STR) to both the Financial Investigation Unit (FIU) and the Revenue Commissioners.

Fundamental to a good monitoring system is obtaining and keeping current customer and transaction information. Once this system is in place and operational, the task of identifying unusual transactions is made easier.

Ongoing monitoring

A good monitoring system should be capable of:

- Highlighting unusual transactions or customer behaviour for further examination;
- Generating reports in relation to such transactions or behaviour for review;
- Ensuring that appropriate action is taken on the findings of any further examination that may include making a suspicious transaction report.

Consider:

- Does the customer perform transactions that involve virtual assets (e.g., Bitcoin or other similar products) or involve other methods of payment facilitating anonymity (prepay cards etc.)?
- Does the transaction make commercial sense?
- Does the transaction seem reasonable based on your knowledge of your customer?
- Is the transaction overly complex or make use of multiple different professionals at different stage?
- Does a charitable transaction make sense from the perspective of the charitable aims?
- Does it appear that assets are being bought and sold in quick succession? ('flipped');
- Is the transaction linked to parties that appear to be anonymous or using nominee arrangements?
- Are there frequent changes in Senior Management or UBO?

As part of the required ongoing monitoring process the Designated Person must ensure that all documents, data and information obtained for the purposes of applying Customer Due Diligence are kept up-to-date. Periodic reviews should be undertaken to identify instances where updated documents are required.

It may also be necessary to reapply or update current information where a transaction is not consistent with the Designated Persons knowledge of the customer and the normal transaction pattern.

Please note there are additional requirements for enhanced Customer Due Diligence for Politically Exposed Persons (PEPs).

4.2.6 Enhanced Customer Due Diligence for Politically Exposed Persons (PEPs)

(Please refer to Section 37 of the Act for full details of these requirements.)

Section 37 provides that a Designated Person must take steps to determine whether a customer or a beneficial owner is a "politically exposed person", an "immediate family member" or a "close associate" of a politically exposed person.

A Designated Person should document their steps, such as open source searches, to meet their obligations under Section 37 of the Act. These records should be available for review by an AMLCU regulatory investigator during an inspection or where requested to do so by a Competent Authority.

Where a Designated Person determines that a customer is a politically exposed person, immediate family member or a close associate of a political exposed person they must adhere to the requirements as set out under Section 37 (4) of the Act. This includes obtaining approval from senior management to initiate or to continue a business relationship with the customer, determine the source of wealth and of funds, and apply enhanced monitoring of the business relationship with the customers.

Section 37 (10) Defines a Politically Exposed Person:
"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 any 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 or supervisory body of a state-owned enterprise;
(c) any individual performing a prescribed function;

"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 or of a similar legislative body;
(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;
(e) an ambassador, chargé d'affairs or high-ranking officer in the armed forces;
(f) a director, deputy director or member of the board of, or person performing the equivalent function in relation to, an international organisation.

Subparagraph (10) of Section 37 also defines the meaning of a ‘‘close associate’’ and ‘‘an immediate family member’’ of a Politically Exposed Person.

4.2.7 Suspicious Transaction Reporting

As a Designated Person you are required to report to the Financial Intelligence Unit (“FIU”) and the Revenue Commissioners if you know, suspect or have reasonable grounds to suspect, on the basis of information obtained in the course of carrying on your business that another person has been or is engaged in an offence of Money Laundering or Terrorist Financing.

As a Designated Person you are required to 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.

As a Designated Person you are also required to report transactions connected with high-risk third countries to the FIU and to the Revenue Commissioners.

Please refer to the Suspicious Transaction Report chapter (Chapter 10) of this guidance document and the AMLCU website at https://www.amlcompliance.ie/suspicious-transaction-reporting/.

4.2.8 Governance

Role of Senior Management/Board
The role of senior management in an organisation is to ensure that it has effective oversight over the identification of risks to the business and to ensure that appropriate and effective controls are implemented to mitigate the risks.

This oversight includes decisions on the risk appetite of the business and whether to accept or maintain higher risk customer/transactions.

Policies and Procedures
A Designated Person shall adopt internal policies, controls and procedures in relation to their business to prevent and detect the commission of money laundering and terrorist financing.

This document should be reviewed yearly (or more frequently if required), and approved at an appropriate management level.

This document should specify the policies, controls and procedures for dealing with the factors listed under Section 54(3) of the Act. AML/CTF Policies, controls and procedures can also include a range of additional measures for the prevention and detection of money laundering.

Good Practices

- **When Researching your Documents:**
  - Link to controls in Business Risk assessment;
  - Review current legislation and Regulator guidance;
  - What is Sectoral best practice?
  - Review current documentation;
  - Get input from roles/departments affected by the policy/procedure.

- **When Drafting your Documents:**
  - Use plain language;
  - Break text into readable chunks;
  - Organise, display information and clarify where appropriate;
  - Use Forms, Tables, Diagrams, Screenshots, Flowcharts, Checklists.

- **Review the documentation on a regular basis or as necessary.**

4.2.9 Training

The importance and value of appropriate and comprehensive AML training and awareness cannot be overstated. It is considerably less likely that a Designated Person or their staff will detect or prevent the occurrence of money laundering and terrorist financing if they are not properly aware or trained on the matter.

Section 54 (6) of the Act requires Designated Persons to ensure that all persons involved in the conduct of the business are instructed on the law relating to money laundering, that training records are maintained and that appropriate ongoing training is provided.

It is essential that all staff involved in the conduct of the business are aware of and alert to the possibility of money laundering and terrorist financing. To achieve this, Designated Persons must implement adequate AML staff awareness and training programs tailored to the size of the business and proportionate to the level of risk associated with providing their business activities.

4.2.10 Records

Record keeping is another essential component of preventing and detecting the occurrence of money laundering and terrorist financing as it provides a valuable audit

trail evidencing the history of services and transactions carried out in relation to each customer.

Section 55 of the Act sets out the obligations of Designated Persons to retain records concerning customer identification and transactions as evidence of the work they have undertaken in complying with their obligations under the Act.

In addition to CDD records and a history of services, Designated Persons are required under Section 55 to retain such other records necessary to evidence their compliance with the provisions of the Act in relation to internal systems, compliance management and training.

As required under Section 55(4) of the Act all records relating to the history of services and transactions carried out shall be retained for a period of not less than 5 years.

4.2.11 Review/Audit

It is best practice to review the implementation of the policies and procedures at an appropriate interval to ensure that they are applied correctly and effectively. Part of this review process should include a sampling of customer records to ensure, for example, that CDD obligations have been met, an STR has been filed where appropriate and that policies and procedures have been adhered to.

This is a good indication to you of how well training has been received and whether additional/refresher training is required. The review and audit process is also a good opportunity to provide AML/CTF training to staff.

There are some recommended good practices when conducting a review of your processes:

- Have end-users test the procedure for gaps in process;
- Content - What does the control achieve?
    - Identify risk;
    - Prevent risk;
    - Mitigate/Correct risk;
- Effectiveness:
    - Does it reduce to acceptable level or prevent a risk occurring?
    - Review of incidents/near misses;
- Formal review and signoff;
- Reviewed and signed off at an appropriate level.

4.2.12 Overview of a Designated Person's obligations under the Act

Table 2: Overview of a Designated Person's obligations under the Act

Section	Obligation on the Designated Person	Offence
Section 30A	Documented Risk Assessment document - identify and assess the risks of money laundering and terrorist financing in relation to the business	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).
Section 30B	Assessment of risk in relation to a customer or transaction in determining the measures to be applied in relation to Customer Due Diligence	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).
Section 33/33A/34A	Customer Due Diligence (CDD) - Identification and verification of customers and beneficial owners. Timing of CDD (prior to commencing relationship or carrying out transaction/service). Electronic Money Derogation provisions (where applicable.)	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).
Section 35	Special measures applying to business relationships.	Except as provided by section 36, a Designated Person who fails to comply with this section commits an offence and is liable—

Section	Obligation on the Designated Person	Offence
		(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).
Section 36A	Examination of background and purpose of certain transactions	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).
Section 37	Enhanced CDD — politically exposed persons.	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).
Section 38A	Enhanced CDD for high risk third countries	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).
Section 39	Enhanced CDD in cases of heightened risk	A Designated Person who fails to comply with this section commits an offence and is liable—

Section	Obligation on the Designated Person	Offence
		(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).
Section 40	Reliance on other persons to carry out CDD	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.
Section 42 & Section 49	Requirement for Designated Persons and related persons to report suspicious transactions and not to tip off or make a disclosure that could prejudice an investigation	s.42: 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). s.49: 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).
Section 54	Internal policies and procedures and training	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

Section	Obligation on the Designated Person	Offence
		(b) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).
Section 55	Keeping of records by Designated Persons.	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).

5 Risk Assessment

5.1 Obligations in respect of Business and Customer Risk Assessments

The obligations required of those Designated Persons supervised by the AMLCU are set out in Part 4 of the Act.

Section 30A outlines the requirements when performing a Business Risk Assessment:

- Used to identify and implement ML/TF controls;
- Used to develop AML/CTF Policies and Procedures;
- Used to develop staff training.

Section 30B outlines the requirements for a Customer or Transaction Risk Assessment:

- Part of Customer Due Diligence (CDD) and ongoing monitoring;
- Determines whether simplified, standard or enhanced CDD is required, and level of ongoing monitoring applied.

The Act takes a risk-based approach to identify and mitigate the risks of money laundering (ML) and terrorist financing (TF) occurring in your business.

Each business will have specific risks arising from the goods and/or services it offers. It is important that businesses take appropriate steps to identify, understand, assess and mitigate the risks of ML and TF occurring in their business.

The Financial Action Task Force (FATF) recommend a risk-based approach as a best practice to:

- Combat Money Laundering and Terrorist Financing (ML/TF);
- Identify and implement Anti Money Laundering and Countering Terrorist Financing controls.

A risk-based approach helps you to:

- Recognise the existence of risk(s);
- Undertake an assessment of the risk(s);
- Develop strategies to manage and mitigate the identified risks.

Such a risk-based approach is required of Designated Persons by Sections 30A and 30B of the Act when applying their AML/TF compliance measures.

5.2 Risk Management

5.2.1 What is Risk?

There are many definitions of risk, however the European Commission defines risk as:

Risk Definition:

'Risk' = the ability of a threat to exploit a vulnerability of a sector.
'Threat': intent + capability.
'Vulnerability': a weakness which can be exploited.

Essentially a risk is any activity or transaction that could be used to exploit your business to legitimise the proceeds of crime including tax evasion or facilitate the funding of terrorist activities.

5.2.2 Risk Management

Risk management is the identification, evaluation, and prioritisation of risks.

Identifying, assessing, and understanding ML/TF risks is an essential part of the identification and implementation of policies, procedures, training and other measures to mitigate ML/TF risks.

5.2.3 Risk Management Process

The key steps in the risk management process:

1. **Risk identification:**

This is an exercise to identify and document the key risks from various sources.

2. **Risk analysis:**

This involves examining how the business may be impacted by identified risks and the likelihood of that risk occurring.

3. **Risk Evaluation:**

This is scoring the identified risks using your risk criteria to prioritise them and select strategies to treat the identified risk.

4. **Risk Treatment strategies:**

This involves identifying controls or actions that can treat the identified risk. This includes:

a) Prevention or avoidance;
b) Mitigation or reduction:
    1) Changing the likelihood of a risk occurring;
    2) Changing the consequence of a risk occurring;
c) Acceptance/contingency (for lower risks);
d) Transfer/share the risk.
e) Retain the risk by informed decision (for higher risks)

5. **Monitor and Review:**

This involves the monitoring of the controls/actions in place and assessing their effectiveness in treating or managing the risks.

5.2.3.1 Risk identification – Stages of Money Laundering and Terrorist Financing

Where are the key areas to analyse and identify risk?

There are two important things to note:

- For money laundering to occur, the funds/assets involved must be the proceeds of criminal conduct e.g. generated by drug dealing, theft, trafficking, fraud, embezzlement, bribery, tax evasion etc.

- For terrorist financing to occur, the source of funds/assets is irrelevant, *i.e. the funds can be from a legitimate or illegitimate source*[4].

Stages of ML and TF:

Consideration of all stages of ML

- Placement.
- Layering.
- Integration.

Consideration of all stages of TF

- Raising / collecting funds.
- Moving funds.
- Using funds.

5.2.3.1.1 Placement

Placement is the first stage of money laundering and is where the criminal proceeds are introduced to the legitimate financial system.

Non exhaustive examples of placement:

- Using legitimate cash based businesses as fronts;
- Unusual income;
- Unusual rise in income;
- Dummy invoices;
- Use of Trusts, Personal Assets holding Vehicles, nominee shareholders and intermediaries to disguise the beneficial owner;
- Undue secrecy and reluctance to meet face to face or to provide adequate CDD documentation;
- Legal structure/names or ownership changes frequently or inexplicably.
- Use of unnecessarily complex organisational or transactional structures to disguise the beneficial owner or source of funds:
    - Shell/Shelf companies;
    - Use of tax havens that may have greater secrecy;
    - Transactions through high risk third countries with weaker AML controls;

[4] Central Bank - Anti-Money Laundering Explained https://www.centralbank.ie/regulation/anti-money-laundering-and-countering-the-financing-of-terrorism

    - Transactions using methods that favour anonymity such as:
        - Cryptocurrencies;
        - Certain prepaid debit/credit cards/gift cards;
        - Significant amounts of cash of unusually high denomination (€200/€500 notes);
    - Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected;
- Transactions that do not make economic sense:
    - payment by unrelated third parties;
    - lots of smaller transactions under the thresholds to avoid triggering AML reporting;
    - Transactions in which funds/assets are withdrawn immediately after being deposited;
    - Transactions involving circular flows where the funds/assets are transferred between multiple accounts and are returned to the originating account (also connected to use of tax havens and high risk third countries);
- Aborted transactions: Funds are lodged with a bank or legal/professional service provider (e.g. solicitor or accountant) for a proposed transaction, but are refunded after a short period to appear to have come from a reputable source;
- Selling/purchasing an asset for an underestimated or overestimated price.

5.2.3.1.2 Layering

Layering is the second stage of money laundering and usually consist of multiple rounds of placement and integration to distance and disguise the funds/assets from the source.

5.2.3.1.3 Integration

Integration is the third stage of money laundering where the funds/assets are extracted from the financial system as seemingly legitimate funds, for example:

- Purchases of businesses or properties (sometimes for an underestimated or overestimated price);
- Purchases of lifestyle/luxury goods: Art, jewellery or high end cars. These can also be used by criminals as “currency” for furthering their criminal activity;
- Loans to directors or shareholders that are not repaid.

5.2.3.2 Risk analysis

A risk can be summarised using a risk statement/definition:

Due to [***vulnerability***] there is a risk that [***threat***] will occur resulting in a [***consequence/impact***].

Example:

Due to **the use of cryptocurrency**, there is a **risk** that **anonymous payments could be made from proceeds of crime** resulting in the **placement of money acquiring legitimate products or services.**

A risk statement can be analysed to produce a risk score to enable the prioritisation of risk.

Two common ways to score risk are:

- Score the "Likelihood" of the risk occurring and the "Impact/Consequence" of the risk.
- Score the "Threat/vulnerability and the "Impact/Consequence" of the risk.

For the purposes of this example, the "Likelihood" and "Impact/Consequence" model are used.

Example (for illustrative purposes only):

See *Table 3 - Likelihood and Impact/Consequence Matrix* for the scoring guide.

1. **Consider the likelihood of the risk occurring.**
   The likelihood of cryptocurrency being used as a form of payment in a transaction is rare but increasing annually.
2. **Consider the impact of the risk occurring**
   As cryptocurrency transactions are anonymous, mostly unregulated and can be associated with criminal activity; there is a catastrophic impact associated these types of payments.

Note: It is the responsibility of each Designated Person to select the appropriate risk methodology to meet their requirements/situation, as well as to be able to demonstrate its suitability and effectiveness to the AMLCU.

5.2.3.3 Risk Evaluation

Risk evaluation is the process of prioritising the risks to determine their severity. This will allow your business to direct its resources effectively towards mitigating the identified risks.

Table 3: Likelihood and Impact/Consequence Matrix

Impact→ **Likelihood↓**	Negligible 1	Minor 2	Major 3	Catastrophic 4
Almost Certain 4	4	8	12	16
Likely 3	3	6	9	12
Unlikely 2	2	4	6	8
Rare 1	1	2	3	4

Example (for illustrative purposes only):

Taking the Risk Analysis values of “Rare” and “Catastrophic” and using the scores in the Likelihood and Impact/Consequence Matrix; the overall Risk Score associated with the use of cryptocurrencies is 4. This translates to a Risk Level of “MEDIUM – LOW” using *Table 4: Risk Score & Response/Treatment* below.

5.2.3.4 Risk Treatment

Risk treatment is the process of identifying and implementing appropriate controls to mitigate the identified risk to an acceptable level, based on the business's risk appetite.

The following table provides *an example* of how to treat the risk effectively.

Table 4: Risk Score & Response/Treatment

Risk Score*	Risk Level	Risk Response/Treatment
1-2	Lowly significant LOW	Depending on Risk Appetite Accept risk Monitor risk at least annually to ensure that risk does not increase
3-5	Moderately Significant MEDIUM – LOW	Depending on Risk Appetite Accept risk with contingency Monitor risk at least annually to ensure that risk does not increase
6-11	Significant MEDIUM – HIGH	Depending on Risk Appetite Action is required to treat risk within a short to medium timeframe Actively monitor risk and efficiency of treatment
12-16	Very Significant HIGH	Immediate action is required to treat risk within a short timeframe. Consider immediately ceasing activity giving rise to risk.

Typical actions taken to treat the risk:

- Prevent/Avoid the risk;
- Mitigate/Reduce the risk;
- Technical controls (technology);
- Organisational controls (manual process, policies, training);
- Share the risk;
- Outsource certain processes to expert third party. (Designated Person is still accountable and needs to ensure that the third party implements correctly);
- Retain/Accept the Risk. Used where risk level is low;
- Where higher risk cannot be avoided or controls cannot mitigate the risk below the acceptable risk level, an informed decision is required by senior management. May require contingency in the event of the risk occurring.

N.B.: Once the Risk Treatment has been applied, you should reassess the risk to ensure that it has been mitigated to a level considered by the Designated Person as acceptable.

Example (for illustrative purposes only):

There are two practical methods to treat the risk associated with the example use of crypto currencies:

1. Prevent/Avoid the risk by not accepting cryptocurrency payments.

2. Mitigate/Reduce the risk by implementing the following controls:
    a. Only accept payments through a regulated Virtual Asset Service Providers (VASP);
    b. Ensure that all Customer Due Diligence is collected:
        i. Ultimate beneficial owner is identified;
        ii. Verification of identity documentation is obtained;
        iii. Proof of source of wealth/funds is obtained.

5.2.4 Practical Application of Risk Management

The effective implementation of a Risk Management Process in any organisation benefits from input from staff and stakeholders at all levels.

5.3 Business Risk Assessment

A Designated Person shall carry out 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.

Your Business Risk Assessment should assess, at a minimum, the following risk factors:

- The type of customer that the Designated Person has;
- The products and services that the Designated Person provides;
- The countries or geographical areas in which the Designated Person operates;
- The type of transactions that the Designated Person carries out;
- The delivery channels that the Designated Person uses;
- Other prescribed additional risk factors.

The Business Risk Assessment must be approved by senior management, must be documented, and kept up-to-date. A record of the Business Risk Assessment must be made available on request to the relevant Competent Authority.

A Business Risk Assessment is a tool that assists you to identify where there is a risk that your business could be exploited for money laundering and terrorist financing. This tool allows you to assess the identified risks so that you can prioritise your controls to mitigate these risks to an acceptable level.

The Business Risk Assessment should document who conducted the assessment and have a revision date to demonstrate when it was last reviewed.

The controls identified in the Business Risk Assessment should be documented in the policies and procedures with appropriate staff training to inform them of the controls.

5.3.1 Risk Factors

Table 5: Examples of business risk factors

Risk Factor	Risk Considerations
Client	• Does the client or its beneficial owner(s) have attributes known to be frequently used by money launderers or terrorist financiers? • Undue client secrecy and/or unnecessarily complex ownership structures; • Cash intensive businesses; • Politically exposed person; • Third country national; • Persons on Financial Sanctions List; • Source of wealth and source of funds enquiries suggest that the money being used to purchase the asset is of criminal origins or otherwise cannot be explained.
Product and Service	• Do any of the products or services have attributes known to be used by money launderers or terrorist financiers? • Insolvency services; • Providing financial advice; • Providing tax advice; • Handling client money; • Managing client assets and financial accounts; • Investment business services.
Country or Geographic	• Are clients established in countries that are known to be used by money launderers or terrorist financiers? • Does the firm have a specific client-base or niche service outside the EU (or from any high-risk third countries?
Type of Transaction	• Transactions that involve virtual assets (e.g., Bitcoin or other similar products) or involve other methods of payment facilitating anonymity (prepay cards etc.)? • Transactions related to oil, arms, precious metals, tobacco products, cultural artefacts and other items of archaeological, historical, cultural and religious importance, or of rare or scientific value, as well as ivory and protected species; • Transaction using larger denominations (€200/500 notes) or notes have attributes suggesting it was physically “stashed” or acquired by criminal means (i.e. bad condition: stains and smell from improper storage, or dyes suggesting robbery).
Delivery Channel	• No face to face meetings; • Use of intermediaries/introducers.
Additional Risk Factors	• Sector specific practices or risk. • Individuals, entities or countries that are subject to restrictive measures, also referred to as sanctions[5].

[5] More recently, in response to the situation in Ukraine, the EU has agreed a number of sanctions packages comprising a range of measures. Information on sanctions in respect of the situation in Ukraine as well as other sanction measures in effect in Ireland is available on the website of the Department of Foreign Affairs. https://www.dfa.ie/our-role-policies/ireland-in-the-eu/eu-restrictive-measures/
All EU sanctions regulations have direct effect in all Member States of the EU, and, as such, are legally binding on all natural and legal persons in Ireland.

5.4 Customer and Transaction Risk Assessment

Section 30A of the Act requires Designated Persons to carry out a Business Risk Assessment and Section 30B requires Designated Persons to utilise risk assessments when applying Customer Due Diligence to its customer and transactions.

A Designated Person shall identify and assess the risk of money laundering and terrorist financing in relation to each customer or transaction concerned, having regard to at least the following:

- The relevant Business Risk Assessment;
- The matters specified in Section 30A. — (2);
- Any relevant risk variables, including at least the following:
  - The purpose of an account or relationship;
  - The level of assets to be deposited by a customer or the size of transactions undertaken;
  - The regularity of transactions or duration of the business relationship;
  - Any additional prescribed risk variable;
  - The presence of any factor specified in Schedule 3 or prescribed under Section 34A suggesting potentially lower risk;
  - The presence of any factor specified in Schedule 4; and
  - Any additional prescribed factor suggesting potentially higher risk.

Customers should have their own individual risk assessment rating assigned to them e.g. low, low-medium, medium, medium-high or high risk.

A customer or transaction risk assessment is a tool that assists you in identifying where there is a risk that a particular customer or transaction could exploit your products or services for money laundering and terrorist financing. This tool allows you to assess the identified risks so that you can determine the level of Customer Due Diligence to apply to the customer:

- Simplified Due Diligence,
- Standard Due Diligence,
- Enhanced Due Diligence.

The factors outlined in the Business Risk Assessment may be used for the customer or transaction risk assessment. A transaction risk assessment should be performed where there are new transactions or changes to existing transactions or where transactions are particularly large or unusual in their nature.

The customer and transaction risk assessment should be documented and explain the rationale for the level of due diligence and monitoring applied.

Schedule 3 (Non-exhaustive list of factors suggesting potentially lower risk) and Schedule 4 (Non-exhaustive list of factors suggesting potentially higher risk) of the Act may be consulted to assist you identify and assess the risk.

5.5 Other resources

National Risk Assessments

https://www.amlcompliance.ie/risk-assessments/

EU Supranational Risk Assessment

https://ec.europa.eu/info/files/supranational-risk-assessment-money-laundering-and-terrorist-financing-risks-affecting-union_en

Financial Action Task Force Guidance (FATF)

https://www.fatf-gafi.org/documents/documents/nationalmoneylaunderingandterroristfinancingriskassessment.html

6 Customer Due Diligence

6.1 Purpose of Customer Due Diligence

Customer Due Diligence (CDD) measures are a key part of the anti-money laundering requirements for Designated Persons to comply with under the Act. It refers to the range of measures used by Designated Persons to: identify and verify the identity of their customers; to identify and verify the identity of beneficial owners; obtaining information on the purpose and intended nature of the business relationship; conducting ongoing monitoring including scrutinising transactions carried out during the business relationship and; establishing the source of the funds where necessary.

The purpose of these measures is to know and understand a customer's identity and intentions so that the money laundering and terrorist financing risks associated with this customer can be properly managed.

They help to protect you and your business from being used for money laundering or terrorist financing.

FATF recommendation number 10[6] provides guidance as to what measures are required to properly apply CDD.

- You must identify and verify your customer;
- You must identify and verify the beneficial owner(s);
- You must understand the purpose and intended nature of the business relationship;
- You must conduct ongoing due diligence throughout the business relationship (requesting updated ID and proof of address documents when appropriate);
- You should review the transactions throughout the business relationship in order to identify where it veers from the norm or what you would expect from your customer that they are consistent with what you know of your customer;
- What is the *norm* for your customer, if the transactions stray from that then you should be revisiting CDD, and consider reviewing that transaction with your customer;
- A transaction outside the norm may prompt you to submit an STR.

CDD is an *ongoing* requirement throughout the life of a business relationship with a customer and is one of your best defences from being used for ML/TF.

[6] FATF Recommendations 2012.pdf (fatf-gafi.org)

6.2 Application of a Risk Assessment

The application of a risk assessment in order to determine the levels of Customer Due Diligence required under Sections 33 and 35 of the Act should be documented and retained on file in accordance with the Designated Person's own record keeping policies and procedures.

A Designated Person who fails to document a determination in accordance with a direction issued by the Minister for Justice commits an offence and is liable to a criminal prosecution.

The requirement to assess the risk of ML/TF in relation to a customer or transaction:

Section 30B (1) of the Act states:
"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."

6.3 Customer Due Diligence

Sections 33 to 39 of the Act set out the Customer Due Diligence/Enhanced Due Diligence measures which a Designated Person must take in order to comply with its obligations in respect of identifying and verifying the identity of:

- The customer;
- The beneficial owner(s);

- Any person acting on behalf of the customer or beneficial owner and;
- Any other information reasonably warranted by the risk of money laundering or terrorist financing on the intended purpose and nature of the business relationship.

Section 33 (1) of the Act requires Designated Persons to identify and verify customers and beneficial owner(s):

(a) prior to establishing a business relationship with the customer,
(b) prior to carrying out an occasional transaction for the customer,
(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 with the customer,
(iii) the type of service, transaction or product in respect of the service sought,
(iv) the purpose (or the customer's explanation of the purpose) of the service, transaction, product or service sought,
(v) the value of any transaction sought,
(vi) the source of funds for the 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
(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 or information that the person has previously obtained for the purpose of verifying the identity of the customer, 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 customer,
(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, or
(f) at any time where the Designated Person is obliged by virtue of any enactment or rule of law to contact a customer for the purposes of reviewing any relevant information relating to the beneficial owner connected with the customer.

The identification phase requires the gathering of information about the customers identity and verification of their identity. Under Section 33(2) of the Act the measures to be applied by a Designated Person include 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 include:

- *Documents from a Government source (whether or not a State Government source), or*
- *Any prescribed class of documents or any prescribed combination of classes of documents.*

As stated above, evidence of identification can take a number of forms and it is recommended that Designated Persons set out in the internal AML Policy Procedure manuals their own list of documents which they are prepared to accept in order to identify and verify the identity of their customers. For this reason, the AMLCU has not included definitive examples of the documents it considers would satisfy this specific AML requirement.

Note: The Public Services Card cannot be requested, or accepted, even when voluntarily offered, as a form of ID by a customer. The Public Services Card cannot be requested by any public or private body or person not included as a specified body in Schedule 5 of the Social Welfare Consolidation Act 2005 (as amended).

Where the customer is met face to face the Designated Person should have sight of the original documents used to identify and verify the identity of the customer. Appropriate copies of these documents should be recorded by the Designated Person and retained on file. These copies should be of high quality and available for examination upon request. Evidence of Customer Due Diligence (CDD) obtained may be kept in either paper or electronic format provided they are capable of being reproduced if required to do so. CDD documentation should be refreshed as required and should be in date for all transactions with your customer.

6.4 Enhanced Customer Due Diligence

Sections 35 to 39 set out the requirements for when and how Enhanced Customer Due Diligence (EDD) should be applied.

In certain situations you are required to carry out EDD. These situations will depend upon the nature of the relationship with the customer, the type of business conducted and the perceived ML/TF risks involved with doing business with the customer.

Examples of when these situations occur are:

- The customer is not physically present when you carry out identification checks;
- When you enter into a business relationship with a 'politically exposed person' – (please refer to the PEPs chapter (Chapter 7) of these guidelines);
- When you enter into a transaction with a person from a high risk third country identified by the EU;
- Any other situation that is considered a higher risk of money laundering or terrorist financing.

The EDD measures for customers who are not physically present when carrying out identification checks and other higher risk situations include:

- Obtaining further information to establish the customer's identity;
- Requesting that the documents provided as part of the CDD process be certified as true copies by an appropriate professional;
- Conducting open source checks to verify that the individual(s) concerned are who they claim to be;
- Requesting documentary evidence supporting a customer's source of wealth or source of funds being used for a particular transaction;
- Applying extra measures to check documents supplied by a credit or financial institution;
- Making sure that the first payment is made from an account that was opened with a credit institution in the customer's name;
- Establishing where funds have come from and what the purpose of the transaction is.

This is not an exhaustive list and you may apply a range of additional measures when applying enhanced Customer Due Diligence on customers in higher risk situations.

The enhanced Customer Due Diligence measures when you deal with a politically exposed person include:

- Establish the exact nature of the customers political connections that make them a potential PEP;
- Making sure that senior management approval is obtained and recorded before agreeing to establishing a new business relationship;
- Taking adequate measures to establish where the customers wealth and the funds involved in the business relationship come from;
- Carrying out stricter ongoing monitoring of the business relationship;
- Conducting regular open source checks on the individual to monitor if their political status changes or if they are associated with any negative media reporting.

Where a business relationship or transaction is identified as representing a higher risk, a Designated Person must apply measures to manage and mitigate the risks of money laundering or terrorist financing.

A business relationship or transaction shall be considered to present a higher degree of risk if a reasonable person taking account of factors highlighted in Section 30B(1) and/or the list of factors set out in Schedule 4 of the Act, indicating a potentially higher risk rating should be assigned, would determine that the business relationship or the transaction represents a higher risk of money laundering or terrorist financing.

6.5 Beneficial Ownership

Under the Act, Designated Persons are required to identify the beneficial owner(s) connected with the customer or service requested. This requires taking measures reasonably warranted by the risk of money laundering or terrorist financing in accordance with Section 33(2)(b) of the Act.

Section 33 (2)(b) of the Act requires Designated Persons to:

- Identify and verify any beneficial owner(s) connected with a customer or service provided to ensure the Designated Person has reasonable grounds to be satisfied that they know who are the beneficial owners;
- Understand the ownership and control structure of customers that are legal entities or legal arrangements;
- To take reasonable measures warranted by the risk of money laundering or terrorist financing to verify the beneficial owner's identity;
- Where the beneficial owner has been identified as a Senior Managing Official referred to in article 3(6)(a)(ii) of the Directive (EU) 2015/849 of The European parliament and of The Council of 20 May 2015, Designated Persons are required to take the necessary steps to verify the identity of that person and keep records of the actions taken to verify the person's identity including any difficulties encountered in the

The procedures to follow and the type of documentation to be relied upon by a Designated Person in establishing the beneficial ownership of a customer should be set out in the Designated Person's AML Policy and Procedures document. These internal controls should include the procedures to follow where it is not possible to identify a natural beneficial owner. In this scenario, the procedures should clearly set out how the Designated Person will manage this situation and the standard it will accept in order to establish a business relationship or provide the service requested.

For example, if a Designated Person or the customer is unable to identify a natural person beneficial owner of a customer, after they have exhausted all possible means to the satisfaction of the Designated Person; Senior Managing Officials, for example Director(s) or CEO, shall be deemed to be the beneficial owners.

In this situation, senior management approval should be obtained and a note of the decision taken should be maintained as part of the Customer Due Diligence records. This type of customer relationship could also be considered higher risk warranting more rigorous ongoing monitoring by the Designated Person.

The purpose of identifying the beneficial ownership of a customer is to identify those individuals that:

- have ultimate control (direct or indirect) over the customer;

- are ultimately the beneficiary of the services provided to the customer;
- are the owners of the wealth/funds used by the customer in particular transactions.

In the event that a Designated Person is unable to satisfy itself concerning the identity of the beneficial owner(s) of a customer, on the basis of the verification methods that it considers appropriate in line with its' own internal controls, no business relationship with the customer should be established nor any service supplied to the customer.

This event outlined above may also be considered suspicious, depending on the nature of the customer and the service requested the Designated Person should consider whether a suspicious transaction report to the FIU and to the Revenue Commissioners is appropriate.

6.6 Reliance on a Relevant Third Party to conduct CDD

Under Section 40(3) of the Act, a Designated Person may rely on a relevant third party to complete CDD obligations for the Designated Person's customers as required under Sections 33 and 35(1) of the Act.

The meaning of "relevant third party" is set out in Section 40 of the Act.

NOTE: Section 40(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.

Under Section 40(4)(a) and(b), Designated Persons may only rely on a relevant third party to undertake CDD on their behalf if there is a documented agreement in place between the Designated Person and the relevant third party provider outlining clear contractual terms in respect of the obligations of the third party to obtain and maintain the necessary records, and to provide the Designated Person with CDD documentation or information as requested and in a timely fashion.

A relevant third party may provide the following services:

- Section 33: Identification and verification of customers and beneficial owners.
- Section 35(1): Special measures applying to business relationships.

Note: A Designated Person may only rely on a relevant third party to carry out CDD measures required by section 33 and 35(1).

When entering into such an arrangement the Designated Person should take note of the following:

- The Designated Person, when relying on a relevant third party should document the specific services provided by the relevant third party;
- The documented arrangement must commit the relevant third party to applying appropriate controls to the provided services to prevent or mitigate the risk of Money Laundering/Terrorist Financing. This provision should ensure that the relevant third party applies controls equivalent to those that the Designated Person would implement if carrying out the CDD themselves;
- That the relevant third party provides the Designated Person with CDD documentation or information as requested and as soon as is practicable after a request from the Designated Person;
- The provision of the CDD documentation or information to the Designated Person upon termination or ending of the arrangement;
- It would also be expected that the Designated Person or their agents on their behalf would have a right to inspect the premises of the relevant third party to ensure compliance with the provisions of the documented agreement;
- The risk identified with reliance on the relevant third party and the mitigated controls implemented should be documented in the Designated Person's Business Risk Assessment;
- This document should be reviewed and approved at an appropriate management level;
- It is best practice to review the implementation of the reliance agreement at appropriate intervals to ensure that they are applied correctly and effectively. Part of this review process should include a sampling of customer records.

Examples of effectiveness and accuracy checks concerning a third party:

- Are all required documents/information collected and retained?
- Have CDD documentation/information been provided in a timely fashion when requested?
- Have AML/CFT controls been implemented?
- Are relevant third party staff aware of their obligations and received appropriate training?
- Review of suspicious incidents.

7 Politically Exposed Persons

7.1 Politically Exposed Persons - Introduction

The following guidance was issued by Department of Justice to all competent authorities on 20 January 2023.[7]

Section 37(12) of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (the 2010 Act), as inserted by the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2021, provides that:

> *The Minister [for Justice] may, with the consent of the Minister for Finance, issue guidelines to the competent authorities in respect of functions in the State that may be considered to be prominent public functions and each Competent Authority shall have regard to any such guidelines.*

These guidelines were issued to competent authorities pursuant to section 37(12). The 2010 Act (as amended) transposes Directive 2015/849 (as amended) ('the Directive').

The guidelines address the obligation under the Directive to issue lists indicating the functions which qualify as prominent public functions in the State.

The guidelines do not override any legal or regulatory requirements. They are subject in all cases to the 2010 Act. In the event of a conflict between these guidelines and the 2010 Act, the provisions of the 2010 Act prevail.

7.2 Legislative Provisions

Section 37 of the 2010 Act includes definitions for 'politically exposed person' and 'specified official':

> *"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 any 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 or supervisory body of a state-owned enterprise;*
>
> *(c) any individual performing a prescribed function*

[7] https://www.gov.ie/en/publication/c8d09-guidelines-under-section-3712-of-the-criminal-justice-money-laundering-and-terrorist-financing-act-2010/

"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 or of a similar legislative body;

(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;

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

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

7.3 General definition of 'prominent public function'

A 'prominent public function,' in respect of such functions within the State, and where not otherwise specified, shall be an office or other employment in a public body in respect of which the remuneration is not less than the lowest remuneration in relation to the position of Deputy Secretary General in the Civil Service.[8]

For the purposes of this definition, 'public body' shall not include courts.

[8] The pay scale for a Deputy Secretary is issued by the Department of Public Expenditure and Reform and is subject to change. The most up-to-date pay scale should be used for the purposes of identifying a person entrusted with a prominent public function. The current pay scale for a Deputy Secretary is set out in Department of Public Expenditure and Reform Circular 19/2022, available at https://www.gov.ie/en/circular/0d4cf-192022-february-2nd-and-october-1st-2022/

7.4 Application of provisions to roles in the State

Table 6: Application of provision to roles in the State

Provision	Application
'a member of the administrative, management or supervisory body of a state-owned enterprise'	'state-owned enterprise' is considered to be limited to commercial bodies and includes bodies listed on the 'Non-Financial Corporation Sector' or the 'Financial Corporation Sector' within the Register of Public Sector Bodies as published and updated by the Central Statistics Office
'a head of state, head of government, government minister or deputy or assistant government minister'	Includes: 1) The President 2) The Taoiseach 3) Government Ministers and Ministers of State
'a member of a parliament or of a similar legislative body'	Includes: 1) Members of Dáil Éireann 2) Members of Seanad Éireann
'a member of the governing body of a political party'	Members of the executive committee and any other executive offices (or equivalents) of any registered political party in the State which has registered under section 25 of the Electoral Act 1992 as amended.
'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'	Includes: 1) Judges of the Supreme Court
'a member of a court of auditors or of the board of a central bank'	Includes: 1) Members of the Commission of the Central Bank of Ireland
'an ambassador, chargé d'affairs or high-ranking officer in the armed forces'	Includes: 1) The most senior official of a foreign embassy in the State 2) Officials from the State's diplomatic corps who hold an equivalent position to (1) 3) The Chief of Staff and Deputy Chief of Staff of the Defence Forces
'a director, deputy director or member of the board of, or person performing the equivalent function in relation to, an international organisation'	'international organisation' refers to an organisation that is established by, or on the basis of, an agreement between two or more states. 'International organisation' refers to the organisation itself, and does not refer to an individual local office.

8 Sanctions

8.1 Sanctions

The AMLCU would like to remind all Designated Persons of their obligations in respect of all international financial sanctions. All EU sanctions regulations have direct effect in all Member States of the EU, and, as such, are legally binding on all natural and legal persons in Ireland. Designated Persons have an obligation to ensure that they are in full compliance with all measures, which are frequently updated.

The EU implements financial sanctions imposed by the UN. It does this through EU regulations, which have direct legal effect in Ireland and all EU Member States. The EU can also impose its own financial sanctions, sometimes referred to as 'EU autonomous' sanctions. These are also implemented through regulations that have direct effect in Ireland and EU Member States.

Once a person or entity is designated ('sanctioned') by the UN Sanctions Committees or set out on the EU lists, you as a Designated Person should:

- Refrain from getting involved in a business relationship or conducting any transactions with the sanctioned person or entity; and
- Submit a suspicious transaction report to An Garda Síochána and to the Revenue Commissioners

Notifications and additional information from the Anti-Money Laundering Compliance Unit in this regard can be found on the AMLCU website[9].

[9] See https://www.amlcompliance.ie/sanctions/

9 The AMLCU inspection process

9.1 Introduction

The AMLCU takes a risk-based approach to supervision of compliance. This section provides general information on the inspection process conduced by the AMLCU as part of its supervisory role as a Competent Authority.

9.2 Notification of Inspection

Where an announced inspection is being conducted, an Authorised Officer (Regulatory Investigator) from the AMLCU will issue a letter notifying the Designated Person of their intention to conduct a compliance inspection on the business. In this letter, the regulatory investigator will:

- Specify a date and time for the inspection;
- Highlight the obligations under review;
- Specify any records required for the inspection. For example: sale transaction records for a particular period, gross turnover of the business etc.

Please note that in some circumstances Designated Persons may be required to forward documents prior to the inspection (via a secure link). An example of this may be that where appropriate the regulatory investigator will require you to supply a list of your customers for them to review. They may select certain clients and ask that documentation relating to them (e.g. CDD, details of transactions or evidence of source of funds) be provided in advance of the inspection date or be available ‘on site’ on the day for inspection.

9.3 Day of the Inspection

On commencing the inspection, the regulatory investigator will give a brief overview of the AMLCU, outline the inspection process and identify the powers of a regulatory investigator as an ‘authorised officer’ under Section 77 of the Act.

Below is an outline of the main areas that the regulatory investigator will inspect (please refer to reference table below for further information):

- The Designated Person will be expected to be in a position to demonstrate to the regulatory investigator that it is fully compliant with the requirements prescribed by the Act.
- The regulatory investigator will examine and assess the anti-money laundering policies and procedures and the systems that are in place to manage and monitor compliance. These policies, controls and procedures should be documented.
- The regulatory investigator may also examine transaction records and related documents to check that the CDD and reporting of suspicious transactions measures are being properly applied and that required records are being maintained.

- The Designated Person will be expected to demonstrate that all relevant staff members are sufficiently trained with regard to the requirements of the Act. In particular, the ability to recognise and deal appropriately with suspicious activity.

Please Note: the legislation requires a risk-based approach and the onus is on the Designated Person to demonstrate through its records that it has complied with its obligations under the Act.

9.4 What type of records may be required for inspection?

Examples include:

- Anti-money laundering policies and procedures, risk assessments, AML documents/manuals, staff anti-money laundering training records/manuals etc.;
- Internal/external audits of compliance with internal anti-money laundering procedures and controls;
- Bank statements relating to relevant business accounts;
- Customer/transaction records;
- Documented and documentary evidence of source of funds checks, evidencing the source of the funding and the source of the cash itself e.g. bank statements to show cash withdrawal, explanation recorded for reason not paid by EFT or bank draft. The Designated Person must be able to record such an explanation that constitutes a reasonable explanation as to the source of the funds;
- Evidence of the checks made in line with CDD requirements;
- Generally, documented proof of the steps taken and copies of references and other material checked to confirm and verify customers' identity;
- Supporting records for the ongoing monitoring of CDD measures;
- Evidence of checks to show obligations relating to Politically Exposed Persons have been met, these can be evidenced by open source checks;
- Where there is some level of suspicion in relation to a transaction but a decision has been made not to submit an STR, it is recommended that the decision and reason for not submitting the STR be documented in writing. This can be presented to the regulatory investigator if they query a transaction.

9.5 Post Inspection

In the post inspection process:

- Regulatory investigators review inspection material and draft inspection reports. Additional information can be requested from the Designated Person to allow the officer to finalise the report.
- A report with findings and recommendations will be forwarded to the Competent Authority (senior management within the AMLCU) for consideration.

- The Competent Authority will assess the findings and recommendations to determine the level of compliance and what corrective actions are required, if any.

There are 3 levels of compliance:

- **Compliant:** The Competent Authority is satisfied the Designated Person has met all of their obligations under the Act;
- **Partially Compliant:** The Competent Authority is satisfied that the Designated Person is mostly compliant but there are some deficiencies. The Competent Authority will issue a findings letter with some recommendations to the Designated Person to bring them to a compliant status. A date by which these remedial actions should be completed will be set out in the letter;
- **Non-Compliant:** The Competent Authority has found that the Designated Person is failing to meet their obligations under the Act. The Competent Authority will issue Direction(s) (under Section 71 of the Act) to the Designated Person directing them to cease or refrain from engaging in certain actions until such time as certain remedial actions are complete, or to undertake specific remedial actions to bring themselves to compliant status. A deadline date by which these actions must be undertaken will be set out.

Section 71. of the Act –

(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 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.

9.6 Inspection Follow-up

Depending on the findings and directions/recommendations issued, there may be certain follow-up actions such as:

- Require a Designated Person to submit documentation by a set date to demonstrate that the findings and directions/recommendations have been correctly implemented.
- A follow-up inspection may be performed to investigate whether the findings and directions/recommendations have been properly implemented.
- In cases of persistent non-compliance and/or an egregious breach of the obligations, a case may be prepared and referred for prosecution.

This table sets out the relevant section of the Act, the obligation on the Designated Person and the evidence that the AMLCU would review to determine compliance by the Designated Person with their legal obligations.

Table 7: Overview of Obligations on Designated Persons

Section	Obligation on the Designated Person	Evidence to be reviewed	Offence
Section 30A	Documented Risk Assessment - identify and assess the risks of money laundering and terrorist financing in relation to the business	An appropriate documented 30A Business Risk Assessment is in place and reviewed and updated regularly. The risk assessment should include consideration of the risk factors in section 30A (1) (a) to (e). In addition the risk assessment should include consideration of Schedule 3 and 4 risk factors in the Business Risk Assessment and any other relevant risk factors. The risk assessment should include any relevant information in the National Risk Assessments (National Risk Assessments)[10]. There should be evidence of approval of the Business Risk	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).

[10] https://www.gov.ie/en/publication/e21f7b-national-risk-assessment-money-laundering-and-terrorist-financing/

Section	Obligation on the Designated Person	Evidence to be reviewed	Offence
		Assessment by senior management.	
Section 30B	Application of risk assessment in applying Customer Due Diligence to a customer or transaction.	There should be evidence of an application of risk assessment under s.30B in relation to the customer or transaction concerned. Sample transactions to be reviewed to see if this provision was applied appropriately.	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).
Section 33/33A/34A	Customer Due Diligence. Identification and verification of customers and beneficial owners. CDD undertaken prior to relationship or carrying out transaction/service Electronic Money Derogation	Sample records should illustrate appropriate CDD applied as appropriate. There should be a transaction tracking methodology in place that takes due account of the need to track given linked transactions. Whether CDD was applied prior to commencement or at what point of the relationship and justification for same should be available. Sample records where any electronic money derogations were applied to ensure the correct	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).

Section	Obligation on the Designated Person	Evidence to be reviewed	Offence
		application of derogations.	
Section 35	Special measures applying to business relationships.	Records demonstrating collection of 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.	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).
Section 36A	Examination of background and purpose of certain transactions	Evidence of examination of background and purpose of all complex or unusually large transactions and those which have no apparent economic or lawful purpose	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).]
Section 37	Enhanced Customer Due Diligence — politically exposed persons (PEPs)	Ascertain that the Designated Person has procedures for identifying domestic and foreign PEPs. Seek records demonstrating enhanced due diligence policies and procedures applied for PEPs. Review PEP CDD	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

Section	Obligation on the Designated Person	Evidence to be reviewed	Offence
		records including 30B risk assessments	exceeding 5 years (or both).
Section 38A	Enhanced CDD for high risk third countries	Where the business in Ireland is facilitating transactions by customers established or residing in high risk third countries, ensure enhanced due diligence has been carried out.	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).]
Section 39	Enhanced due diligence	Evidence that EDD is applied in all cases of heightened risk	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).
Section 40	Reliance on other persons to carry out CDD	Evidence that the provisions of s.40 were correctly applied	
Section 42 & Section 49	Requirement for Designated Persons and related persons to report suspicious transactions and not to tip off or make a disclosure that could	Copies of suspicious transactions reports submitted. Records evidencing suspicious activity reported to MLRO Documented rationale for where suspicious activity	s.42: 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

Section	Obligation on the Designated Person	Evidence to be reviewed	Offence
	prejudice an investigation	did not result in an STR and justification for same.	(b) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both). s.49: 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).
Section 54	Internal policies and procedures and training	Documented policies, controls and procedures dealing with all matters set out in s.54 (3) (a) to (l) of the Act Training documentation, records of communication and training completed demonstrating that persons involved in conduct of the Designated Persons business are: instructed on the law relating to money laundering and terrorist financing, and provided with ongoing training on identifying a transaction or other activity that may be related to money	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).]

Section	Obligation on the Designated Person	Evidence to be reviewed	Offence
		laundering or terrorist financing, and on how to proceed once such a transaction or activity is identified.	
Section 55	Keeping of records by Designated Persons.	Customer records including • CDD; Sample transactions; Evidence of monitoring of transactions and customers; Methods of payment; EDD (where applicable - PEPS etc.)	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 Suspicious Transaction Reports

10.1 Obligation to Report Suspicious Transactions

The Act sets out the obligations on Designated Persons in relation to suspicious transaction reporting.

Designated Persons are obliged to make suspicious transactions reports (STRs) to both the Financial Intelligence Unit (FIU) ***and*** the Revenue Commissioners *if they know, suspect, or have reasonable grounds to suspect that another person has been or is engaged in money laundering or terrorist financing.*

Section 42(1) of the Act states:

"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 FIU Ireland and the Revenue Commissioners that knowledge or suspicion of those reasonable grounds"

For the purposes of STRs, Section 41 the Act extends the obligations of a Designated Person to any person acting, or purporting to act on behalf of the Designated Person; employees, agents, directors or other officer of, any person engaged under a contract for services with the Designated Person.

10.2 When to Report

It is important for Designated Persons to be aware that there is no minimum monetary or transactional value for the reporting of a suspicious transaction to FIU or Revenue.

Where they have knowledge, suspicion, or reasonable grounds for suspicion of money laundering or terrorist financing the person should submit a report.

Where, following evaluation of information available, a decision is made not to submit a report, the Designated Person should keep written records detailing the reasoning for this decision.

Under Section 42(2) of the Act, a Designated Person must make a STR as soon as practicable after acquiring knowledge of, becoming suspicious, or acquiring reasonable grounds to suspect that the other person has or is engaged in money laundering or terrorist financing.

Designated Persons should be aware that "as soon as is practicable" requires them to make the report as soon as possible once they have acquired that knowledge or reasonable grounds or formed a suspicion.

This may occur before the transaction takes place, during it or after the transaction has taken place. Regardless of when the Designated Person acquires knowledge or reasonable grounds of, or develops suspicions of money laundering or terrorist financing they must submit an STR to the FIU and the Revenue Commissioners immediately.

A Designated Person must make a STR where that person has *knowledge, suspicion, or reasonable grounds* for suspicion of money laundering or terrorist financing arising from the person's normal course of business.

- *Knowledge:* This means to substantially *know* something.
- *Reasonable grounds:* The Designated Person should consider whether this is the behaviour of a reasonable person or someone engaged in money laundering or terrorist financing. Are there facts or circumstances known to the Designated Person from which a reasonable person engaged in their business would form a suspicion that another person was engaged in money laundering or terrorist financing?
- *Suspicion:* A suspicious transaction is a transaction that causes a Designated Person to think that there is the possibility or potential that the transaction may be related to money laundering or terrorist financing.

This is more than mere speculation or conjecture; whilst there does not have to be factual basis for the suspicion, the Designated Person should have a belief that extends beyond speculation.

10.3 Identifying suspicious transactions

The Act gives some guidance as to when a Designated Person may have cause to submit an STR.

Section 42 of the Act –
(4) "… 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 Persons 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 the 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"

A Designated Person should evaluate transactions in terms of what seems appropriate and is within normal practices in their line of business and based on their knowledge of their customer.

They should continually evaluate transactions taking into account relevant factors including but not limited to: their knowledge of the customer's business; whether the transactions are in keeping with normal industry practices; financial history; background; and behaviour. They should also be vigilant from beginning to end of any business relationship, be it a long term relationship, either continually active, sporadic in nature or a one-off transaction.

The Designated Person should know their customer. This will aid them in identifying suspicious transactions.

10.4 Submitting a Suspicious Transaction Report

Section 42(1) of the Act requires that suspicious transaction reports should be made by Designated Persons to *both* FIU Ireland and the Revenue Commissioners.

Both FIU Ireland and the Revenue Commissioners require that Designated Persons submit STRs electronically via online portals.

In order to make a report to the FIU Ireland Designated Persons must first register with an online application called Go AML at the following: https://fiu-ireland.ie/Home

Reports to Revenue must only be submitted by using Revenue's Online Service (ROS). To submit a report a Designated Person must be registered for ROS. Information can be found on www.revenue.ie.

Section 42(6) of the Act requires that STRs submitted include:

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 Persons knows, suspect 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 money laundering, or the funds the subject of the terrorist financing, as the case may be;*
d) *any other relevant information.*

Under Section 42(6A) of the Act, where FIU Ireland or Revenue request additional information from the Designated Person who makes the report, the Designated Person is required to respond to that request as soon as is practicable and to take all reasonable steps to provide any information specified in the request.

10.5 Tipping Off

Section 49 of the Act provides for two separate but related offences of 'tipping off' where the Designated Person knows or suspects, on the basis of information obtained in the course of carrying on business as a Designated Person:

1 That a STR has been or is required to be made, the Designated Person shall not make any disclosure likely to prejudice an investigation that may be conducted following the submission of the STR.
2 That an investigation may take place or is already being conducted into whether an offence of money laundering or terrorist financing has been committed, the Designated Person shall not make any disclosure likely to prejudice the investigation.

Section 49(1) of the Act states:

(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.

10.6 Training

Section 54(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.

Designated Persons must ensure that all persons involved in the conduct of their business are provided with *ongoing* training and advice around the identification and treatment of suspicious transactions and the measures/actions they should take. This should include the offence of 'Tipping Off'.

10.7 Policies and Procedures

Designated Persons must include details on monitoring of transactions and business relationships, and the reporting of suspicious transactions in their AML/CFT internal policies and procedures; this should include details on the offence of 'Tipping-off', the need for caution not to commit the offence and the penalties upon conviction for the offence.

Section 2

Additional Guidelines for Specific Designated Persons

11 Trust or Company Service Providers (TCSP)

11.1 Introduction

Trust or Company Service Providers are a category of Designated Persons whom are required take various measures and comply with the obligations on Designated Persons in the Act to ensure their business is not being used for money laundering or terrorist financing by criminals.

The particular activities that bring a person within the definition of a TCSP are outlined in Section 24 of the Act.

Section 24 of the Act provides a definition of a 'trust or company service provider' as follows:

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

- *(a) Forming companies and 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.*

NOTE: To perform any of the above activities without an authorisation from the Department of Justice is an offence under Section 87 of the Act. The offence can

be tried as either a summary or indictable matter with a maximum penalty of a prison sentence of not more than 5 years[11].

Details on how to apply for authorisation may be found on the AMLCU's website[12]. It should be noted that under Section 84 the following categories are specifically excluded from the definition of a TCSP[13] for the purpose of Chapter 9 of the Act:

- A member of a designated accountancy body;
- A barrister or solicitor;
- A credit institution or financial institution.

Therefore, an obligation to register and be authorised by the Minister for Justice does not generally apply to the above categories, however, there are circumstances in which an obligation to register can arise as a result of the particular business set up chosen by a person that is in the above categories.

Two examples that illustrate this includes:

1. Where a firm of solicitors sets up a separate limited company to provide Trust or Company Services, and

2. Where an accountancy firm is not a member of a designated accountancy body.

For further detail on the scenarios that give rise to a requirement to be authorised by the Minister for Justice, please have regard to the Memoranda of Understanding signed with the Law Society of Ireland and the Designated Accountancy bodies. Both are available on the AMLCU website.[14]

11.2 Why the TCSP sector is attractive to money launderers

The TCSP sector provides a wide range of services which can be used by criminals to set up companies and trusts which can be used to hide or move the proceeds of crime.

A Trust or Company Service Providers Risk Assessment was completed in 2022 by a subcommittee of the Anti-Money Laundering Steering Committee, chaired by the Department of Finance[15]. At section 2.1 of the Report some helpful theoretical examples of why a TCSP is vulnerable to money laundering are outlined, they are detailed in the box below.

[11] S.87(2)(b) https://revisedacts.lawreform.ie/eli/2010/act/6/revised/en/html#SEC87
[12] See https://www.amlcompliance.ie/trust-or-company-service-providers-tcsps/
[13] S.84 definitions https://revisedacts.lawreform.ie/eli/2010/act/6/revised/en/html#SEC84

[14] https://www.amlcompliance.ie/memoranda-of-understanding/

[15] https://www.amlcompliance.ie/wp-content/uploads/2022/03/TCSP-Risk-Assessment.pdf

Example 1: Illicit proceeds of crime are generated by criminals. The criminals ask a TCSP to set up a trust on their behalf and ask the TCSP to provide a trustee service. Illicitly generated funds are sent to the trust. The trust uses the funds to acquire shelf companies and to create a complex network of companies. The TCSP is asked to provide nominee shareholder services. Payments and transactions take place between the various companies. All of the companies' profits are received as profits by the trust. The TCSP as trustee then distributes the funds back to its client.

Example 2: The TCSP sets up a company for its client. The company established is a shell company. The TCSP is asked to provide nominee shareholder services to the shell company. The shell company is used to open a bank account. Criminals make payments from criminal proceeds to the bank account for fictitious services provided by the shell company.

Example 3: One or a number of TCSPs are appointed as nominee directors of multiple legal entities across multiple jurisdictions. Third party advisors instruct the TCSPs to make transfers between the legal entities. Due to the layers created, the transactions are complex and permit the criminal to distance illicitly generated funds from their source.

At paragraphs 3.1.7 & 3.2 the National Risk Assessment concluded that TCSP services are considered to present a Significant Inherent Risk for Money Laundering and a moderately significant risk for Terrorist Financing. These risks were measured based on the EU's Supranational Risk Assessment (SNRA) rating scale.

Trust or Service Company Providers should also be familiar with the factors tending to suggest high risk as listed in Schedule 4[16] of the Act.

11.3 Obligations of TCSPs

The Act imposes obligations on TCSPs as 'Designated Persons' to provide for the prevention of money laundering and terrorist financing. TCSPs must apply anti-money laundering controls in order to identify customers and/or beneficial owners; report suspicious transactions to the FIU and the Revenue Commissioners and have specific procedures in place for the prevention of money laundering and terrorist financing including record keeping and staff training.

[16] https://revisedacts.lawreform.ie/eli/2010/act/6/revised/en/html#SCHED4

Extracts from the Act on Obligations:
Sections 30A & 30B: Obligations regarding risk assessments for the business, clients and transactions.
Sections 33/33A/34A: Obligations in relation to Customer Due Diligence (CDD)
Section 35: Special measures applying to business relationships
Section 36A: Examination of the background and purpose for transactions.
Section 37: Enhanced CDD – politically exposed persons
Section 38A: Enhances CDD – high risk third countries.
Section 39: Enhanced CDD – in the cases of heightened risk
Sections 42 & 49: Obligations to report suspicious transactions and not tipping off or making a disclosure that could prejudice an investigation.
Section 54: Obligations regarding internal policies and procedures, and training.
Section 55: Record keeping obligations of Designated Persons

11.4 Risk-Based Approach

Businesses operating in the TCSP sector should adopt a risk-based approach to identify potential money laundering/terrorist financing risks involved in the business. This centres on having a good understanding of the money laundering and terrorist financing risks the business is exposed to as a TCSP and taking appropriate mitigating measures in accordance with the level of risk identified.

Section 30A of the Act requires Designated Persons to prepare a documented Business Risk Assessment to assist in identifying where there is a risk in the business that could be exploited for money laundering and terrorist financing purposes.

This assessment should be an accurate appraisal of the all risks specific to the business activities as a TCSP. The exercise will allow Designated Persons to assess the risks identified and to put in place appropriate internal controls to manage and mitigate these risks in such a way that they are aligned with the company's risk appetite. It should be noted that internal controls and mitigating actions should be tested for efficacy on a regular basis and form part of the regular review of the Business Risk Assessment. Measures include complying with the obligations under the Act.

The FATF Guidance for a Risk-Based Approach to Combating Money Laundering and Terrorist Financing – Trust and Company Service Providers[17] outlines the basic process for assessing risk. Section III of the document sets out specific advice guidance for the

[17] https://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Trust-Company-Service-Providers.pdf

TCSP sector. The FATF guidance was utilised in preparing the national Trust or Company Service Providers Risk Assessment which outlined specific risks in Ireland.

Table 8: Risk Factors in TCSP Sector below sets out specific risks posed by each service provided by the TCSP sector that Designated Persons in the TCSP sector should be mindful of when considering the risk of money laundering or terrorist financing that exists in their business.

Table 8: Risk Factors in TCSP Sector

TCSP Service	Specific Risks
Forming companies or other bodies corporate	• Intermediaries located outside of Ireland (often offering offshore services) seeking to set up companies. • Persons seeking to set up numerous companies in a short period of time. • Shelf companies – aged companies used to create a veneer of legitimacy. Sometimes companies are created simply to permit the owner to open an Irish bank account. • Use of nominees.
Acting as director/ secretary/ partner in partnership or arranging someone to act as same	• Jurisdiction – even without a location being a high risk jurisdiction they present a higher risk ML/TF due to the difficulty in verifying the beneficial owner and understanding the nuances of any relevant foreign law. • Nominee directors sometimes operate under the mistaken belief that they don't have the same duties as other company directors. See the judgment in ***Powers v. Greymountain Management Limited &Ors [2022] IEHC 599***[18] • Some TCSPs fail to sufficiently assess the risks of providing these services, as a consequence their risk mitigation measures can be lacking.
Providing a registered office, business address, correspondence or administrative address or other related services for a body corporate or partnership	• High risk service where it is offered on its own. The TCSP may have limited insight into the business, does not scrutinise the mail it forwards etc. • A non-Irish resident company or person availing of the service heightens risks. • The risks are not well understood or appreciated by all TCSPs. • The service is useful for the purposes of investment fraud and cross border tax evasion.

[18] https://www.courts.ie/acc/alfresco/0e0f6c20-b36f-4ade-828b-8e4645c1a583/2022_IEHC_599.pdf/pdf#view=fitH

TCSP Service	Specific Risks
	• Can be used in conjunction with a company formation service to create a reason for funds to be transferred into the State, despite their being no genuine underlying economic activity.
Acting, or arranging for another person to act, as a trustee of a trust	• A trust can be misused to obscure the beneficial ownership and source of funds. • Orphan structures. • A TCSP acting as trustee may not have proper oversight of the assets of the trust to prevent bank accounts or other elements of the trust's administration framework being misused for unrelated purposes.
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	• Nominee services provide a degree of confidentiality as to the actual owner. • there is a risk that this service has been requested as the beneficial owners do not wish their business relationships to be scrutinised.
Multiple services provided by the TCSP to a single client	• The risks of each of the individual services described above may be compounded if a TCSP provides multiple services to a client over a long period without any apparent commercial basis for the use of these services.

11.5 Risk Indicators for the TCSP sector

AML/CFT TCSP indicators (for customers and transactions) include:

Customer Risk

- Customer identified as being linked to or active in criminality (including regulatory criminality);
- Politically Exposes Persons (PEPs) including persons closely associated with PEPs;
- 3rd parties acting on behalf of unidentified customers;
- New customers based in, operating or banking from/in higher risk jurisdictions;
- Complex corporate structures, off shore companies, trusts etc.;
- Is the customer from a country subject to sanctions?

Transaction/Service and associated delivery channel risk

- Customer fails to comply fully with the Customer Due Diligence process;
- Any concern regarding information provided by the customer;
- Use of third parties for payment or receipt of payments;
- Transactions that appear (based on your knowledge/experience) have no obvious commercial reasoning;
- Transactions that appear (based on your knowledge/experience) to be overly complex or lack in economic sense;
- Customers who take an unusual interest in AML processes.

The AMLCU regularly hosts webinars and other outreach events which relevant parties may find beneficial and informative. Details of these, and other occasional significant updates, may be found on the AMLCU website www.amlcompliance.ie.

12 Private Members Clubs (PMCs)

12.1 Obligations for PMCs

Persons directing Private Members' Clubs (PMCs) where gambling activities are carried on are described as 'Designated Persons' under Section 25(1)(h) of the Act below.

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—

(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

Under the Act, a PMC at which gambling is carried on is a 'Designated Person.' A Designated Person is a category of business that must guard against its business being used for money laundering or terrorist financing purposes.

The Act places a number of obligations on Designated Persons, specifically for those persons directing private members' clubs where gambling activities are carried on. These include:

- To register with the Minister for Justice;
- To identify customers and/or beneficial owners;
- To conduct Customer Due Diligence checks;
- To have specific procedures in place for the prevention of money laundering and terrorist financing;
- These procedures relate to a Business Risk Assessment for the club and its members, recordkeeping, staff training and the maintenance of appropriate money laundering/terrorist financing procedures and controls;
- To report suspicions of money laundering or terrorist financing transactions to the FIU and the Revenue Commissioners.

12.2 Registration

(The most up to date details and information regarding registration can be found on the AMLCU website [www.amlcompliance.ie)](http://www.amlcompliance.ie).

Section 109(1) of the Act, places a requirement on Designated Persons directing private members' clubs where gambling activities are carried on to register with the Minister for Justice. They must do this in accordance with such procedures as may be prescribed or otherwise imposed by the Minister.

The following particulars are required for registration under Section 109(3):

(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.

When applying for registration, the Designated Person must submit an 'application to register form' to the AMLCU (the form can be found on the AMLCU website).

The application form should be accompanied by the following documents:

- **a.** A completed application form signed by the chairman or secretary of the club;
- **b.** A certificate of fitness and probity *for each* director/beneficial owner of the club;
- **c.** Two copies of the rules of the club;
- **d.** A list of the names and addresses of the officials and committee of management or governing body;
- **e.** A list of the names of the members of the club.

The application form requires you to provide the particulars of the PMC; address of the premises, contact details, phone number and email address, opening hours and objects of the club. The form also requires details of all individuals who effectively direct the PMC and/or details of all beneficial owners of the PMC.

In order to be able to register with the AMLCU, the PMC must submit the appropriate certificate(s) of fitness to the AMLCU along with the registration form.

Section 109A of the Act as amended sets out that an individual who effectively directs a PMC at which gambling is carried on, or is the beneficial owner of such an entity, must hold a certificate of fitness and probity.

Section 109B of Act requires that where the persons who direct the club or are the beneficial owners are *ordinarily resident in the State they are required to apply to An Garda Síochána* for the certificate of fitness. Where the persons who direct the club or are the beneficial owners are *ordinarily resident outside the State* they must apply to the *Minister from Justice (AMLCU)* for a certificate of fitness.

All individuals who effectively direct a private members club at which gambling activities are carried on, **or**, who are beneficial owners of a private members club at which gambling activities are carried on, *are legally required to hold a valid certificate of fitness*.

Under Section 109A(2) of the Act, a relevant individual who fails to comply with this requirement 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.

A certificate of fitness remains valid for 3 years. Persons that effectively direct or are the beneficial owners of such clubs are required to reapply to An Garda Síochána or the Minister for Justice for a certificate of fitness before the end of this period.

The Minister may publish the register in written, electronic or other form and the particulars entered in the register may be removed from the register where the person ceases to be a Designated Person pursuant to the Act.

The register is published on the Registers page of the AMLCU website here: https://www.amlcompliance.ie/registers/

11.3 Who are PMC customers?

All persons who engage in gambling activities in a private members' club will be members of that club.

Throughout the Act reference is made to "a customer". In the context of a private members' club, a member who engages ***in any transaction*** is automatically a customer for the purposes of the Act.

In the context of a private members club at which gambling activities are carried on a ***"transaction"*** means:

"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 club by a customer of the club"

A PMC has a business relationship with its customers and in that context should identify and verify the identity of ***all members***, as well as carrying out Customer Due Diligence prior to ***occasional transactions*** and Customer Due Diligence or enhanced Customer Due Diligence as required in the context of all obligations under Sections 33-39 of the Act.

In the case of a PMC at which gambling is carried on, an ***occasional transaction*** is when the amount (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.***

Designated Persons should monitor such transactions with customers from the date of the most recent transaction in order to identify customers who may be attempting to split large transactions into several smaller less conspicuous amounts.

If a Club recognises that two or more transactions have totalled more than €2,000 then the CDD obligations should be applied to that member.

11.4 Customer Due Diligence

Customer Due Diligence (CDD) is a key part of the anti-money laundering requirements for Designated Persons to comply with under the Act. CDD refers to the range of measures used by Designated Persons to:

(i) Identify and verify the identity of the customer;
(ii) To identify and verify the identity of the beneficial owner if not the customer;
(iii) Obtaining information on the purpose and intended nature of the business relationship;
(iv) Conducting ongoing monitoring including scrutinising transactions carried out during the business relationship;
(v) Establishing the source of the funds where necessary.

The purpose of these measures is to know and understand a customer's identity and intentions so that the money laundering and terrorist financing risks associated with this customer are managed as appropriate. *Know your customer*.

Identification and verification measures must be applied by a PMC at the following times:

a) Prior to establishing a business relationship (Section 33(1)(a)) which means CDD must be applied whenever a club takes on a new member;
b) Prior to carrying out a transaction of €2,000 or more;
c) Prior to carrying out any service if the Designated Person has reasonable grounds to believe that there is a real risk or suspicion of money laundering or terrorist financing (Section 33(1)(c));
d) Where there are doubts about the veracity or adequacy of previously obtained customer identification information (Section 33(1)(d));
e) On an ongoing basis and at appropriate times to existing customers on a risk-sensitive basis.

11.4.1 What measures are to be taken in establishing identity?

Evidence of identification and verification of the customer's identity is based on documents and information that the Designated Person has reasonable grounds to be relied upon, for instance, documents from a government source or any prescribed class of documents.

A Designated Person should set out in their AML policies and procedures the level of documentation or information they are willing to accept and the circumstances under which they are willing to accept them in order to identify and verify the identity of their customer.

For new customers, satisfactory identification documentation must be obtained. The verification of their identity is required and it should normally be obtained immediately.

Verification of a customer's identity is required in all cases before a customer or the club carries out a transaction that:

1. exceeds the threshold of €2,000 (whether in one transaction or in a series of transactions that appear to be linked), or
2. if transactions raise suspicions in any other circumstance.

If verification cannot be undertaken *immediately* the following applies:

Although verification of a customer's identity should be undertaken when membership is first taken out (before a business relationship commences), Section 33(5) of the Act provides for circumstances where the requirement to do so might interrupt the normal flow of business, *and the transaction(s) is for an amount less than €2,000.*

Sections 33 to 39 of the Act provides the CDD measures that a Designated Person must take in order to comply with obligations in respect of identifying and verifying customers, persons purporting to act on behalf of customers and beneficial owners.

Where the PMC has assessed a customer and made a determination that there is no real risk that the customer concerned, or the service being sought, is for the purpose of money laundering or terrorist financing, the Act permits the verification to be undertaken "during the establishment of the business relationship". In such cases the Designated Person must verify the identity of the customer or beneficial owner *as soon as practicable.*

It is important for the Designated Person to note that identification and verification must take place in all instances where the customer or the club carries out a transaction(s) that exceed €2,000 or if the transaction raises suspicions.

11.5 What might constitute suspicious activity?

Designated Persons are required to pay special attention to any activity which they regard as particularly likely, by its nature, to be related to money laundering or terrorist financing and in particular complex or unusually large transactions and all unusual patterns of transactions. It should be apparent if a customer behaves in an unusual manner.

Any effort to deviate from what is the normal routine or pattern of customer activity in the PMC can be enough to alert you to suspicious activity.

In order that suspicious activity is identified in your PMC, staff training is key.

If your staff are not fully aware of what is the norm for your PMC customers then they will be less likely to identify activity outside that norm. They should also be fully trained on the risk tolerances for your PMC.

11.6 Ongoing monitoring

In its simplest terms, monitoring customer activity and transactions is for the purpose of identifying unusual transactions or customer behaviour that may be linked to money laundering or terrorist financing activity.

A PMC 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. This includes:

1. Monitoring all transactions and the business relationship it has with the customer.

2. Taking measures to keep documents and information relating to customers and the Customer Risk Assessments up to date.
3. Identifying and scrutinising any complex or large transactions, unusual patterns of transactions that have no apparent economic purpose requested by the customer.

Fundamental to a good monitoring system is obtaining and keeping current customer and transaction information. Once this system is in place and operational, the task of identifying unusual transactions is made easier.

A good monitoring system should be capable of:

1. Highlighting unusual transactions or customer behaviour in a timely manner for further examination;
2. Generating reports in relation to such transactions or behaviour for review;
3. Ensuring that appropriate action is taken on the findings of any further examination which may include making a suspicious transaction report.

To facilitate this a PMC should ensure they have up to date CDD for all members, that it is recording/tracking transactions (placements and pay outs) and that a proactive approach is taken to the monitoring process.

As part of the required ongoing monitoring process the Designated Person must ensure that all documents, data and information obtained for the purposes of applying Customer Due Diligence are up to date. All such information retained by the Designated Person should be reviewed at regular intervals to ensure that it is up to date.

It may also be necessary to reapply or update current information where a transaction is not consistent with the Designated Person's knowledge of the customer and the normal transaction pattern in a PMC.

Please note there are additional requirements for enhanced Customer Due Diligence for Politically Exposed Persons (PEPs).

11.7 Risk identification and assessment

Please note that the below is not intended to be an exhaustive guide to risk identification and assessment, every PMC should take all measures necessary to identify, assess, and mitigate AML/CFT risk to their own business.

11.7.1 Risk factors for a PMC to consider include factors relating to:

- Its customers;
- The geographic area in which it operates;

- Its products or services;
- Its transactions.

11.7.2 In assessing their level of risk PMCs should consider the following questions:

- What risk is posed by the business profile and customers using the PMC?
- What risk is posed to the PMC operator/Designated Person by transactions with business associates and suppliers, including their beneficial ownership and source of funds? Are they open to undue influence?
- Is the business high volume consisting of many low spending customers?
- Is the business low volume with high spending customers?
- Is the business a mixed portfolio? Are customers a mix of high spenders and lower spenders and/or a mix of regular and occasional customers?
- Are procedures in place to monitor customer transactions to mitigate any money laundering potential?
- Is there gaming including peer to peer where there is potential for collusion between players?
- Is there gaming where there is potential for collusion between staff and customers?
- Are there adequate systems in place to detect efforts at collusion?
- Is the business local with regular and generally well-known customers?
- Are there a large proportion of overseas customers such as stag Groups or corporate events using foreign currency or overseas based bank cheque or debit cards?
- Are customers likely to be individuals who hold public positions (PEPs)?
- Are customers likely to be engaged in a business which involves significant amounts of cash?
- Are there likely to be situations where the source of funds cannot be easily established or explained by the customer?
- Are there likely to be situations where the customer's purchase or exchange of chips is irrational or not linked with gaming, i.e. goes against what you know to be the norm for a given scenario?
- Is there a local clustering of gambling outlets which makes it easier for a person to launder criminal proceeds over multiple venues and products?
- Does the customer have multiple or continually changing sources of funds (for example, multiple bank accounts and cash, particularly where this is in different currencies or uncommon bank notes)?
- Does the customer have multiple or changing addresses?
- Has the customer ever presented a fraudulent identity document or failed to provide an identity document repeatedly on request?
- Does the customer's behaviour follow a pattern or is it constantly changing, or did it abruptly change recently?

(Note: the above is not an exhaustive list)

11.8 Assessing your Customer Risk:

A PMC should assess and risk rate its customers, assigning higher risk ratings as appropriate; by identifying the higher risk category you are then in a position to implement mitigation measures.

Doing so will help protect your business from being unwittingly used for the purposes of money laundering or terrorist financing and protect your business brand.

The following list of customers may require a higher risk rating:

- Customers who are PEPs, family members of PEPs or known close associates of PEPs;
- High spenders – the level of spending which will be considered to be high for an individual customer will vary among s depending on their size, geographical area and customer profile;
- Disproportionate spenders – PMCs should be aware of the source of wealth/funds for their customers, with that knowledge they should be in a position to identify those spending beyond their known means;
- Casual customers – this includes tourists, participants in junkets and local customers who are infrequent visitors, these represent an opportunity for those seeking to launder money to fund 'junkets', stags etc. In return for money being laundered.
  Such customers represent an opportunity for criminals to engage in the practise of 'smurfing', i.e. Spreading money out in smaller amounts amongst a group, breaking up large amounts of cash into smaller amounts, ensuring that each individual remains below thresholds for CDD and obscuring the true ownership of the money being wagered. Junkets or stags from abroad afford a particular opportunity for cross border laundering;
- Regular customers with changing or unusual spending patterns, this relates to previously referenced disproportionate spenders.

(Note: the above is not an exhaustive list)

11.9 Other factors to consider in assessing risk for a PMC

Transaction risk:

- The exchange of chips/tokens etc. After minimal or low levels of actual play;
- Use of large amounts of cash. Large amounts of cash in circulation in society is becoming less common;
- Use of large denomination notes or stained/damaged notes;
- Use of prepaid cards that can obscure user and source of funds;
- Customers borrowing funds from each other.

Products offered:

- Certain products may afford greater opportunity for money laundering/terrorist financing;
- Peer to peer gaming;
- The capacity for two or more customers to offset their wagers against each other, e.g. Betting similar stakes on red and black in a game of roulette.

11.9 Mitigating Risks:

Where a customer is assessed as being in the higher risk category it does not mean that they are engaged in money laundering but rather they have been assessed as representing a higher risk to the PMC. Likewise, where a customer is assessed as being in the lower risk category it doesn't mean they won't engage in money laundering. Staff should remain vigilant in all cases, diligently applying all appropriate AML/CFT policies.

Effectively applying AML/CFT obligations and best practise is the best way to prevent your PMC being used for money laundering and terrorist financing purposes:

- Adopting and implementing AML policies and a Business Risk Assessment, updating them annually or as required. Ensure staff fully understand and implement them;
- CDD/EDD;
- Ongoing monitoring of customer transactions;
- Effective staff training;
- Report suspicious activity as soon as practicable;
- Comprehensive record keeping as required;
- Stay up to date with latest AML/CFT guidance for PMCs.

13 Gambling Service Providers

13.1 Introduction:

The definition of a Gambling Service Provider as a Designated Person is set out in Section 25 of the Act.

Under *S.I. 487 of 2018*, providers of gambling services became a class of Designated Person for the purpose of Section 25(1)(j) of the Act

"Section 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—
(j) any other person of a prescribed class."

SI 487/2018:
"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 ."

"Gambling services" *in the SI has the same meaning as Directive 2015/849. Under article 3 of the Directive:*

*"**gambling services**" means a service which involves wagering a stake with monetary value in games of chance, including those with an element of skill such as lotteries, casino games, poker games and betting transactions that are provided at a physical location, or by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services.*

13.2 Risk Management

The 2022 European Commission Supranational Risk Assessment report has rated **land based/offline betting activities as High risk** for money laundering activities and **online betting activities as Very High risk** (EU Commission Supra National Risk Assessment, 2022)**.**

13.2.1 Business Risk Assessment

A Designated Person shall carry out 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. This exercise should be appropriately documented and take account of the money laundering and terrorist financing risks involved in carrying out the business of a gambling service provider.

Where the gambling service provider operates more than one retail outlet, each retail gambling outlet should hold a copy of the documented global Business Risk Assessment for the group on each premises. All staff should know where the document is located in the event of an inspection by the AMLCU. In addition there should be a Business Risk Assessment document for each outlet that should take into account any relevant local, or geographical, risk factors and should assign a specific risk rating to the particular outlet.

The Designated Person should document consideration of the risks pertaining to the retail gambling outlet's particular services/products, customers, jurisdictions and distribution channels mindful of the nature, scale and complexity of the business model.

Where a retail gambling outlet is part of a larger group structure it is recommended that the individual outlet's risk assessment is driven by that outlet. Local staff should be the drivers for completion of their outlets risk assessment given their familiarity with the outlet, its locality and particular risks. Local risk assessments, in particular their risk rating, should contribute to and help inform the company's global Business Risk Assessment.

The document should be updated annually by senior management or more frequently where required. All staff should be familiar with the contents.

Copies of signed and dated Business Risk Assessments should be located in each individual retail bookmaker outlet in the event of a scheduled or unannounced inspection.

In the case of "online" Gambling Service Providers who do not have a physical presence in the Republic of Ireland it is incumbent on these providers to be capable of providing copies of their Business Risk Assessment document upon request by Authorised Officers of the AMLCU.

13.2.2 Risk Factors

Table 9: Non-exhaustive examples of business risk factors

Risk Factor	Risk Considerations
Customer	• Does the customer or its beneficial owners have attributes known to be frequently used by money launderers or terrorist financiers? • Reluctance to provide CDD documents/ satisfactory source of funds explanation. • Spending inconsistent with stated source of wealth. • Unusual forms or patterns of betting, or a bet out of character from a known/existing customer. • High Value Customers. • Individuals involved with cash intensive businesses.
Product and Service	• Do any of the products or services have attributes known to be used by money launderers or terrorist financiers? • Online Gaming. • Peer to Peer Gaming. • Self Service Betting Terminals. • Cash Cards.
Country or Geographic	• Are customers established in countries that are known to be used by money launderers or terrorist financiers? • Does the firm have a specific customer-base or niche service outside the EU (where AML regulation may not be so tight) (or from any high-risk third countries? • Risk factors particular to outlet localities, examples being level of crime, seasonal cultural/sporting events, proximity to public houses, proximity to border.
Type of Transaction	• Transactions that involve virtual assets (e.g., Bitcoin or other similar products) or involve other methods of payment facilitating anonymity (prepay cards etc.) • Cash transactions including large denomination notes. • Accepting foreign currency. • Large amounts of funds lodged to accounts with minimal betting. • Betting structured to avoid AML/CFT triggers (spreading bets across different outlets within same operator). • Persons attempting to lodge and withdraw funds with different payment methods.
Delivery Channel	• No face to face meeting. • Use of intermediaries/introducers/runners. • Online Gaming. • Peer to Peer Gaming. • Self Service Betting Terminal.
Additional Risk Factors	• High staff turnover. • Collusion with staff.

13.2.3 Customer/Transaction Risk Assessment

A Designated Person shall identify and assess the risk of money laundering and terrorist financing in relation to each relevant customer or transaction concerned. For Gambling Service Providers, this is in respect of customers and transactions of at least €2,000 in value (whether in one transaction or a series of transactions that appear to be linked).

Gambling Service Providers should gather sufficient information regarding the customer or specific transaction so they can make a determination on the level of risk the customer or transaction represents to the business. This assessment is an important part of the Customer Due Diligence process and will determine the level of due diligence the business will need to apply to the customer or transaction. For example, the application of standard due diligence in cases of low risk and the application of enhanced due diligence in cases of higher risk.

13.2.4 Sector specific risks

For Gambling Service Providers, the following is a non-exhaustive list of risks to consider:

- A failure to properly/adequately carry out the CDD process for customers leading to an inability to properly track customer spends as required and comply with AML/CTF obligations;
- A failure to engage effectively with customers leading to missed opportunities to prevent ML/TF;
- A failure to fully implement company policies and procedures when 'on-boarding' new customers, in particular online customers;
- The use of stolen or fraudulent CDD documentation;
- Unusual forms or patterns of betting, or a bet out of character from a known/existing customer;
- Large stakes on short odds;
- 'Smurfing' - a common money laundering method where multiple launderers will make numerous small transactions to minimise suspicion and evade "Know Your Customer" requirements at the threshold of gambling;
- Use of large denomination banknotes (e.g. €500 note);
- Use of damaged notes or notes with dye marks;
- Repeated requests by customers who stake in cash but request pay out by cheque or debit card;
- "Proxy stakes"/third party stakes – i.e. cash stakes laid by a person acting on behalf of another person or persons whose identity is not known to the bookmaker;
- Unusual use of customer accounts; e.g. a customer loading credit onto their pre-paid cards or e-card accounts using cash and then withdrawing the same amount of cash at a nearby branch without making a bet;
- Use of 'mule' accounts allowing for money launderers to spread large quantities of money across numerous accounts;
- Foreign currency being used as stake money;
- The use of crypto currency for online gambling;
- Transferable betting slips;
- Online customers from jurisdictions considered to be high risk;
- Peer to Peer betting;
- Bets placed on unregulated sporting events e.g. cricket tournaments, with no links to any recognised association;
- Use of self-service betting terminals, the associated challenges for local staff attempting to monitor their use in particular for tracking customer spends/pay-outs.

The identification of one or more of the above risks (or others identified by the Designated Person) when examining customers or transactions is not necessarily indicative of ML or TF taking place, however, it should serve as a risk indicator to a gambling service provider.

13.3 Customer Due Diligence

CDD documentation should be available for/accessible by staff at retail outlets in order that they may verify the identity of customers at the point/time of transactions where required. The staff member interacting with the customer should be able to view CDD documentation in order that they can accurately verify the individuals identify.

You should keep these documents on file and make them available for examination by regulatory investigators of the AMLCU during AML compliance inspections.

Records of Customer Due Diligence documentation should be accessible during an inspection. Electronic copies/scans that can be viewed on-site by regulatory investigators of the AMLCU are acceptable.

In the case of “online” Gambling Service Providers who do not have a physical presence in the Republic of Ireland it is incumbent on these providers to be capable of providing copies of such CDD records upon request by regulatory investigators of the AMLCU.

Monitoring of betting: Cash stakes of €200 or more must be monitored and stakes or pay-outs of €2,000 or more must not proceed until appropriate CDD is conducted and appropriate documentation obtained and retained.

CDD documentation should be in date at time of each transaction, where they require ‘refreshing’ no stakes should be accepted or pay out made until such time as it has been provided by the customer.

13.4 Ongoing Monitoring

In its simplest terms, monitoring customer activity and transactions is for the purpose of identifying unusual transactions or customer behaviour that may be linked to money laundering or terrorist financing activity.

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. This includes:

- Monitoring all transactions and the business relationship it has with the customer;
- Taking measures to keep documents and information relating to customers and the Customer Risk Assessment s up to date;
- Identifying and scrutinising any complex or large transactions, unusual patterns of transactions that have no apparent economic purpose requested by the customer.

Fundamental to a good monitoring system is obtaining and keeping current customer and transaction information. Once this system is in place and operational, the task of identifying unusual transactions is made easier.

A good monitoring system should be capable of:

1. Highlighting unusual transactions or customer behaviour for further examination;
2. Generating reports in relation to such transactions or behaviour for review;
3. Ensuring that appropriate action is taken on the findings of any further examination that may include making a suspicious transaction report.

As part of the required ongoing monitoring process the Designated Person must ensure that all documents, data and information obtained for the purposes of applying Customer Due Diligence are up to date. All such information retained by the Designated Person should be reviewed at regular intervals to ensure that it is up to date.

Cash stakes of €200 or more must be monitored and stakes or pay-outs of €2,000 or more must not proceed until appropriate CDD is conducted and appropriate documentation obtained and retained.

It may also be necessary to reapply or update current information where a transaction is not consistent with the Designated Person's knowledge of the customer and the normal transaction pattern.

Please note there are additional requirements for enhanced Customer Due Diligence for Politically Exposed Persons (PEPs).

13.5 Policies and Procedures

Each individual retail gambling outlet should have an up to date copy of their policies and procedures manual or documentation located on the premises. These documents should be easily accessible in the event of an inspection by the AMLCU. All staff employed at the outlet should know the location of the document/manual and should be familiar with their content. Electronic copies accessible by the staff on site are acceptable. These policies and procedures should be understood and adhered to by relevant staff.

In the case of "online" Gambling Service Providers who do not have a physical presence in the Republic of Ireland it is incumbent on these providers to be capable of providing copies of their policies and procedures upon request by regulatory investigators of the AMLCU.

13.6 Training

The importance and value of appropriate and comprehensive AML training and awareness cannot be overstated. It is considerably less likely that a Designated Person or their staff will detect or prevent the occurrence of money laundering and terrorist financing if they are not properly aware or trained on the matter.

Section 54 (6) of the Act requires Designated Persons to ensure that all persons involved in the conduct of the business are instructed on the law relating to money laundering, that training records are maintained and that appropriate ongoing training is provided.

Records of staff training should be created and maintained by the Designated Person. These training records should be readily accessible (hard-copy or electronic format) on-site and should be updated at least annually. AMLCU regulatory investigators shall assess the level of training/staff knowledge throughout the inspection process, for example where a failure to adhere to CDD requirements is identified, this may indicate a lack of staff awareness or training. Where evidence of training for that particular member of staff has been provided, this may indicate inadequacies in the current training regime.

In the case of “online” Gambling Service Providers who do not have a physical presence in the Republic of Ireland it is incumbent on these providers to be capable of providing copies of the relevant records upon request by regulatory investigators of the AMLCU.

14 External Accountants & Tax Advisers

14.1 Introduction

The definitions for those Designated Person supervised by the AMLCU are included under Section 25 of the Act detailed below:

Section 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—

(c) an auditor, external accountant, tax adviser or any other person whose principal business or professional activity is to provide, directly or by means of other persons to which that other person is related, material aid, assistance or advice on tax matters.

External Accountants and Tax Advisers are classed as "relevant professional adviser".

As per Section 24 of the Act:

"relevant professional adviser" means an accountant, auditor or Tax Adviser who is a member of a designated accountancy body or of the Irish Taxation Institute

Note: The AMLCU only supervises Tax Advisers and External Accountants not within the remit of a Designated Accountancy Body [DAB] listed below:

- Association of Chartered Certified Accountants (ACCA)
- Chartered Institute of Management Accountants (CIMA)
- Association of International Accountants (AIA)
- The Institute of Certified Public Accountants (CPA)
- Chartered Accountants Ireland (CAI)
- Chartered Institute of Public Finance and Accountancy (CIPFA)

The obligations under the Act for this cohort apply, when any Designated Person is acting in the course of business carried out by that person and meets the definition for their cohort.

The definition of an external accountant, tax adviser and a relevant transaction are further outlined in Section 24 of the Act:

24. "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,
…
"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—
(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…

Note: Where an individual provides tax advice *as part of their employment/in house services,* they are ***not*** considered to be a Designated Person as defined under Section 25 of the Act.

Consequently, the obligations set out for Designated Persons under the Act for AML/CTF do not apply to such Tax Advisers and therefore, are not subject to supervision by the AMLCU.

It should be noted that if those same Tax Advisers were to advise on tax matters outside of their employment then they may fall within the definition of a Designated Person under the Act and may fall to be supervised by the AMLCU.

14.2 Risk Indicators

Table 10: Risk Indicators

Risk indicator	Notes
Cash dependent or rich businesses.	Unexpected level of cash receipts or payments. Unexplained cash and or other banking practises. If this is not what would be expected it could indicate funds from illicit sources.
Unnecessary transaction splitting.	Transactions may be split unnecessarily across different service providers to prevent anyone involved in the transactions getting a full picture and becoming suspicious.
Provision of services with no face to face interaction.	Historic and ongoing engagement with customer can mitigate risk if they are consistently open and honest with their service provider, and financial indicators follow expected trends in their circumstances. Avoidance of face to face interaction should be assessed and viewed with heightened suspicion. Has the customer deliberately avoided face to face interaction and why so?
Payment in and out of a designated customer account controlled by a customer with no restrictions. Operation of pooled accounts.	The provision of a customer account provides the opportunity to obscure the source or beneficial owner of funds and can therefore be used to launder funds. This is particularly the case if the service provider is not subject to client rules and independent checks.

13.3 Tax Advisers

There are a number of offences that may give rise to money-laundering where there is criminal intent that Tax Advisers should be conscious of such as:

- Failing to file tax returns;
- Filing an incorrect tax return;
- Claiming a relief the taxpayer is not entitled to;
- Producing or assisting to produce a false invoice;
- Failing to deduct dividend withholding tax;
- Failing to pay the appropriate tax.[19]

[19] AML-Guidance-Notes-for-Tax-Advisers-2020.pdf (taxinstitute.ie)

The incidents where a Tax Adviser should consider that a customer may be involved in money laundering/terrorist financing and attempting to involve the Tax Adviser in this process would generally fall into two categories:

1. The customers actions with regard to their tax returns such as claiming reliefs they have been advised they are ineligible for, or an under declaration of income on a return or generally the falsification of returns;
2. The identification by the tax adviser of funds held by the customer that the tax adviser believes may be the proceeds of criminal activity (activity that may not be tax related).

In such instances the Tax Adviser must give consideration as to whether they have suspicions that their customer is engaged in money laundering/terrorist financing and whether they should submit a suspicious transaction report to the FIU and Revenue Commissioners.

Indicators of greater risk for a particular customer can include (but not limited to):

- A customer actively/aggressively seeking to reduce their tax bill, moving from tax liability minimisation/tax avoidance to tax evasion;
- Where services are sought but face to face meetings are avoided/discouraged by the customer.

13.4 External Accountants

The 2019 National Risk Assessment rated the ML/TF risk for the Accountancy Service Provider sector as medium-high[20]. The ease of access and range of services provided by accountants, along with their potential involvement at all stages of transactions of a wide nature mean that the potential to be unwittingly involved in money laundering or terrorist financing is considered to be significant.

Accountants should be aware of the risk that they will be used to legitimise funds and/or transactions by criminals or those seeking to fund terrorist activities, their client fund accounts are seen as being particularly vulnerable to being used for this purpose. This highlights the importance of well-structured and fully implemented policies and procedures, Business Risk Assessments, staff training and the awareness of when to submit an STR, for the sector to prevent it from being used for ML or TF.

The range of risk indicators for accountants to be aware of is significant, some general indicators include (but not limited to):

- Customer has funds, or engages in transactions inconsistent with the accountants' knowledge of their business activities;

[20] https://assets.gov.ie/8242/80ab9a41b1354405adcec66bfb1c0715.pdf

- Repeated/regular change of accountants, which may indicate an attempt to prevent any accountant from becoming too familiar with their business activities;
- A refusal to have face to face meetings;
- The structure of the business is inconsistent with what would be expected, for example few or no employees in a business where it would be the norm for a high number;
- The customer expects their accountant to draw up accounts or complete returns based on incomplete records, with a lack of original documents, receipts etc;
- Customer records consistently reflect sales at less than cost despite this placing them into a loss position and they continue this practise without offering any business/economic rationale for doing so;
- Customer makes payments to subsidiaries or similarly controlled companies that are not within the normal course of business;
- Customer acquires large personal and consumer assets (luxury goods, cars etc.) when this is inconsistent with what the accountant knows of the customer and/or their business;
- Where a customer account facility is provided and controlled by a customer there are frequent payments in and out which may be an indication of attempts to launder the funds by obscuring the source or beneficial owners of the funds.

15 Notaries Public

15.1 Introduction

Notaries fall under the definition of a Designated Person under Section 25 of the Act:

Section 25 of the Act lists "relevant independent legal professional[s]' as Designated Persons, Section 24 of the Act defines the meaning of a "relevant independent legal professional".

Section 24 says a "relevant independent legal professional" means a barrister, solicitor or notary who carries out any of the following services:

(a) the provision of assistance in the planning or execution of transactions for clients concerning any of the following:

(i) buying or selling land or business entities;

(ii) managing the money, securities or other assets of clients;

(iii) opening or managing bank, savings or securities accounts;

(iv) organising contributions necessary for the creation, operation or management of companies;

(v) creating, operating or managing trusts, companies or similar structures or arrangements;

(b) acting for or on behalf of clients in financial transactions or transactions relating to land;

Under Section 25 of the Act, a relevant independent legal professional is a 'Designated Person' only in respect of carrying out of the services specified in the definition of 'relevant independent legal professional'.

15.2 Why a Notary Public may be attractive to those engaged in ML/TF

Notaries are potentially an attractive target to money launderers/terrorist financers for a number of reasons, not least the opportunity of utilising a respected legal profession to give illicit moneys or transactions a veneer of legitimacy.

The role of a notary includes authenticating and legalising documents for individuals and corporate entities. A notary is often required in legal matters involving an international element of a legal or commercial transaction. In many cases this involves assisting the parties with property, financial transactions, inheritances and documents. It is the provision of these services that make Notaries attractive to those engaged in money laundering and terrorist financing.

This is particularly the case in instances where a Notary Public has involvement, either directly or indirectly, in transactions featuring high levels of cash. Although, in general, Notaries in Ireland do not handle customer funds or property on behalf of its customers, it is important to be aware of the risks posed by indirect or peripheral involvement in these kinds of transactions.

An example of indirect involvement could be a notary attesting documents that are related to a transaction (such as verification of documents). Although at no stage has the notary actually processed or held any funds on behalf of the customer, the legitimacy of these attested documents provides the appearance of authenticity to the overall transaction.

Notaries should be conscious of the risks posed through carrying out services for customers that may seem simple or routine, every service provided has the potential to aid or facilitate those engaged in money laundering/terrorist financing.

15.3 Supervision of Notaries

Section 60 of the Act determines who the Competent Authority for anti-money laundering (AML) supervision of Designated Persons is. Although all Notaries must be practising barristers or solicitors at the time that they apply to become Notaries, this position may change over a period of time resulting in two categories of Notaries to be considered as 'Designated Persons' under the Act:

1. Notaries who are practising solicitors or barristers;
2. Notaries who are no longer practising solicitors or barristers.

Section 60 of the Act provides:

> *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:*
> *[…]*
> *(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 Legal Services Regulatory Authority;*
> *(e) in the case of any Designated Person other than a Designated Person referred to in paragraph (a), (b), (c) or (d), the Minister.*

The Competent Authority for anti-money laundering (AML) supervision for Notaries that no longer practice as solicitors or barristers is the Minister for Justice through the Anti-Money Laundering Compliance Unit (AMLCU).

15.4 Customer Due Diligence

Each customer availing of the services of a relevant independent legal professional, should be individually risk assessed and assigned an individual risk rating. Please refer to Chapter 6 for further guidance on CDD. The Customer Risk Assessment should be documented and used to determine the extent of Customer Due Diligence (CDD) and ongoing monitoring to be taken in relation to the customer or transaction. This exercise should have regard to the factors listed under Section 30B(1) and the factors outlined in Schedule 3 and Schedule 4 of the Act where appropriate.

Checks should be conducted (such as open source checks) on customers in order to identify Politically Exposed Persons (in particular when 'on-boarding' customers), evidence of the open source checks should be retained as part of CDD records for each customer. This provision should also be documented in the AML/CTF Policy and Procedures document for the notary.

15.5 Risk-Based Approach

A notary should consider a wide range of risk factors which may impact on their business which include risks that are applicable across the legal professions. FATF have prepared and published a comprehensive document detailing, for legal professionals, best practice guidelines for adopting a risk-based approach (Risk-Based Approach Guidance For Legal Professionals (fatf-gafi.org)[21].Some of the risk factors to consider are detailed below and the AMLCU recommends that the full document should be reviewed.

- Unusual transactions:
  - The type of operation being notarised is clearly inconsistent with the size, age, or activity of the legal entity or natural person acting;
  - The transactions are unusual because of their size, nature, frequency, or manner of execution;
  - There are remarkable and highly significant differences between the declared price and the approximate actual values in accordance with any reference which could give an approximate idea of this value or in the judgement of the legal professional;
  - Legal person or arrangement, including NPOs, that request services for purposes or transactions, which are not compatible with those declared or not typical for those organisations;

[21] [21] https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Legal-Professionals.pdf

  - The transaction involves a disproportionate amount of private funding, bearer cheques or cash, especially if it is inconsistent with the socioeconomic profile of the individual or the company's economic profile;
- The customer or third party is contributing a significant sum in cash as collateral provided by the borrower/debtor rather than simply using those funds directly, without logical explanation;
- Unusual source of funds:
  - Third party funding either for the transaction or for fees/taxes involved with no apparent connection or legitimate explanation;
  - Funds received from or sent to a foreign country when there is no apparent connection between the country and the client;
  - Funds received from or sent to high-risk countries;
- The customer is using multiple bank accounts or foreign accounts without good reason;
- Private expenditure is funded by a company, business or government;
- Selecting the method of payment has been deferred to a date very close to the time of notarisation, in a jurisdiction where the method of payment is usually included in the contract, particularly if no guarantee securing the payment is established, without a logical explanation;
- An unusually short repayment period has been set without logical explanation;
- Mortgages are repeatedly repaid significantly prior to the initially agreed maturity date, with no logical explanation;
- The asset is purchased with cash and then rapidly used as collateral for a loan;
- There is a request to change the payment procedures previously agreed upon without logical explanation, especially when payment instruments are suggested that are not appropriate for the common practice used for the ordered transaction;
- Finance is provided by a lender, either a natural or legal person, other than a credit institution, with no logical explanation or economic justification;
- The collateral being provided for the transaction is currently located in a high-risk country;
- There has been a significant increase in capital for a recently incorporated company or successive contributions over a short period of time to the same company, with no logical explanation;
- There has been an increase in capital from a foreign country, which either has no relationship to the company or is high risk;
- The company receives an injection of capital or assets in kind that is excessively high in comparison with the business, size or market value of the company performing, with no logical explanation;
- There is an excessively high or low price attached to the securities transferred, with regard to any circumstance indicating such an excess (e.g. volume of revenue, trade or business, premises, size, knowledge of declaration of systematic losses or gains) or with regard to the sum declared in another operation;
- Large financial transactions, especially if requested by recently created companies, where these transactions are not justified by the corporate purpose, the activity of

the customer or the possible group of companies to which it belongs or other justifiable reasons.

The above factors constitute some of the risks associated with operating as a Notary Public. A bespoke Business Risk Assessment should be conducted to account not only for inherent risks that apply to a specific sector, but must also account for the particularities of the individual business and the risks to which it is exposed. Additional guidance is provided in Chapter 5 on assessing risk.

Some risk indicators that Notaries should consider, as part of conducting their Business Risk Assessment and/or dealing with individual customers are detailed in the table below.

Table 11: Non-exhaustive list of Risk Factors for Notaries

Risk Factor	Specific Risks
Customer Risk	• Is this a new customer? • Is the customer known to you? • Is introduction from a 3rd Party? If channelled through a 3rd Party is reason OK? • Is customer a PEP? • Face to Face: Will you meet customer face to face? If not why? • Has the person travelled a great distance? • Does the person exhibit suspicious/evasive or distressed behaviour? • Does the person demonstrate appropriate knowledge about the purpose and particulars of the transaction?
Countries or geographical areas served	• International Market and Networks. • Customers from High Risk Jurisdictions. • Is client based in Ireland? If not, note below and consider country risk. • Is client / transaction linked to a high risk jurisdiction/ high risk third country? • Connections to a jurisdiction where ML controls are not as good as EU? • Are funds being channelled through any of these places? • Is the client/jurisdiction subject to a sanctions regime?
ID and Address Verification	• Have all required documents been checked and scans / copies kept? (non-exhaustive list of checks below) ○ Names and Addresses match with ID and Proof of Address Documentations ○ Damage to ID documentation ○ Signatures are all present and match ○ Documents relate to the proposed transaction

Risk Factor	Specific Risks
	○ Are all forms fully completed? (strikethrough or N/A in blank spaces) ○ Unusual document formatting ○ Missing or altered numbers/text • Has client been cooperative in the process? • Has the necessary corporate documentation been provided (incl. UBO / structure)? • If an intermediary third party has been used: ○ Is the third party an appropriate supervised legal or professional service provider (solicitor accountant etc.?) Has this been confirmed with relevant professional bodies? ○ Has CDD been obtained for the intermediate third party as well as the UBO?
Source of Funds	• Is the source of funds and source of wealth clear and identifiable? • Note level of funds and associated risk factor. • Are funds coming from a recognised institution (e.g. a loan)? • If personal funds? Enquire into the source of wealth and note same. If risk level merits it, consider asking for supporting evidence and then reconsider risk factors. • Is any funding coming from overseas? Note from whom, where and their connection to client. • Are any of the funds being paid by a third party otherwise unconnected to the transaction?
Other Risk Factors	• Awareness and Training of Staff of AML/CTF requirements. • Does it make sense that the notary has been asked to carry out the type of transaction?

16 Art Traders & Art Intermediaries

16.1 Introduction

Since the transposition of 5AMLD in April 2021, High Value Art Traders and Art Intermediaries in the trade of works of art including when carried out in a free port, have been Designated Persons under the Act. This means they are required to take various measures and comply with the obligations on Designated Persons in the Act to ensure their business is not being used for money laundering or terrorist financing by criminals.

Under the provisions in the Act, persons trading or acting as an intermediary in the trade of works of art (including when carried out by an art gallery or an auction house) but only in respect of transactions of at least €10,000 in value (whether in one transaction or a series of transactions that appear to be linked) are a category of Designated Person obliged to take the measures set out in the Act to ensure their business is not being used for money laundering and/or terrorist financing.

Section 25 of the Act defines the meaning of 'Designated Persons' as follows:

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-

(ib) a person trading or acting as an intermediary in the trade of works of art (including when carried out by an art gallery or an auction house) but only in respect of transactions of a total value of at least €10,000 (whether in one transaction or a series of transactions that are or appear to be kinked to each other),

(ic) a person storing, trading or acting as an intermediary in the trade of works of art when this is carried out in a free port but only in respect of transactions of a total value of at least €10,000 (whether in one transaction or a series of transactions that are or appear to be linked to each other),

At date of publication Ireland has no free ports in operation in the State.

Works of art are generally considered to mean paintings, drawings, sculptures, carvings etc. As set out in the FATF report on "Money Laundering and Terrorist Financing in the Art and Antiquities Market", at present there are no standard, universally accepted definitions of the types of objects handled in the sector.

In this report FATF has proposed the definition:

"Art, artwork, or work of art:

An object of artistic interest. Some forms of art include paintings, drawings, collages, decorative plaques, or similar pictures executed by hand; original engravings, lithographs or other prints; sculptures or statues; sculpture casts; tapestries or other hangings; ceramics; enamels on copper; photographs; and others. Art can also include digital art or collectable items, such as those secured through or represented as NFTs." [22]

Linked transactions refers to transactions involving the same beneficiary of the goods e.g. someone may make four purchases which together but not individually amount to €10,000 or over.

16.2 Why the art sector is attractive to money launderers

In 2021, it is estimated that globally combined sales of art and antiques by dealers and auction houses in the global art market reached an estimated $65.1 billion[23]. This represented a 29% increase on the previous year. Criminals are continually searching for new ways to launder or move funds and the art sector has become an attractive option.

Some of the reasons that make the art sector attractive to money launderers include the following:

1. Transportation and concealment

Works of art are relatively easy to transport. High value works of art can be small in size and easily transported from one country to another. This could be facilitated using, for example fake invoices or private planes e.g. a fake invoice may understate the value of artwork to avoid attention and detection from officials. Artwork could also be placed in storage (including for lengthy periods) to conceal its whereabouts. During storage, the value of the artwork could increase substantially, surpassing the value of the proceeds of crime initially used to purchase the item. Non-Fungible Tokens (NFTs) pose additional risks as digital assets can potentially be exchanged instantly and anonymously. NFTs are digital assets, only existing in digital form, i.e. they can't be touched. They can be any

[22] https://www.fatf-gafi.org/en/publications/Methodsandtrends/Money-Laundering-Terrorist-Financing-Art-Antiquities-Market.html

[23] Art Basel and UBS Global Art Market Report 2022 https://www.ubs.com/global/en/our-firm/art/collecting/art-market-survey.html#:~:text=Global%20art%20sales%20rebounded%20above,2019%20value%20by%20%240.7%20billion.

kind of digital file art works, an article, music, video, meme etc. Their ownership details are stored on a block-chain, a shared ledger of sorts.[24]

2. Pricing

The price paid for an artwork is generally determined by a range of factors e.g. artists reputation, popularity and current trends. Items are often unique which can make it difficult to detect how appropriate the pricing of a piece of art is. Furthermore the price of art can fluctuate in a short period of time, these fluctuations and the unique pricing for art works, can allow criminals to manipulate the market to increase the value of the artwork, thereby, achieving greater value when divesting themselves of the work.

3. Privacy

Criminals may seek to maintain privacy, with valuable pieces of artwork often sold to “anonymous buyers.” This is a particularly significant risk where non-face-to-face transactions are facilitated and where there are digital transactions involving NFTs. The use of intermediaries such as shell companies could also make it potentially difficult to confirm the identity of buyers or sellers and ultimate beneficial owners, and potentially also facilitate criminals and/or individuals evading the ramifications of sanctions imposed on individuals or countries.

4. Origins of the artwork

Works of art sometimes have gaps in their ownership records, consequently the true origins of the artwork may be unclear. This may mean that suspicious gaps in the origins of an item of artwork aren’t always detected or reported to law enforcement, they are incorrectly accepted as being the ‘norm’ for transactions in the art world.

5. Non face-to face transactions

Transactions made online, over the phone or via an intermediary increase the vulnerability to money laundering by decreasing the opportunity to interact with the customer. Meeting a customer face-to-face can facilitate in determining if the customer has a legitimate reason for the purchase and whether the transaction is in line with expectations.

6. Use of Cash/anonymous payment methods

Use of cash to purchase items of art is a way to launder funds and hide cash proceeds of criminal activities. Purchasing in cash allows for an additional layer of anonymity as it is difficult to trace the funds used for a cash purchase, both in identifying the routing of the funds and the identity of the buyer and the seller. Purchasing works of art legitimises illicit cash and converts it into an asset that

[24] What is NFT Art: All you Need to Know - NFTexplained

can increase in value, and can be sold on at a later stage. Once the art work has been sold, either for a profit or a loss, the cash has been washed and the criminal can evidence the source of funds as being legitimate i.e. from the sale of an art work.

7. Fictitious Sales

A money launderer could sell works of art at an auction, which are bought by an accomplice using funds earned from the proceeds of crime. The money launderer then receives payment from the auctioneer, by EFT or cheque, the funds generated can enter into the legitimate financial system with the credibility of a payment from a business supporting them.

16.3 Risk-Based Approach

Businesses operating in the art sector should adopt a risk-based approach to identify potential money laundering risks involved in the business. This centres on having a good understanding of the money laundering and terrorist financing risks the business is exposed, and taking appropriate mitigating measures in accordance with the level of risk identified.

Section 30A of the Act requires Designated Persons to prepare a documented Business Risk Assessment to assist in identifying where there is a risk in the business that could be exploited for money laundering and terrorist financing purposes. This assessment should be an accurate appraisal of the risks specific to the business as an art trader or art intermediary. The exercise will allow Designated Persons to assess the risks identified and to put in place appropriate internal controls to manage and mitigate these risks to an acceptable level. Measures include complying with the obligations set out in the Act (See Chapter 4).

The FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing - High Level Principles and Procedures[25] and the FATF Report: Money Laundering and Terrorist Financing in the Art and Antiquities Market[26] outline the basic process for assessing risk. Additional guidance is provided in Chapter 5 on risk assessment.

The table under sets out specific risks in the art sector that Designated Persons in the art sector should consider in assessing the risks their business is exposed to.

[25] FATF Guidance – Risk-Based http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatfguidanceontherisk-basedapproachtocombatingmoneylaunderingandterroristfinancing-highlevelprinciplesandprocedures.html

[26] https://complyadvantage.com/insights/fatf-report-nft-art-money-laundering-risks/

16.4 Risk Factors in the Art sector[27]

Table 12: Risk Factors in the Art sector

Risk Factor	Specific Risks
Type of customer	• Culture of discretion. Buyer and seller often unknown to each other. • Art seen as status symbol in criminal world. • Use of shell companies, trusts, third party intermediaries to purchase, sell or hold art.
Products and services	• High value nature of goods. • Value of art varies greatly, making it attractive to varying levels of criminals. • Subjective pricing can allow criminals to inflate or deflate the price of an asset to facilitate 'wash trading' to manipulate the market or transfer value • Varying value provides option to launder money through small number of high value purchases or large number of low value purchases.
Countries or geographical areas served	• International Market and Networks. • Customers from High Risk Jurisdictions. • Transnational nature of the market means that it is common practice for art to regularly be moved to other jurisdictions.
Types of transactions	• Common use of intermediaries or proxies for transactions. • Common use of foreign/offshore structures and accounts. • Concealment of source of funds through complex layers of offshore companies and trusts, agents or intermediaries. • Increase in online art market places and trading platforms, where buyers and sellers can interact directly, could also increase the risks in the sector, representing an even greater move away from face-to-face transactions. • Transactions involving art market participants (AMPs) without expertise in concluding high-value purchases or sales • Use of large denomination notes e.g. €500 banknote. • Use of cryptocurrency and other payment methods facilitating a degree of anonymity
Delivery channels	See transactions
Other risk factors	• Awareness and Training of Staff.

[27] Source: UK NRA 2020 and http://responsibleartmarket.org/guidelines/guidelines-on-combatting-money-laundering-and-terrorist-financing/

Risk Factor	Specific Risks
	• Ability to conceal beneficial owner and final destination of art. • Previous lack of regulation. • Ease with which items can be transported in the State or across borders. • Transactions involving market participation without appropriate expertise in concluding the high value sale or purchase.

16.5 Risk indicators for the art sector

AML/CFT art sector risk indicators (for customers, the artwork itself and transactions) include:

Customer

- Customers identified as being linked to or active in criminality (including regulatory criminality);
- Politically exposed persons (PEPs) including persons closely associated with PEPs;
- 3rd parties acting on behalf of unidentified buyers/sellers;
- New customers based in, operating or banking from/in higher risk jurisdictions;
- Complex corporate structures, off shore companies, trusts etc.;
- Is the customer from a country subject to sanctions?

Artwork

- Insufficient supporting documentation;
- Reluctance or failure to provide written evidence of the artwork provenance;
- Is the artwork from a country subject to sanctions?

Transaction

- Customer fails to comply fully with the Customer Due Diligence process;
- Any concern regarding information provided by the customer;
- Use of anonymous payment methods by a buyer such as cryptocurrencies or prepay debit cards;
- Use of significant/multiple amounts of cash by buyer or sellers asking to be paid in cash;
- Multiple payments in low amounts of cash may be an indicator of attempts to avoid triggering CDD requirements;
- Use of third parties for payment or receipt of payments by buyers/sellers;
- Transactions that appear (based on your knowledge/experience) to be suspiciously low or high in value e.g. subjective pricing of artworks;
- Transactions that appear (based on your knowledge/experience) to be overly complex or lack in economic sense e.g. an asset has changed ownership rapidly over a short period of time;
- Customers who take an unusual interest in AML processes.

17 High Value Goods Dealers (HVGDs)

17.1 Introduction

A High Value Goods Dealer (HVGD) is any person trading in goods, but only in respect of transactions involving payments to the person or by the person in cash, of at least €10,000 or more (whether in one transaction or a series of transactions that appear to be linked).

Section 25 of the Act, defines the meaning of Designated Person as it relates to a HVGD.

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—

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

Examples include (not limited to):

- Antique Dealers
- Marine Dealers
- Car Dealers
- Gold Bullion Dealers
- Jewellers
- Plant Hire

In accordance with Section 25 of the Act, a person is only considered a Designated Person (HVGD) if they are trading in goods but only in respect of transactions involving payments in cash of at least €10,000 whether this be in one transaction or a series of transactions that appear to be linked. Such cash transactions of €10,000 or more include both cash payments received by the person and cash payments made by the person e.g. cash used by the business to purchase stock.

Persons trading in goods involving payments in cash of less than €10,000 or not involving payments in cash whatsoever, are therefore not considered a Designated Person for the purposes of the Act.

Only those persons trading in goods that have never previously accepted or made a cash payment of €10,000 or more in one transaction or a series of transactions that appear to be linked, can be classified as not a Designated Person.

All other persons that are or have previously traded in goods involving payments in cash of €10,000 or more whether this be in one transaction or a series of transactions that appear to be linked either to or by the person, regardless of when these transactions were conducted, is considered a Designated Person (HVGD) and must comply with their obligations set out in the Act.

17.2 Why the HVGD sector is attractive to ML/TF

The buying and selling of high value goods using illicit funds is one of the most common forms of money laundering/terrorist financing. Even where sold at a loss, the sale of the item generates 'clean money' for the individual/organisation. By virtue of being 'high' in value, the goods are attractive to money launderers as they can launder more illicit funds in one transaction.

The risk of individual HVGDs being used for money laundering/terrorist financing will vary from business to business depending on their own specific business activities, the nature of their 'product', their business structure, their customer base, their level of AML awareness, their internal AML controls and training, and their overall risk appetite i.e. their willingness to accommodate large cash payments.

The National Risk Assessment Ireland Money Laundering and Terrorist Financing (April 2019)[28] gives some examples of why the High Value Goods Dealers Sector is attractive to money launderers.

1. The accessibility and cash intensive nature of transactions in this sector increases its vulnerability to money laundering (and/or terrorist financing). An individual/organisation who wishes to dispose of illicit funds could simply purchase a high value good, on an anonymous basis, with cash or seek a third party to purchase the item on their behalf to further anonymise the transaction.

2. HVGDs can deal in ranges of luxury goods (although they may not always be considered 'luxury' items) and products that make them vulnerable to ML/TF due to the highly portable nature (allowing them to be moved between jurisdictions) and intrinsically high value of the goods and products.

3. In addition, transactions with HVGDs are typically occasional in nature (repeat customers are not uncommon though) and will not result in ongoing business relationships being established with customers.

[28] www.amlcompliance.ie

Gold and Silver Bullion dealers are a category of HVGD that are considered to be more susceptible for being used for money laundering. The Financial Action Task Force Report Money laundering / terrorist financing risks and vulnerabilities associated with gold July 2015[29] sets out why gold as a product is attractive to money launderers and would be relevant to Gold Bullions Dealers and Jewellers:

- The Gold Market is cash intensive;
- Gold can be traded anonymously and transactions are difficult to trace and verify;
- Gold is a form of global currency and acts as a medium for exchange in criminal transactions;
- Investment in gold provides reliable returns;
- Gold is relatively easily smuggled and traded – both virtually and in person.

Certain HVGDs sectors/types have traditionally afforded their customers a higher degree of discretion and confidentiality, this has made them attractive to individuals/organisations involved in ML/TF wishing to avoid detection.

The above factors constitute some general, inherent risks associated with the High Value Goods Dealers sector.

A bespoke Business Risk Assessment should be conducted to account not only for inherent risks that apply to a specific sector, but also to account for the particularities of the individual business and the risks to which it is exposed.

The AMLCU have prepared a sample template Business Risk Assessment which may be of assistance to HVGDs. This can be accessed on the AMLCU website[30] .

Further specific risk factors to consider are discussed below.

[29] https://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-risks-vulnerabilities-associated-with-gold.pdf
[30] https://www.amlcompliance.ie/forms-guides/

Examples of risk indicators of suspicious transactions:

- Use of €500 notes;
- The notes appear to be stained or washed;
- The customer claims to have withdrawn the funds directly from the bank but the notes are not new/crisp and do not have bank bands (where sufficient cash amounts are involved);
- A transaction that does not make commercial sense. For example, a customer may be willing to pay over the odds once they can pay in cash.
- A customer refusing to provide ID when requested;
- A customer that seems evasive about the source of the cash;
- A customer that is not local to the business making a large once off transaction without reasonable explanation;
- A customer based in, or conducting business through, a jurisdiction considered high risk;
- A customer who wishes to transact primarily in cash.

17.3 Risk indicators that are common to all HVGDs include:

- **Customers that pay large amounts of cash in one off transactions:** In these instances the cash being used is unlikely to have a proper audit trail. Questions to ask include, does the cash look like it was recently withdrawn from a bank or does it appear widely used? Is the cash bank banded? Is the cash in large or small denomination? What is the physical condition of the notes, do they appear to have been washed or is there traces of die on the notes?
- **Customers that make multiple cash payments below the threshold that appear to be linked:** Has the customer tried to avoid the Customer Due Diligence requirement by making numerous small cash payments? To mitigate against this risk, the HVGD should have in place a suitable system for tracking and monitoring potential linked transactions. If the accumulative of linked cash transactions reaches €10,000 or more, Customer Due Diligence must be conducted on this customer;
- **Individuals that make large cash payments on behalf of the ultimate beneficial owner of the item:** For example, where an individual presents with a cash payment of €10,000 or more but is not the ultimate beneficial owner of the item, the HVGD should obtain Customer Due Diligence for both individuals involved in the transaction i.e. the beneficial owner of the item and the individual presenting with the cash;
- **Customers who pay in large amounts of cash but don't appear to have the means to support these levels of payment:** In these instances the HVGD should establish, as best they can, the true source of the funds (both wealth and funds) used in the transaction. The explanation should be recorded on the

Customer Transaction Form. This form is available on the AMLCU webpage. In cases of heightened suspicion, the HVGD may request further proof from the customer as to the source of the wealth and the funds;

- **One off customers:** In this instance the business will have little or no trading history with this customer. It is important to establish if the customer is genuine or a front for another individual or business that may be involved in possible money laundering;
- **Customers that are not local to the business:** If a customer travels a long distance to purchase an item when the same item is readily available near their home address, this may be considered unusual and require further scrutiny. Particularly, if they are paying in cash. In this instance, the transaction does not appear to make commercial sense;
- **Customers who have unusual delivery instructions:** If a customer requests delivery to an address not apparently linked to them or to a third country outside the EU/one considered to be high risk for ML/TF without satisfactory explanation.
- **Transactions that appear to be out of the norm for your business sector and lacking in commercial or economic rationale.**

When conducting a Business Risk Assessment the individual characteristics of a HVGDs operations should be considered. The non-exhaustive list below details a number of questions that should be considered as part of this process. This will help inform a HVGD as to the risks their operations expose them to, with regard to money laundering/terrorist financing:

- Does your business have a high turnover of customers (higher risk) or a stable existing customer base made up of repeat customers? (lower risk);
- Is there a high proportion of one-off customers/deals? (higher risk);
- Do you know your customers personally? If not, what additional steps do you take to mitigate the risks that this poses? (Please note that whether you know a customer personally or not, the obligations for proper implementation of your AML obligations remain the same);
- Does the business have a significant number of non-EU-based clients (where AML regulation may not be to the same standard) or any high-risk third countries? (higher risk);
- What is the source of customers – referrals, walk-in or from internet advertisements? (Consider the different levels of risk that can arise from different customer channels);
- Consider your stock profile and whether any products you offer are attractive to money launderers. This should include whether products sold are new or used, higher or lower value etc.;
- Does the business undertake work which may be of lower AML risk (E.g. parts and servicing, jewellery repair, antique restoration);
- Does the business sell stock that facilitates anonymity for the beneficial owner? (higher risk);
- Does the business sell stock that can be easily transported out of the jurisdiction and resold in another jurisdiction? (higher risk);

- Does the business have a large amount of transitory customers? (i.e. non-residents/tourists) (higher risk);
- Could the areas in which your customers are based (or from which they operate their businesses) have high levels of crime? (higher risk);
- Does your business conduct trade across borders? (higher risk);
- Does the firm have a specific client-base, niche or sell products to customers from outside the EU (where AML regulation may not be to the same standard) (or from any high-risk third countries? (higher risk);
- Do you sell products to customers online? Does this process include controls to mitigate against the risk of money laundering and/or terrorist financing?
- Do you sell products to customers you have not met face-to-face? (higher risk)
- What percentage of your business is on a non-face-to-face basis? (higher the percentage means higher risk);
- Do you always meet the true beneficial owner of the item face-to-face? (lower risk);
- Do you always meet/have a relationship with the underlying customer? (lower risk);
- Do you undertake work which is conducted through intermediaries or other third parties? (higher risk);
- Do you deliver products to customers without meeting them in the first instance? Do you deliver to third party addresses?(higher risk);
- Do you accept cash payments? (higher risk);
- What percentage of overall sales are attributed to cash payments? (greater the percentage, the higher the risk);
- Do you have a limit to the amount of cash you will accept? E.g. don't accept cash over €5,000. (accepting large cash sums is a high risk activity);
- For large cash payments, are you in a position to accurately identify the source of that cash considering your customer profile?
- How frequently do you carry out higher risk transactions? Are these necessary? Are there any features in transactions delivered by the business which may represent higher risk? How can these be mitigated?

17.4 Customer Due Diligence (CDD) measures specific to HVGDs

Chapter 6 regarding general CDD requirements should be reviewed prior to considering the HVGD specific due diligence measures outlined in this section.

The requirement to apply Customer Due Diligence (CDD) measures relates to all cash transactions of at least €10,000 whether this be in one transaction or a series of transactions that are or appear to be linked involving the HVGD. This includes both cash payments of €10,000 or more received by the HVGD and cash payments made by the HVGD. In both instances, full CDD measures must be applied to the individual(s) involved.

HVGDs must apply CDD to all cash transactions of €10,000 or more in a single transaction or a series of linked transactions. For HVGDs, there is a requirement to have in place procedures to identify and verify the identity of the customer. There is also

a requirement to establish the source of the funds used in the large cash transaction. The Designated Person must record the method of payment (e.g. cash, cheque, EFT, etc.) on all of their transactions. This method of payment should be clearly evident to an AMLCU regulatory investigator during an AML compliance inspection.

Where appropriate, additional checks or Enhanced Customer Due Diligence (ECDD) should be carried out to ascertain if a prospective customer making a cash payment over €10,000, including linked transactions, is potentially a *Politically Exposed Persons ("PEP").* Please refer to Chapter 7 for further information regarding PEPs. These checks can be achieved by open source checks, and evidence of same should be retained on file as part of Customer Due Diligence records.

A key requirement of CDD is obtaining proof of a customer's identity and verifying the customer's identity in circumstances whereby the prospective customer is making a cash payment over €10,000, including linked transactions.

Prior to carrying out a transaction the AMLCU recommends that a HVGD should:

1 **Identify the customer**
In order to identify the customer, photographic I.D should be requested and a copy of same retained. For example, a customer's driving licence or passport.

2 **Verify the customers identity**
In order to verify the customer's identity, a recent utility bill should be requested, dated within 6 months of the transaction date, which is in the name of the customer and includes the customer's current address.

Please note: In order to accept an Irish Driving License as both proof of address (POA) and identification (ID), it must be dated/have been issued within the previous 6 months.

17.5 Source of Funds and Due Diligence Cash Transaction Record Form

In order to assist HVGDs in carrying out appropriate Customer Due Diligence, the AMLCU has prepared a HVGD Due Diligence Cash Transaction Record. This document is available on the AMLCU's website[31] www.amlcompliance.ie.

The AMLCU recommends that this form be utilised to record the source of funds where there are cash payments, particularly one off cash payments of €10,000 or more, or a series of linked cash transactions of €10,000 or more over a twelve month period. Regarding linked transactions, it is important that the HVGD has a system in place whereby all cash transactions can be identified and tracked in order to identify when the €10,000 cash threshold is reached through linked transactions.

The customer's explanation for the source of the funds/wealth (cash) should also be recorded on the Cash Transaction Form (available on the AMLCU website) and this form should be kept as part of the overall Customer Due Diligence records for this

[31] https://www.amlcompliance.ie/forms-guides/

individual. It is important that this cash transaction form is completed in full by the Designated Person.

In cases of heightened suspicion, or where the explanation given by the customer provides little or vague detail regarding the source of funds, the Designated Person should request additional proof from the customer as to the source of the funds. This is applying enhanced due diligence, for further information regarding EDD please refer to Chapter 6. In these instances, the HVGD should request further information on the customer and proof of the source of the wealth and the source of the funds, i.e. what is the source of the wealth (loan, savings, sale of a previous car, inheritance, lotto etc.) and what is the source of the funds/cash itself (withdrawn from bank account, credit union, etc.). This process will assist you in establishing the legitimacy (or illegitimacy) of the funds and in making the decision as to whether to proceed with the transaction.

In all instances the Designated Person should adopt and practise a risk based approach to source of funds, and sufficient questioning of the customer explanation should be conducted to allow you to document and record such an explanation that constitutes a reasonable explanation as to the source of the funds.

An example of such a scenario might be where a customer states the source of funds as 'savings' without further context (i.e. savings accrued from employment income). In this instance a risk based approach should be adopted and follow up questions should be asked that allow the Designated Person to record such an explanation that constitutes a reasonable explanation as to the source of the funds. Examples of such questions may include:

- what was the source of the savings?
- Was it withdrawn from a bank a/c?
- Why was the payment not made by bank draft or EFT?

(Note: these are examples and not intended to limit range of questions, the Designated Person should ask sufficient questions, including requesting supporting documentation to allow them to record a reasonable explanation as to the source of funds).

The Designated Person should note the customer’s response to these questions on their records to adequately reflect their work when they are inspected by an authorised officer from the AMLCU. Equally the responses/information gathered will better inform them in their assessment process of the customer/transaction for the risk of money-laundering or terrorist financing, whether they should proceed with the transaction, and whether they should submit an Suspicious Transaction Report to FIU and Revenue.

18 Appendix

Additional Useful Links

FIU Ireland:
www.fiu-ireland.ie/Home
Revenue STR:
www.revenue.ie/en/online-services/services/register-for-an-online-service/submit-suspicious-transaction-reports.aspx
CRO Register of Beneficial Ownership:
www.cro.ie/Registration/Beneficial-Ownership
Revenue CRBOT Central Register of Beneficial Ownership of Trusts:
www.revenue.ie/en/crbot/index.aspx
Central Bank of Ireland Beneficial Ownership for Certain Financial Vehicles:
www.centralbank.ie/regulation/anti-money-laundering-and-countering-the-financing-of-terrorism/beneficial-ownership-register
Department of Foreign Affairs (Sanctions):
www.dfa.ie/our-role-policies/ireland-in-the-eu/eu-restrictive-measures/
Financial Action Task Force (FATF):
www.fatf-gafi.org/en/home.html