

Criminal Justice (Money Laundering and Terrorist Financing) Act 2010

Guidelines

On the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

February 2012

Part I

These guidelines are structured in two parts. This Part (Part I) contains core guidance which provides generic guidance that is applicable to all financial services designated persons.

It is intended that Part II will set down additional supplemental guidelines for specific sectors. Any sectoral guidelines are incomplete on their own and must be read in conjunction with the core guidelines.

It is intended that the following will produce sectoral guidelines to supplement these core guidelines:

- Banking
- Investment Funds
- Stockbrokers
- Insurance
- Credit Unions
- Payment Institutions
- Bureaux de Change

Contents

SECTION I: BACKGROUND	4
A. ABOUT THIS GUIDANCE	4
B. INTRODUCTION TO THE LEGISLATION	5
C. WHAT IS MONEY LAUNDERING?	7
D. WHAT IS TERRORIST FINANCING?	11
E. DATA PROTECTION REQUIREMENTS IN RELATION TO AML	14
SECTION II: SCOPE	15
A. TO WHOM DOES THE ACT APPLY?.....	15
B. WHEN DOES THE CUSTOMER DUE DILIGENCE OBLIGATIONS OF THE ACT APPLY?	19
C. EXISTING CUSTOMERS	21
D. COMPETENT AUTHORITIES	24
SECTION III: ASSESSMENT AND MANAGEMENT OF RISK / RISK BASED APPROACH	26
A. INTRODUCTION	26
B. LEGISLATIVE BASIS.....	27
C. THE ROLE OF SENIOR MANAGEMENT.....	30
D. AML/CFT RISK POLICY AND PROCEDURES.....	32
E. CONDUCTING THE RISK ASSESSMENT.....	33
F. ASSESSING THE RISK OF TERRORIST FINANCING	37
G. OTHER FACTORS TO CONSIDER IN DESIGNING A RISK BASED APPROACH.....	37
H. SECTORAL NOTES	38
SECTION IV: CUSTOMER DUE DILIGENCE	39
A. WHAT IS CUSTOMER DUE DILIGENCE?	39
B. IDENTIFICATION AND VERIFICATION OF THE CUSTOMER'S IDENTITY.....	40
C. IDENTIFICATION AND VERIFICATION OF THE BENEFICIAL OWNER	45
D. WHEN MUST IDENTIFICATION AND VERIFICATION BE UNDERTAKEN?.....	48
E. OBTAINING INFORMATION ON THE PURPOSE AND NATURE OF THE BUSINESS RELATIONSHIP	49
F. CONDUCTING ONGOING MONITORING OF THE BUSINESS RELATIONSHIP	50
G. WHAT IS SIMPLIFIED CUSTOMER DUE DILIGENCE?	51
H. WHEN CAN SIMPLIFIED CUSTOMER DUE DILIGENCE BE APPLIED?	52
I. WHAT IS ENHANCED CUSTOMER DUE DILIGENCE?	55
J. ADDITIONAL CUSTOMER DUE DILIGENCE WHERE A CUSTOMER WHO IS AN INDIVIDUAL DOES NOT PRESENT IN PERSON (NON FACE-TO-FACE)	60
SECTION V: RELIANCE ON THIRD PARTIES TO UNDERTAKE DUE DILIGENCE	62
A. INTRODUCTION.....	62
B. FOR WHAT PURPOSE CAN THIRD PARTIES BE RELIED UPON?.....	63
C. WHAT PARTIES CAN BE RELIED UPON?	64
D. WHAT OVERSIGHT OF RELEVANT THIRD PARTIES MUST BE UNDERTAKEN?.....	65
E. CONDITIONS ATTACHING TO RELIANCE ON RELEVANT THIRD PARTIES	67
F. ONGOING MONITORING	68
G. RESPONSIBILITY FOR RECORD KEEPING AND PROVISION.....	69
H. GROUP INTRODUCTIONS	70
I. BUSINESS ACQUISITIONS.....	71
SECTION VI: INTERNAL POLICIES AND PROCEDURES	73

A. INTRODUCTION	73
B. WHAT DOES THE ACT REQUIRE?	73
C. SENIOR MANAGEMENT’S RESPONSIBILITIES AND THE ROLE OF THE MONEY LAUNDERING REPORTING OFFICER (MLRO)	77
SECTION VII: REPORTING OF SUSPICIOUS TRANSACTIONS.....	78
A. INTRODUCTION	78
B. WHAT DOES THE ACT REQUIRE?	78
C. TIMING OF REPORTS	79
D. KNOWLEDGE, SUSPICION AND REASONABLE GROUNDS FOR SUSPICION	79
E. WHEN REPORTS DO NOT HAVE TO BE MADE	82
F. THE INTERNAL REPORTING PROCESS.....	83
G. PROCESS FOR REPORTING TO THE FIU AND REVENUE COMMISSIONERS.....	85
H. REPORTING OF SUSPICIOUS TRANSACTIONS	86
I. TIPPING OFF	87
J. DIRECTIONS AND ORDERS.....	90
SECTION VIII: RECORDKEEPING	92
A. INTRODUCTION.....	92
B. WHAT RECORDS SHOULD BE MAINTAINED	94
C. POSSIBLE FORMATS IN WHICH RECORDS MAY BE KEPT.....	97
D. LOCATION.....	97
SECTION IX: TRAINING	97
A. INTRODUCTION	97
B. WHAT DOES THE ACT REQUIRE?	97
C. WHAT SHOULD DESIGNATED PERSONS DO?.....	98
D. ADDITIONAL ISSUES FOR CONSIDERATION BY STAFF	100
SECTION X: ENFORCEMENT	102
APPENDIX 1.....	115
Guidance On Identification And Verification Procedures	115
APPENDIX 2.....	128
documentation (and documentation supporting financial inclusion).....	128

Ref	SECTION I: BACKGROUND
Art = Directive S = Section of the Act	A. ABOUT THESE GUIDELINES
	<p>1. These guidelines have been drafted jointly by various sectors of the financial services industry.</p> <p>The guidelines are stated to be for the purpose of guiding designated persons on the application of Part 4 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010. While these guidelines have not been approved under Section 107 of the Act, the Central Bank will have regard to these guidelines in assessing compliance by designated persons with the Act.</p> <p>Part 4 of the Act sets out the obligations of designated persons in relation to customer identification, verification and monitoring as well as enhanced CDD, suspicious transaction reporting etc. It also contains a number of criminal offences for a failure on the part of a designated person to meet those obligations. The offences are punishable by terms of imprisonment of up to five years and unlimited fines. A regulated financial service provider may also be subject to the administrative sanctions procedure of the Central Bank.</p> <p>The guidelines are designed to guide designated persons on the application of the relevant provisions of the Act. The guidelines do not constitute secondary legislation and designated persons must always refer directly to the Act when ascertaining their statutory obligations. The guidelines are subordinate to the Act.</p> <p>The guidelines are not intended to be exhaustive nor to set the limits for the steps to be taken by designated persons in working to prevent money laundering or terrorist financing. The Act involves a combination of risk-based and rules-based approaches to the prevention of money laundering and terrorist financing; the general approach of designated persons should be to take the steps warranted by the risk of money laundering in any given circumstance.</p> <p>The guidelines, also reflect the wider context in which the Act was developed, namely the Third Anti-Money Laundering Directive 2005/60/EC and Implementing Directive 2006/70/EC and Ireland’s membership of the Financial Action Task Force, EU, UN, Council of Europe, and the OECD all of which play a role in the prevention of money laundering and terrorist financing.</p> <p>Words or expressions used in the guidelines and also in the Act have the same meaning unless the contrary intention appears.</p>

	<p>2. In addition to providing guidance on the requirements of the Act, and how designated persons covered by its provisions can best meet their obligations, the guidelines also;</p> <ul style="list-style-type: none"> - Indicate good standards of industry practice in Anti-Money Laundering/Counter Terrorist Financing (“AML/CTF”) procedures through a proportionate, risk-based approach; and - Assist designated persons to design and implement the systems and controls necessary to mitigate the risk of the designated person being used in connection with money laundering and the financing of terrorism. <p>In considering the content of the guidelines, it is important that designated persons appreciate that the board of directors (or equivalent) is ultimately responsible for ensuring that the designated person maintains an effective internal AML/CTF control structure. The board of directors and senior management must create a culture of compliance, ensuring that the designated person's policies, procedures and processes are designed to limit and control risks of money laundering and terrorist financing and are fully consistent with the law. The board of directors and senior management should be fully engaged in decision making processes and take ownership of the risk-based measures adopted since they will be held accountable/liable to fines and/or imprisonment if the approach is found to be inadequate. Further detail on the role and responsibilities of senior management is to be found in Sections III and VI.</p>
	<p>3. The guidelines are structured in two parts. This document, Part I, contains core guidance which provides generic guidance that is applicable to all financial services designated persons. It is intended that Part II will set down additional supplemental guidelines for specific sectors. Any sectoral guidelines are incomplete on their own and must be read in conjunction with the core guidelines.</p>
	<p>4. The guidelines use the term “must”, “shall”, “are required to” or “are obliged to” to indicate a legal or regulatory requirement. The term “should” is used to indicate ways in which the statutory and regulatory requirements may be satisfied.</p> <p>Where definitions or sections of the Act are used in the guidelines, these will appear in italicised text.</p>
B. INTRODUCTION TO THE LEGISLATION	
	<p>5. The guidelines are based on the 2010 Act , which transposes the requirements of the Third Anti-Money Laundering Directive 2005/60/EC and Implementing Directive 2006/70/EC, and which repeals certain sections¹ of the Criminal Justice Act, 1994 (as amended) (“CJA 1994”) and the statutory instruments which are detailed in Schedule I of the 2010 Act.</p>
	<p>6. The key features of the Act are as follows:</p> <ul style="list-style-type: none"> - The obligation on designated persons to apply Customer Due Diligence (CDD) procedures to their customers in specific

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

<p>S. 54(2)(a)</p> <p>S.49</p> <p>S17 – 21</p> <p>Chapter 9</p>	<p>circumstances, which not only require the initial identification and verification of identity, but also require the ongoing monitoring of the business relationship with customers and reporting of any suspicions of money laundering or terrorist financing;</p> <ul style="list-style-type: none"> - The obligation to also identify and take measures reasonably warranted by the risk of money laundering or terrorist financing to verify beneficial owners of customers; - In line with a risk-based approach, the Act sets down that; <ul style="list-style-type: none"> o designated persons shall adopt policies and procedures to prevent and detect the commission of money laundering and terrorist financing, including for the assessment and management of the risks; o simplified customer due diligence (“SCDD”) procedures may be applied to specified products and/or specified customer types; o enhanced customer due diligence is required for certain types of business or customers (such as correspondent banking relationships and politically exposed persons) and is also provided for in cases where a designated person considers that there is a heightened risk of money laundering or terrorist financing. - Designated persons are permitted to rely on certain relevant third parties to meet the CDD requirements of the Act, but not as a means of fulfilling their obligation to conduct ongoing monitoring of business relationships. Where designated persons choose to place reliance on relevant third parties to conduct elements of CDD, ultimate responsibility for ensuring compliance with the full CDD obligation still resides with those designated persons; - Designated persons covered by the Act are obliged to promptly report suspicions of money laundering or terrorist financing to the Garda Síochána (the FIU) and to the Revenue Commissioners; - A designated person who knows or suspects, that an investigation is being contemplated or carried out, is prohibited from making any disclosure that is likely to prejudice the investigation; - There are explicit provisions relating to the powers of An Garda Síochána to issue directions, and of the District Court to make orders, not to provide services or carry out transactions while the Gardai carry out preliminary investigations as to whether or not giving effect to the service or transaction might comprise or assist in money laundering or terrorist financing; - There are explicit provisions relating to the basis for monitoring by the competent authority; - There are explicit provisions on the obligations of designated persons in relation to recordkeeping, staff training and the maintenance of appropriate procedures and controls; and - There are new provisions imposing an authorisation requirement on providers of trust and company services. Applications for authorisation must be made to the Anti-Money Laundering Compliance Unit within the Department of Justice and Equality.
---	--

S. 6-11

C. WHAT IS MONEY LAUNDERING?

7. “Money Laundering Offences” are provided for in Part 2 of the Act. Part 2 also contains the key terms “criminal conduct” and “proceeds of criminal conduct”.

In essence, the activity of money laundering involves the intentional or reckless conversion of tainted property, generated from “criminal conduct”, into clean property, so that the criminal origin of the tainted property is difficult to trace.

“Criminal conduct” is defined in the Act as conduct that constitutes an offence or conduct occurring in a place outside the State that constitutes an offence under the law of the place and would constitute an offence if it were to occur in the State. This definition encompasses all offences whether minor or serious, summary or indictable.

The Act’s definition of “proceeds of criminal conduct” (“*any property that is derived from or obtained through criminal conduct, whether directly or indirectly*”) effectively means that ‘self-laundering’ is criminalised just in the same way as the laundering of the proceeds of the criminal conduct of a third party.

There are three recognised stages in the money laundering process:

Placement involves placing the proceeds of criminal conduct in the financial system.

Layering involves converting the proceeds of criminal conduct into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds. This stage may involve transactions such as the buying and selling of stocks, commodities or property.

Integration involves placing the laundered proceeds back in the economy to create the perception of legitimacy.

Credit and Financial Institutions, the subject of these guidelines, are designated persons with specific obligations under Part 4 of the Act because their normal activities expose them to the risk that their businesses will be used by launderers to place, layer or integrate the proceeds of criminal conduct.

While credit or financial institutions may never form a clear intent to conceal or convert the proceeds of criminal conduct, they may nonetheless be exposed to criminal liability under the Act as a consequence of the passive acquisition of tainted funds.

<p>S.7(4)</p> <p>S. 7(5)</p>	<p>content of which one might not care to have;</p> <ul style="list-style-type: none"> - Knowledge of circumstances which would indicate the facts to an honest and reasonable person; and - Knowledge of circumstances which would put an honest and reasonable person on inquiry and failing to make the reasonable inquiries which such a person would have made. <p>The Act states explicitly at <i>section 7(4)</i> that knowing or believing that property is the proceeds of criminal conduct includes a reference to knowing or believing that the property probably comprises the proceeds of criminal conduct.</p> <p>The Act makes express provision in relation to recklessness:</p> <p>For the purposes of section 7(1) and (2), section 7(5) provides “a person is reckless as to whether or not property is the proceeds of criminal conduct if the person disregards, in relation to property, a risk of such a nature and degree that, considering the circumstances in which the person carries out any act referred to in subsection (1) or (2), the disregard of that risk involves culpability of a high degree.”</p>
<p>S.8</p>	<p>10. The Act also details an offence, of money laundering outside the State, where certain conditions are met. A person who, in a place outside the State, engages in conduct that would, if the conduct occurred in the State, constitute an offence under <i>section 7</i> of the Act, commits an offence if certain circumstances apply. Full detail is covered in <i>section 8</i> of the Act but designated persons should note that the circumstances in question relate generally to -</p> <ul style="list-style-type: none"> (i) conduct on board certain ships associated with the State or aircraft registered in the State, (ii) conduct that constitutes an offence in the place in which it occurred and was engaged in by an Irish citizen or resident or a company registered in Ireland, (iii) a request for a person’s surrender under the Extradition Act 1965 has been made and finally refused or (iv) a European Arrest Warrant has been received and the courts have decided not to accede to the surrender request contained therein.
<p>S. 16</p>	<p>11. In relation to offences committed outside the State, it is important to note that <i>section 16</i> of the Act provides that this jurisdiction regards an offence under the law of a place outside the State as including an offence relating to taxes, duties, customs or exchange regulation. This is explicitly stated in the Act because certain jurisdictions may regard a revenue-related offence committed abroad as not constituting a criminal offence.</p>

S. 7(7)	<p>12. <i>Section 7(7)</i> of the Act provides legal protection where a person breaches a provision of <i>section 7</i> so long as the person does so in accordance with a direction, order or authorisation given under Part 3 of the Act, for example by the Garda or a judge or, having made a report in relation to the property, breaches <i>section 7</i> in accordance with <i>section 42</i>.</p>
S.11 and S.54	<p>13. In the context of credit or financial institutions obtaining information or knowledge of circumstances “which would put an honest and reasonable person on inquiry” <i>section 11</i> of the Act is of note in that it sets out scenarios in which it “is reasonable to conclude that property is the proceeds of criminal conduct” where:</p> <ul style="list-style-type: none"> - the value of property being dealt with by a person is out of proportion to the normal income and expenditure of that person; - the price of goods or services is out of proportion to the market value of those goods or services; - false names are used in transactions; - the person dealing with the property purports to be acting on behalf of a third party but has not provided An Garda Síochána with information necessary to identify that third party; - an accused has concealed or disguised the true nature, source, location, disposition, movement or ownership of the property, or any rights relating to the property and the accused has no reasonable explanation for that concealment or disguise.
S.7 – S.10	<p>While the section provides for presumptions that apply in criminal proceedings for the principal money laundering offences, those statutory presumptions can be taken into account and referred to by credit and financial institutions engaged in training their staff pursuant to their obligations under Chapter 6 of the Act.</p>
S.11(2)	<p>Under <i>Section 11(2)</i> of the Act, where an accused has acted in a way which it is reasonable to believe that he knew, believed or was reckless as to whether property was the proceeds of criminal conduct, the accused will be presumed to have known, believed or been reckless in that regard unless a court or jury is satisfied otherwise by the accused.</p> <p>Given the international nature of modern financial services, <i>sections 9</i> and <i>10</i> (and <i>section 8</i> to a lesser degree) may be of particular relevance to the Money Laundering Reporting/Compliance Officers of credit and financial institutions.</p> <p><i>Section 9</i> of the Act provides that it is an offence for a person to attempt to</p>

	<p>commit an offence under section 7(1) of the Act outside the State.</p> <p>In addition, <i>section 10</i> of the Act provides for a separate offence of aiding, abetting, counselling or procuring, in a place outside the State, the commission of an offence in the State.</p> <p>To give non-exhaustive examples:</p> <ul style="list-style-type: none"> - Staff of a corporate entity registered in Ireland could commit, while abroad, acts which constitute an offence under Section 7. - Regardless of residence or nationality, a person may while abroad give instructions (in relation to assets within the State) which could constitute an attempt to launder within the State. - Similarly a person outside the jurisdiction could, by giving instructions relating to assets within the State, aid, abet, counsel or procure the commission of an offence under Section 7.
	<p>14. Tax offences are not in a special category; the proceeds of a tax offence, like the proceeds of the other examples of criminal activity, may be the subject of money laundering offences under the Act. Consequently, where the suspicion arises in the course of the business relationship that the customer or other person² is evading tax, it should be reported in accordance with the designated person’s obligations under <i>section 42</i> of the Act. However, in fulfilling its requirements under the Act a designated person may, unless there are contrary indications, reasonably assume that a customer has discharged his/her tax liabilities. There is no positive obligation on the designated person to verify whether the customer has or has not done so.</p>

	<p>D. WHAT IS TERRORIST FINANCING?</p>
	<p>15. It is important to distinguish between:</p> <ul style="list-style-type: none"> - Terrorist financing, as it is addressed in the Act; and - The financial sanctions regime that imposes restrictive measures, directed against persons and entities, contained in EU Regulations drawn up within the framework of the EU Common Foreign and Security Policy. The requirement to monitor against various sanctions lists is not included within the Act or these guidelines. Please refer to separate guidelines on the subject of Financial Sanctions on the Central Bank and Department of Finance websites.
<p>Art 1 (4) S.13</p>	<p>16. “Terrorist financing” means an act that constitutes an offence under <i>section</i></p>

² For example, a person who is seeking to establish a business relationship or to undertake an occasional transaction.

<p>CJ(TO)Act 2005 S.13(1)(a)</p> <p>CJ(TO)Act 2005 S.13(1)(b)</p>	<p>13 of the Criminal Justice (Terrorist Offences) Act 2005.</p> <p><i>Section 13 provides:</i></p> <p><i>“a person is guilty of an offence if, in or outside the State, the person by any means, directly or indirectly, unlawfully and wilfully provides, collects or receives funds intending that they be used or knowing that they will be used, in whole or in part in order to carry out—</i></p> <p><i>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</i></p> <p><i>b) an act (other than one referred to in paragraph (a)) —</i></p> <p><i>i. That is intended to cause death or serious bodily injury to a civilian or to any other person not taking an active part in the hostilities in a situation of armed conflict, and</i></p> <p><i>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.”</i></p>
	<p>17. The objective of terrorist activity is to intimidate a population or compel a government to do something. This is done by intentionally killing, harming or endangering people, causing property damage or by disrupting services, facilities or systems.</p> <p>There is little difference between terrorists and other criminals in their use of the financial system. Like criminal groups, terrorist groups seek to build and maintain financial infrastructures to support their activities. For this purpose, they seek different sources of funding but also seek to obscure the links to the sources of the funds and the terrorist activities supported.</p> <p>Use of the financial system ensures that the funds can be made available to obtain the equipment or services needed to commit acts of terrorism.</p> <p>However, there are two key differences between terrorist property and criminal property more generally:</p> <ul style="list-style-type: none"> - The sums needed to fund terrorist attacks are not always large and the associated transactions are not necessarily complex; - Terrorists can be funded from legitimately obtained income, including charitable donations, and it is difficult to identify the stage at which legitimate funds become terrorist property.
	<p>18. Terrorist organisations can, however, require quite significant funding and property to resource their infrastructure. Terrorism may be state-sponsored though this source of funding is believed to have declined in recent years. Terrorist groups may also resort to criminal acts such as kidnapping and extortion, which serve the dual purpose of providing needed financial</p>

	<p>resources while at the same time furthering the main terrorist objective of intimidating a target population.</p> <p>Terrorist groups may also resort to tobacco and fuel smuggling, fraud, theft, robbery, and drug trafficking to generate funds.</p> <p>Terrorist groups also generate legitimately earned income. Groups collect subscriptions, they sell publications, they organise cultural and social events, and they make appeals to the community they purport to represent. Such fundraising initiatives may be carried out in the name of charitable organisations and donors may genuinely understand they are funding a legitimate cause. Alternatively non-profit organisations or charitable organizations may be infiltrated so as to divert a portion of donations to terrorist activities.</p>
S.35(3)	<p>Given that sums needed to fund terrorist attacks may not necessarily be large or the associated transactions complex, ongoing monitoring of transactions and scrutiny of the source of wealth or of funds for those transactions may be key to identifying patterns that may indicate the financing of terrorism.</p> <p>Diligent recordkeeping will serve as the foundation for meeting any information requests from the Garda Síochána in respect of terrorist financing. Further detail on record-keeping requirements is available in Section VIII of this Guidance.</p> <p>Designated persons should pay particular attention to their responsibilities under Regulation (EC) No. 1781/2006 on information on the payer accompanying the transfer of funds. This Regulation was developed with the objectives of preventing terrorists from having unfettered access to wire transfers for moving their funds and for detecting such misuse when it does occur. To the extent that Regulation 1781/2006 is applicable, the required information in respect of wire transfers should be obtained, recorded and available to law enforcement and the Central Bank.</p>
S.42(1) and S.(5)	<p><i>“Nothing limits the circumstances in which a designated person may have reasonable grounds ...to suspect that another person has committed an offence of money laundering or terrorist financing”</i>. Where such suspicions arise designated persons are obliged to report the suspicious activities of customers or other persons to the FIU.</p>
S.17(1)	<p>Reports made may prompt the making of a 7-day direction or a 28-day court order not to carry out a specified service or transaction for a customer where such a direction is <i>“reasonably necessary to enable the Garda Síochána to carry out preliminary investigations into whether or not there are reasonable grounds to suspect that the service or transaction would, if it were to proceed, comprise or assist in money laundering or terrorist financing”</i>.</p>

	<p>The screening of customers against relevant financial sanctions lists is another key aspect of combating terrorism. Guidance on implementing the financial sanctions regime is approved by the Money Laundering Steering Committee.</p>
	<p>E. DATA PROTECTION REQUIREMENTS IN RELATION TO AML</p>
	<p>19. Firms shall consider the requirements under the Data Protection Acts 1988 and 2003 when implementing the requirements under the Act. In particular, consideration should be given to the eight principles of data protection legislation in relation to the following;</p> <ul style="list-style-type: none"> - obtaining and processing documentation and information applying to CDD obligations, including enhanced due diligence measures where required; - the measures or sources used to verify customer data and where consent obligations may apply ; - the retention of documentation and information required under the Act in relation to customer and transactional information ; - training obligations; and - agreements and contracts put in place with third parties acting for and on your behalf <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p><u>Eight principles of Data Protection</u></p> <ol style="list-style-type: none"> 1. Obtain and process information fairly. 2. Keep it only for one or more specified, explicit and lawful purposes. 3. Use and disclose it only in ways compatible with these purposes, 4. Keep it safe and secure. 5. Keep it accurate, complete and up-to-date. 6. Ensure that it is adequate, relevant and not excessive. 7. Retain it for no longer than is necessary for the purpose or purposes. 8. Give a copy of his/her personal data to the individual, on request. </div> <p>Designated persons should ensure that personal data is only used for the purpose for which it was obtained as stated in the Data Protection Acts and is not used for other purposes without prior consent.</p>

	SECTION II: SCOPE
	A. TO WHOM DOES THE ACT APPLY?
<p>S. 25 (1)</p> <p>Directive 2006/48/EC Annex 1</p>	<p>20. “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—</p> <ul style="list-style-type: none"> a) a credit institution, except as provided by subsection (4); b) a financial institution, except as provided by subsection (4); c) an auditor, external accountant or tax adviser; d) a relevant independent legal professional; e) a trust or company service provider; f) a property service provider; g) a casino; h) a person who effectively directs a private members’ club at which gambling activities are carried on, but only in respect of those gambling activities; i) any person trading in goods, but only in respect of transactions involving payments to the person in cash of a total of at least €15,000 (whether in one transaction or in a series of transactions that are or appear to be linked to each other); or j) any other person of a prescribed class.
S.25(6)	<p>Note that Irish branches of credit or financial institutions authorised in another Member State are also designated persons under the Act.</p> <p>It is also important for a designated person to note the prescribed class referred to at (j) above. This relates to the Minister’s power under section 25(7) of the Act to prescribe a class of persons as designated persons within the meaning of the Act. Designated persons and persons involved with the industry should remain alert to the possibility that a designation pursuant to section 25(7) of the Act could affect their legal obligations.</p> <p>21. “Credit institution” means –</p> <ul style="list-style-type: none"> a) a credit institution within the meaning of Article 4(1) of the Recast Banking Consolidation Directive (including Credit Unions), or b) An Post in respect of any activity that it carries out, whether as principal or agent, that would render it, or a principal for whom it is an agent, a credit institution as a result of the application of paragraph (a). <p>22. “Financial institution” means –</p> <ul style="list-style-type: none"> (a) an undertaking that carries out one or more of the activities listed in points 2 to 12, 14 and 15 of Annex I to the Recast Banking Consolidation Directive or foreign exchange services, but does not include an undertaking— <p>(i) that does not carry out any of the activities listed in</p>

	<p><i>those points other than one or more of the activities listed in point 7, and</i></p> <p><i>(ii) whose only customers (if any) are members of the same group as the undertaking,</i></p> <p><i>(b) an insurance company that carries out the activities covered by the Life Assurance Consolidation Directive and is authorised in accordance with that Directive,</i></p> <p><i>(c) a person, other than a person falling within Article 2 of the Markets in Financial Instruments Directive, whose regular occupation or business is—</i></p> <p><i>(i) the provision to other persons of an investment service, within the meaning of that Directive, or</i></p> <p><i>(ii) the performance of an investment activity within the meaning of that Directive,</i></p> <p><i>(d) an investment business firm within the meaning of the Investment Intermediaries Act 1995 (other than a nonlife insurance intermediary within the meaning of that Act),</i></p> <p><i>(e) a collective investment undertaking that markets or otherwise offers its units or shares,</i></p> <p><i>(f) an insurance intermediary within the meaning of the Insurance Mediation Directive (other than a tied insurance intermediary within the meaning of that Directive) that provides life assurance or other investment related services, or</i></p> <p><i>(g) An Post, in respect of any activity it carries out, whether as principal or agent—</i></p> <p><i>(i) that would render it, or a principal for whom it is an agent, a financial institution as a result of the application of any of the foregoing paragraphs,</i></p> <p><i>(ii) that is listed in point 1 of Annex I to the Recast Banking Consolidation Directive, or</i></p> <p><i>(iii) that would render it, or a principal for whom it is an agent, an investment business firm within the meaning of the Investment Intermediaries Act 1995 (other than a non-life insurance intermediary within the meaning of that Act) if section 2(6) of that Act did</i></p>
--	---

<p>Art 31 (1)</p>	<p>26. Money laundering and terrorist financing are international problems and the efforts to combat them are global. Where an Irish credit or financial institution has branches or subsidiaries in countries outside the EU / EEA where AML/CTF legislation may be deficient, the Act requires the institution, where possible, to adopt EU standard AML-CTF procedures throughout the group.</p>
<p>S.57 (1)</p>	<p>Accordingly the Act provides:</p> <p><i>“A credit institution or financial institution that is a designated person and incorporated in the State shall ensure that any branch of the institution, or any subsidiary of the institution that is also a credit institution or financial institution, in a place other than a Member State, applies requirements equivalent to those specified in Chapters II and IV of the Third Money Laundering Directive”.</i></p>
<p>S.57(2)</p>	<p><i>If the place concerned does not permit the application of requirements equivalent to those specified in Chapters II and IV of the Third Money Laundering Directive, the designated person shall—</i></p> <ul style="list-style-type: none"> <i>a) Inform the competent authority for the designated person, and</i> <i>b) Apply measures, determined in consultation with the competent authority to deal with the risk of money laundering or terrorist financing arising from the absence of those requirements.</i>
<p>S.57 (3)</p>	<p><i>A credit institution or financial institution that is a designated person and incorporated in the State shall communicate any policies and procedures that it has adopted to any branch or subsidiary that is in a place other than a Member State.”</i></p>
<p>S.54(1)</p>	<p>Section 57 of the Act applies to branches and subsidiaries in non-Member States only and requires the adoption of group wide standards where possible. Where it is not possible to apply group wide standards to non-Member State branches or subsidiaries, for example, where local requirements require deviation from the group standard, the Central Bank must be consulted in this regard. Geography-driven deviations from an institution’s standard AML-CTF procedures in these circumstances should be documented in detail. Failure to comply with the requirements of section 57 is an offence which carries a penalty of up to 5 years imprisonment and/or an unlimited fine.</p>

	<p>B. WHEN DO THE CUSTOMER DUE DILIGENCE OBLIGATIONS OF THE ACT APPLY?</p>
<p>Art 7 S.33 (1)</p>	<p>27. A designated person shall apply CDD measures:</p> <ul style="list-style-type: none"> a) <i>prior to establishing a business relationship with the customer;</i> b) <i>prior to carrying out an occasional transaction with, for or on behalf of a customer, or assisting the customer to carry out an occasional transaction. [An “occasional transaction” in relation to a customer of a designated person means a single transaction, or a series of transactions that are, or appear to be linked to each other, where,</i> <ul style="list-style-type: none"> i. <i>The designated person does not have a business relationship with the customer, and</i> ii. <i>The total amount of money paid by the customer in a single transaction or series of transactions is greater than €15,000.]</i> c) <i>prior to carrying out any service for the customer, if the person has reasonable grounds to believe that there is a real risk that the customer is involved in, or the service sought by the customer is for the purpose of, money laundering or terrorist financing, based on any of the following, or other, circumstances:</i> <ul style="list-style-type: none"> i. <i>the customer, or the type of customer, concerned;</i> ii. <i>if the person has a business relationship with the customer, the type of business relationship concerned;</i> iii. <i>the type of service or any transaction or product in respect of which the service is sought;</i> iv. <i>the purpose (or the customer’s explanation of the purpose) of the service or any transaction or product in respect of which the service is sought;</i> v. <i>the value of any transaction or product in respect of which the service is sought;</i> vi. <i>the source (or the customer’s explanation of the source) of funds for any such transaction or product, or</i> d) <i>prior to carrying out any service for the customer if:</i> <ul style="list-style-type: none"> i. <i>the person has reasonable grounds to doubt the veracity or adequacy of documents (whether or not in electronic form) or information that the person has previously obtained for the purpose of verifying the identity of the customer, whether obtained under this section or section 32 of the Criminal Justice Act 1994 (“the 1994 Act”) prior to its repeal by the Act or under any administrative arrangements that the person may have applied before section 32 of the 1994 Act operated in relation to the person, and</i> ii. <i>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</i>

	<i>identity of the customer.</i>
Art 3 (9) S.24 (1)	28. A “business relationship”, <i>in relation to a designated person and a customer of the person, means a business, professional or commercial relationship between the person and the customer that the person expects to be ongoing.</i>
	<p>29. Examples of features of an arrangement that could suggest it is a “business relationship” might include:</p> <ul style="list-style-type: none"> - The establishment of the relationship involves the signing of a contract of engagement to provide services; - It is expected that services will be provided to the customer for a period of time whether that period is determined or not at the outset of the arrangement; - The total amount of any payments to be made by any person to any other person in the course of the arrangement is not known or capable of being ascertained at the outset; - It is expected when any transaction is undertaken that it will be followed by further transactions; - The customer seeks the provision of services on a frequent or regular basis; or - The establishment of the relationship involves a formal account opening process including the opening of an internet e-money/payments account where terms & conditions are accepted by electronic means.
	<p>30. Examples of features that could suggest that a transaction is an “occasional transaction” include:</p> <ul style="list-style-type: none"> - A single foreign currency transaction or an isolated instruction to purchase shares and the shares are immediately forwarded to the customer; - At the time the transaction is undertaken there is no intention or indication that a further transaction will be undertaken; - The total sum involved in the transaction is known at the outset; or - The proceeds of a once off transaction are reinvested for the benefit of the customer, irrespective of the amount involved.
	<p>31. Examples of features that could suggest occasional transactions may be “linked”:</p> <ul style="list-style-type: none"> - They are for the benefit of the same customer or beneficial owner; - They occur within a reasonably close timeframe; - They are for the benefit of two customers that the designated person knows to have close links (e.g. an individual and a company in which the individual is a beneficial owner); - They are for the benefit of more than one customer but come from the same source; or - They are for the benefit of one customer but come from more than one source in a pattern that may indicate linkage.

	<p>32. There is no explicit requirement in the Act that designated persons must provide additional computer and administrative systems specifically to identify and aggregate linked transactions. However, designated persons are required to apply CDD measures under S.33(1) prior to carrying out an occasional transaction with, for or on behalf of the customer.</p> <p>Failure to comply with the requirements of section 33 is an offence which carries a penalty of up to 5 years imprisonment and/or an unlimited fine.</p>
	<p>C. EXISTING CUSTOMERS</p>
	<p>33. Designated persons must carry out CDD before establishing a business relationship with a customer. In effect designated persons should have reliable CDD information for an existing customer prior to carrying out any service for such a customer. Designated persons should monitor their dealings with existing customers, keep CDD information up to date as warranted by the overall knowledge the person has of the customer, the nature of the business relationship and the risk of money laundering or terrorist financing.</p> <p>CDD requirements are addressed throughout Part 4 of the Act.</p> <p>Section 33 (1) (c) requires CDD measures to be carried out prior to carrying out any service for the customer, if the person has reasonable grounds to believe that there is a real risk that the customer is involved in, or the service sought by the customer is for the purpose of, money laundering or terrorist financing, based on any of the following, or other, circumstances:</p> <ul style="list-style-type: none"> i. the customer, or the type of customer, concerned; ii. if the person has a business relationship with the customer, the type of business relationship concerned; iii. the type of service or any transaction or product in respect of which the service is sought; iv. the purpose (or the customer’s explanation of the purpose) of the service or any transaction or product in respect of which the service is sought; v. the value of any transaction or product in respect of which the service is sought; vi. the source (or the customer’s explanation of the source) of funds for any such transaction or product <p>Section 33(1)(d) of the Act provides that CDD must be carried out prior to carrying out any service for a customer where:</p> <ul style="list-style-type: none"> (i) the person has reasonable grounds to doubt the veracity or adequacy of documents (whether or not in electronic form) or information that the person has previously obtained for the purpose of verifying the identity of the customer, whether obtained under this section or section 32 of the Criminal Justice Act 1994 (“the 1994 Act”) prior to its repeal by this Act or under any administrative arrangements that the person may have applied before section 32 of the 1994 Act operated in relation to the person, and

	<p>(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.</p> <p>In the event that both of the elements of section 33(1)(d) occur, then the designated person must apply the customer due diligence measures specified in section 33(2) and, where applicable, 33(4). The test for “reasonable grounds to doubt the veracity or adequacy of documents” is an objective test. In other words it is not the subjective opinion of the designated person which is important, rather it is a question of whether there are, on objective consideration, grounds to doubt the veracity or adequacy of CDD information. Designated persons should also bear in mind that other CDD measures may also be applicable in respect of existing customers, for example, section 37 of the Act. Other CDD measures will always be applicable in respect of existing customers, for example, the ongoing monitoring requirement contained in section 35(3) of the Act. Designated persons should refer to Section IV of these Guidelines for guidance on these other aspects.</p>
	<p>34. Under section 33(1)(d) of the Act, designated persons are obliged to conduct CDD for existing customers where they have reasonable grounds to doubt the <i>veracity</i> or <i>adequacy</i> of <i>documents or information</i> previously obtained. Therefore, either documentation <u>or</u> information can be used by a designated person to satisfy itself that it meets its obligations under this section. Where new documentation is sought or obtained, its acceptability should be considered by reference to the risk-based documentation classifications set out in Appendix 1 and, if applicable, Appendix 2 to the core guidelines. Each designated person should satisfy itself that where information is used for these purposes, that it is reliable, documented and capable of being evidenced to the Central Bank, for example a documented history of customer communications may satisfy this requirement.</p> <p>Designated persons should keep CDD information for existing customers up to date as warranted by the overall knowledge the person has of the customer, the nature of the business relationship and the risk of money laundering or terrorist financing. Documentation or information that had been previously obtained in respect of an existing customer but which no longer meets the precise recommendations under the “Authenticity of Documentation” section of Appendix 1, should not automatically be considered inadequate or unreliable for the purposes of section 33(1)(d) of the Act.</p> <p>Designated persons should consider all relevant aspects of the information held on file.</p>
	<p>35. The Act also requires designated persons to apply the measures contained in section 33(2)(b) i.e. identify the beneficial owners connected with the customer or service concerned, which includes existing customers, where both of the elements of section 33(1)(d) occur.</p>
	<p>36. The Act requires CDD to be applied to existing customers prior to carrying out any services, where section 33 (1) (c) applies (reasonable grounds to believe there is a risk of money laundering or terrorist financing) or where there are</p>

	<p>doubts concerning previously obtained customer identification data. Unless there are reasons to doubt the processes and procedures that the designated person has implemented in respect of its obligations under the Act, a designated person may, on reasonable grounds, and in the absence of any evidence to the contrary, determine that it is unlikely that such a doubt will arise in respect of customers that have been taken on after the Act became law. However, the basis for such a determination must be recorded and capable of being evidenced to the Central Bank of Ireland. In all other cases, the designated person must assess whether a doubt arises prior to carrying out any services and if so, apply the requirements under Section 33(1) of the Act. In determining their approach to this assessment, designated persons should take into account the level of risk posed by the service and the customer.</p>
	<p>37. Designated persons should develop and implement a framework containing one or more trigger events which will provide an opportunity to require customers to provide documentation or information meeting the requirements under Section 33(1) of the Act. Designated persons should decide which trigger events are appropriate to its business on a risk basis and should ensure that the approach is included in its AML/CTF policies and procedures in accordance with Section 54(2). Designated persons should develop their own criteria as appropriate to their business. The following are examples of relevant trigger events, but the list should not be regarded as exhaustive or mandatory:</p> <ul style="list-style-type: none"> - A customer requests the designated person to provide a new professional service; - A customer opens a new type of account or seeks to invest in a new type of investment product; - The customer's account has been inactive for a certain period of time where this is unusual for the nature of the service being provided; - A designated person's risk-based assessment of its business provides grounds to move the customer in question to a higher-risk category, calling into question the adequacy of documentation or information previously obtained; - Doubt has arisen in the normal course of business in relation to previous documentation or information, if any, provided in relation to the customer; - Doubt has arisen in the normal course of business as to whether the customer, contrary to previous information, is acting on his/her own behalf; - Where the customer had previously only entered into an occasional transaction with the designated person and CDD information had not been collected, the customer now commences a business relationship; - The output from the designated person's transaction monitoring process has identified behaviour not in keeping with the customer's profile;

	<ul style="list-style-type: none"> - A transaction of significance takes place; - Customer documentation standards change substantially; - There is a material change in the way that the account is operated; - Information is provided by a third party or the authorities or through internal investigation that warrants a review and, potentially, a change of risk rating; - It is discovered that a customer in a lower risk category is party to a transaction within a facility that is deemed to be high risk. In this instance a review of the assignment to the lower category is required to determine whether the risk rating needs to be aligned.
	<p>38. Where a customer fails to supply the required documentation or information either on the occurrence of a trigger event or in other circumstances, the designated person should not provide that new service and the business relationship with the customer should be discontinued for so long as that failure continues. Designated persons should take an objective approach when considering what constitutes a failure to provide documentation or information in any particular situation. There may be circumstances where it is reasonable to delay discontinuing a business relationship while the designated person facilitates the customer’s efforts to rectify the failure. The reasonableness of such a delay will vary depending on the circumstances of each case. Where a customer refuses to provide requested documentation or information then the business relationship should be discontinued once the customer has been warned of the potential implications and given time to respond accordingly.</p>
	<p>39. In addition, designated persons should also consider on a risk basis how existing services should be treated and should be aware of their obligations in respect of tipping off the customer. Designated persons should also decide if it would be appropriate to make a suspicious transaction report in accordance with section 42 in such circumstances.</p>
	<p>D. COMPETENT AUTHORITIES</p>
<p>Art 37 S.60 (2)</p>	<p>40. The Act provides that competent authorities shall effectively monitor and take the necessary measures with a view to ensuring compliance by designated persons with the obligations imposed on designated persons as follows:</p> <ul style="list-style-type: none"> - For credit and financial institutions – the Central Bank; - For auditors, external accountants, tax advisers or Trust or Company Service Providers who are members of a designated accountancy body – the designated accountancy body of which they are a member; - For solicitors - the Law Society of Ireland; - For barristers - the General Council of the Bar in Ireland; and

S.63(1)	<ul style="list-style-type: none"> - For any other type of designated person not mentioned above, including Trust or Company Service Providers and tax advisers who are not solicitors, barristers or members of a designated accountancy body, - the Minister for Justice and Equality.
	<p>41. Under the Act the Central Bank has the following duties and powers:</p> <ul style="list-style-type: none"> - The duty to “<i>effectively monitor</i>” credit and financial institutions for compliance by them “<i>with the requirements of Part 4</i>” of the Act; - The power to take measures, including administrative sanction, reasonably necessary to ensure such compliance; - The duty to report to the Garda Síochána and the Revenue Commissioners any knowledge or suspicion of money laundering on the part of a designated person;
S.65	<ul style="list-style-type: none"> - The duty to include, in each of its annual reports, “<i>an account of the activities that the Central Bank has carried out in performing its functions under the Act during the year to which the annual report relates</i>”.
S.66(1) and (2)	<ul style="list-style-type: none"> - The power to “<i>request any public body, or anybody that represents, regulates or licenses, registers or otherwise authorises persons carrying on any trade, profession, business or employment, to provide the Central Bank with any relevant information, in relation to—</i> <ul style="list-style-type: none"> (a) <i>any designated persons for whom the Central Bank is a competent authority, or</i> (b) <i>any persons whom the body reasonably considers may be such designated persons.</i>
S.67(1)	<ul style="list-style-type: none"> - The power to “<i>direct</i>” (by notice in writing) “<i>a designated person for whom the</i>” Central Bank “<i>is competent authority to provide such information or documents (or both) relating to the designated person specified in the notice</i>”;
S.68(1)	<ul style="list-style-type: none"> - The power to “<i>direct a designated person to give explanations of documents</i>” either provided by the designated person or removed from the designated person’s premises by the Central Bank’s authorised officers;
S.71	<ul style="list-style-type: none"> - The power “<i>to direct (by notice in writing) a designated person for whom the authority is a competent authority to discontinue, or refrain from engaging in, specified conduct that in the opinion of the Central Bank constitutes...a breach of any specified provision of this Part 4 of the Act</i>”.
S.72 S.75 S.77	<ul style="list-style-type: none"> - The power to “<i>appoint ...persons ... to be authorised officers for the purpose of monitoring of designated persons</i>” and (by means of the deployment of such authorised officers) to lawfully enter and inspect the premises of designated persons for the purpose of exercising general powers of inspection set out in the Act;
S114(4)	<ul style="list-style-type: none"> - The duty and the power to initiate administrative sanctioning procedures where the work of authorised officers reveals instances of non-compliance with the requirements of Part 4 of the Act.

	<p>SECTION III: ASSESSMENT AND MANAGEMENT OF RISK / RISK BASED APPROACH</p>
	<p>A. INTRODUCTION</p>
<p>Art 8 (2) S.33</p>	<p>42. The abuse of the financial system for the purpose of money laundering or the financing of terrorist activities has long been recognised as a threat to society and a risk impacting on the reputation of individual credit or financial institutions, their clients and the financial sector as a whole. In line with international developments, the need for the assessment and management by each designated person of the money laundering and terrorist financing risks they face is now reflected in the Act. The Act, in line with international practice including EU law and the FATF guidelines adopts a combination of a rules-based and a risk-based approach to countering the threat of money laundering and terrorist financing. Section 54 (2) requires that designated persons adopt policies and procedures to apply to all persons involved in the conduct of their business. This requirement includes the assessment and management of risks of money laundering and terrorist financing. In doing so designated persons will find helpful the FATF guidance on the risk based approach (FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures June 2007) www.fatf-gafi.org/dataoecd/43/46/38960576.pdf . The Act refers to risk in various sections, for example, while section 33(1) (a) requires the application of CDD measures to customers as a rule prior to the commencement of a business relationship, section 33 (1) (c) requires a risk-based approach to the application of CDD measures prior to the carrying out of any service where the designated person “has reasonable grounds to believe that there is a real risk that the customer is involved in, or the service sought by the customer is for the purpose of money laundering or terrorist financing”. The CDD and monitoring requirements laid down in section 35 (1) and 35 (3) relate to the “risk of money laundering or terrorist financing”. In implementing a risk-based approach, designated persons should consider the specific requirements of the various sections of the Act, while keeping in mind the need to fulfil their overall obligations under the Act as a whole to prevent and detect money laundering and terrorist financing.</p> <p>43. The following paragraphs seek to guide designated persons in developing a basis for:</p> <ul style="list-style-type: none"> i) Identifying and categorising the risks of money laundering or terrorist financing arising from their business; ii) Mitigating and managing those risks in compliance with the Act in an effective and (particularly where a degree of discretion is permitted) proportionate manner; and iii) Developing policies and procedures for risk assessment and management and maintaining meaningful records of implementation decisions.

S.54(3)	<ul style="list-style-type: none"> a. <i>complex or large transactions or unusual patterns of transactions that have no apparent economic or visible lawful purpose; and</i> b. <i>any other activity that is likely to be related to money laundering or terrorist financing.</i>
---------	--

S.33(1)C	<p>48. The Act provides for risk-based measures to be applied by designated persons. Certain sections contain express references to “risk” while others do not. Taken as a whole, however, Part 4 broadly requires a risk based approach. There are express references to “risk” in the following circumstances:</p> <ul style="list-style-type: none"> a. Prior to carrying out any service for the customer if there are reasonable grounds to believe that there is a real risk that the customer is involved in or the service sought is for the purpose of, money laundering or terrorist financing, based on any of the following: <ul style="list-style-type: none"> i. the customer or type of customer; ii. the type of business relationship (if any); iii. the type of service, transaction or product; iv. the purpose (or the customer’s explanation of the purpose) of the service; v. the value of the transactions or products; vi. the source (or the customer’s explanation of the source) of funds.
S.33(2)(b)	<ul style="list-style-type: none"> b. In verifying the beneficial owner’s identity.
S.33.(5)(b)	<ul style="list-style-type: none"> c. In deciding whether it is warranted to accept verification of the identity of a customer (or beneficial owner) ‘during the establishment’ rather than, as normal, prior to the establishment of a business relationship, the designated person should first consider whether use of this concession could give rise to a ‘real risk’ of money laundering or terrorist financing.
S.35(1)	<ul style="list-style-type: none"> d. In seeking information as to the purpose and intended nature of a business relationship with a customer prior to the establishment of the relationship, the designated person should consider potential risks of money laundering or terrorist financing.
S.35(3)	<ul style="list-style-type: none"> e. In monitoring customer transactions, a designated person should enquire into the source of wealth or source of funds related to transactions to the extent reasonably warranted by the risk of money laundering or terrorist financing.
S.37(1) S.37(3)	<ul style="list-style-type: none"> f. In ascertaining whether a customer, or a beneficial owner connected

<p>S 39</p> <p>S.54(2)</p> <p>S.57(2)</p>	<p>with the customer, residing in a place outside of the State, is a politically exposed person, the steps taken to do so should be such as are reasonably warranted by the risk that the customer or beneficial owner (as the case may be) is involved in money laundering or terrorist financing.</p> <p>g. Where the designated person considers that there is a heightened risk of money laundering or terrorist financing, the designated person has the discretion to apply additional customer due diligence measures.</p> <p>Where a designated person adopts policies and procedures to be followed by persons involved in the conduct of the designated person’s business, the policies and procedures should be based on the designated person’s assessment of the risk of money laundering or terrorist financing;</p> <p>h. Where a designated person has branches or subsidiaries in a place other than Member States of the EU, and where the place concerned does not permit the application of requirements equivalent to those specified in Chapters II and IV of the Third Money Laundering Directive, the designated person shall inform the competent authority for the designated person, and should apply measures, determined in consultation with the competent authority, to deal with the risk of money laundering or terrorist financing arising from the absence of those requirements.</p>
<p>S.33(2)</p> <p>S. 33(2)(b)</p> <p>S.33(1)d(ii)</p> <p>S.33(8)</p>	<p>49. Note that the Act does not provide express reference to risk-based discretion to designated persons in a number of provisions. They can be seen as rules-based rather than risk-based. However, care should be taken to see these provisions in their proper context as part of the whole Act. Some examples of such prescriptive requirements are:</p> <ul style="list-style-type: none"> - When identifying and verifying a customer; this must be done by the designated person “<i>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</i>”; - Identification of any beneficial owner connected with the customer or service provided; - Where a designated person has reasonable grounds to doubt the veracity or adequacy of documents or information previously gathered in relation to an existing customer, it is obliged to apply the CDD measures as outlined in section 33(2) and, where applicable, s.33(4). However, “adequacy” is a relative concept and in this case it relates to the purpose of identifying the customer in the overall context of reducing the risk of money laundering; - Where a designated person is unable to comply with its customer

S.42	<p>verification obligations under the Act;</p> <ul style="list-style-type: none"> - Where a designated person knows, suspects, or has reasonable grounds to suspect that another person has been or is engaged in an offence of money laundering or terrorist financing, the formation of such a suspicion triggers a reporting duty which is absolute.
C. THE ROLE OF SENIOR MANAGEMENT	
	<p>50. In order for financial institutions to have effective risk-based approaches, the risk-based process must be imbedded within the internal controls of the institutions.</p> <p>The board of directors is ultimately responsible for ensuring that a designated person maintains an effective internal control structure, including suspicious activity monitoring and reporting. Strong senior management leadership and engagement in AML/CTF is an essential component of the design and implementation of a risk-based approach.</p> <p>The board of directors and senior management must create a culture of compliance, ensuring that the designated person's policies, procedures and processes, designed to limit and control risks of money laundering and terrorist financing, are fully consistent with the law and that staff adhere to them. The board of directors and senior management should be fully engaged in the decision making processes and take ownership of the risk-based measures adopted, since they will be held accountable if the approach is found to be inadequate.</p> <p>Section 111 of the Act provides (in circumstances where there is consent, connivance or neglect) for the personal criminal liability of directors, managers, secretaries, management committee members etc. of bodies corporate and unincorporated for offences committed by or on behalf of such a body.</p>
	<p>51. Senior management has a responsibility to ensure that the designated person's control processes and procedures are appropriately designed and implemented, and are effectively operated to reduce the risk of the designated person being used in connection with money laundering or terrorist financing.</p> <p>Senior management will need to:</p> <ul style="list-style-type: none"> - establish procedures to ensure that there is objective validation of risk assessment and management processes and of related internal controls; - obtain appropriate assurance that the adopted risk-based methodology reflects the risk profile of the financial institution. <p>The extent and timing of this independent testing should take into account the size, nature and complexity of the designated person and reporting should be</p>

conducted by, for example, the internal audit department, external auditors, compliance monitoring, specialist consultants or other qualified parties who are not involved in the implementation or operation of the financial institution's AML/CTF compliance programme.

The testing should be risk based (focusing attention on higher-risk customers, products and services); it should evaluate the adequacy of the financial institution's overall AML/CTF programme and the quality of risk management for the financial institution's operations, departments and subsidiaries; and it should include appropriate and comprehensive testing procedures for all relevant business units.

The Act sets out a framework for these controls by requiring designated persons inter alia, to perform appropriate CDD, report suspicions of money laundering, terrorist financing and other prohibited transactions (whether completed or not) and to establish and maintain appropriate procedures, training and record keeping.

	D. AML/CFT RISK POLICY AND PROCEDURES
S.54	<p>52. Each designated person shall adopt policies and procedures to prevent money laundering and terrorist financing that should, at a minimum, include the following:</p> <ul style="list-style-type: none"> - An assessment and management of risks of money laundering or terrorist financing, based on a methodology proportionate in its detail and complexity to the size and nature of the business and the inherent risks of money laundering or terrorist financing; - Details of risk-appropriate internal controls, including internal and external reporting procedures for suspicious transactions; - Procedures to identify large/complex transactions and unusual patterns and any other activity that is likely to be related to money laundering or terrorist financing; - Measures to be taken to identify, risk-assess, and if appropriate prevent transactions that favour or facilitate anonymity; - The basis for monitoring, communication and management of compliance with the policy and procedures, including the roles of the Board of Directors, senior management, the Money Laundering Reporting Officer and compliance functions, and where applicable the role of internal audit and external audit; and - Procedures to ensure the effective ongoing training of all relevant personnel.
	<p>53. Based on their own risk analysis, designated persons should determine such additional matters as are appropriate for inclusion in the policy and procedures, as tailored for their business. Best practice guidance proposes that the following should also feature in AML/CTF risk policy and procedures:</p> <p>Guiding principles:</p> <ul style="list-style-type: none"> - a statement of the culture and values to be adopted and promulgated throughout the designated person towards the prevention of money laundering and the financing of terrorism; - a statement of commitment to ensuring that AML/CTF requirements are not used to unreasonably deny access to financial services including access by vulnerable groups who may be financially excluded by merit of their age, gender, ethnicity, disability, educational attainment, income, etc. - a commitment to ensuring that customers’ identities will be verified, where so required by the Act, before the designated person accepts them; - a commitment to the designated person ‘knowing its customers’ appropriately - both at acceptance and throughout the business relationship - through taking appropriate steps to verify the customer’s identity and business, and its reasons for seeking the particular business relationship with the designated person and by keeping that knowledge of its customers up-to-date; - a commitment to ensuring that staff are trained and made aware of the law

	<p>and their obligations under it, and to establishing procedures to implement these requirements; and</p> <ul style="list-style-type: none"> - recognition of the importance of staff promptly reporting their suspicions internally. <p>Risk mitigation approach for each business area as applicable:</p> <ul style="list-style-type: none"> - a summary of the designated person’s approach to assessing and managing and, where feasible, mitigating its money laundering and terrorist financing risk; - allocation of responsibilities to specific persons and functions; - a summary of the designated person’s procedures for carrying out appropriate identification and monitoring checks on the basis of their risk-based approach; and - a summary of the appropriate monitoring arrangements in place to ensure that the designated person’s policies and procedures are being carried out. <p>As noted, AML/CTF policies and procedures should be reviewed at least annually and revised as needed to remain current.</p>
	<p>E. CONDUCTING THE RISK ASSESSMENT</p>
	<p>54. Money laundering risks may be measured (or at least estimated) by using criteria to allocate the customer base into a range of risk categories. Application of risk categories provides a strategy for managing potential risks by enabling designated persons to subject customers to proportionate controls and oversight, as appropriate to the risk category to which they are assigned. The most commonly used risk criteria for allocation to categories are: country or geographic risk; customer risk; product/services risk; and risks arising from channels of distribution.</p> <p>The weight given to these risk criteria (individually or in combination) in assessing the overall risk of potential money laundering or terrorist financing are discretionary for each designated person, subject to compliance with the provisions of the Act. The following paragraphs outline circumstances within the various categories that may suggest a heightened risk of money laundering or terrorist financing.</p> <p>A variety of approaches may be taken to documenting the risk profile of a designated person’s business. Designated persons may adopt an iterative approach so as to revise its risk profile in accordance with business-change.</p>
	<p>Country/Geographic Risk</p> <p>55. Country risk, in conjunction with other risk factors, provides useful information as to potential money laundering and terrorist financing risks. Country risk is not solely related to the country of origin of a customer. It should also take into account that a customer may have business interests in or relevant links to a country that may signify that the customer should be placed in a higher risk</p>

	<p>category. Factors that may result in a determination that customers from, in or connected with a particular country pose a higher risk include:</p> <ul style="list-style-type: none"> - Countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (“UN”) or European Union. In addition, countries subject to sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognised, may be given credence by a designated person because of the standing of the issuer and the nature of the measures; - Countries identified by credible sources (e.g. FATF, FATF-style regional bodies or other recognised evaluation bodies and EU Commission) as lacking adequate money laundering laws and regulations; - Countries identified by credible sources as providing funding or support for terrorist activities; or - Countries identified by credible sources as having significant levels of corruption, or other criminal activity.
	<p>Customer Risk</p> <p>56. Determining the potential money laundering and terrorist financing risks posed by a customer, or category of customers, is critical to the development of an overall risk framework. Based on its own criteria (and with due regard to the limitation on discretion in some provisions of the Act), a designated person will determine whether a particular customer poses a higher risk of money laundering and terrorist financing and whether, in some cases, mitigating factors are sufficient to conclude safely that customers engaged in such activities do not, in reality, pose a higher risk of money laundering or terrorist financing. Application of risk variables may increase or decrease the perceived risk in each case. The following are some characteristics of customers or customer activity that may indicate a higher risk of money laundering and terrorist financing:</p> <ul style="list-style-type: none"> - Significant and unusual geographic distance between the designated person and the location of the customer, without reasonable explanation; - Frequent and unusual movement of accounts or engagements to different designated persons, without reasonable explanation; - Frequent and unusual movement of funds between designated persons in various geographic locations, without reasonable explanation; - Where there is no commercial rationale for the customer buying the product or service he seeks; - Requests to associate undue levels of secrecy with a business relationship; - Situations where the origin of wealth and/or source of funds cannot be easily verified, or where the audit trail has appears to have been deliberately broken and/or unnecessarily layered; - The unwillingness of non-personal customers to give the names of their owners and controllers (beneficial owners); - Doubts as to whether a personal customer is acting on his own behalf or may be fronting on an undeclared basis for the beneficial owner; - Customers where the structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interests (beneficial owners); - Cash (and cash equivalent) intensive businesses for example: exchange

	<p>and payment services businesses (e.g. remittance houses, currency exchange houses, casas de cambio, bureaux de change, money transfer agents and bank note traders or other businesses offering money transfer facilities);</p> <ul style="list-style-type: none"> - Casino like activities, betting and other gambling related activities; - Businesses that while not normally cash intensive generate substantial amounts of cash for certain transactions; - Unregulated charities and other unregulated “not for profit” organisations (especially those operating on a “cross-border” basis); - Dealers in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers); - Use of intermediaries within the relationship who are not subject to adequate anti-money laundering regulation and who are not adequately supervised; or - Customers that are Politically Exposed Persons (PEPs) (See section IV). <p>A designated person’s objective must be to know who has ownership or control over the funds which form or otherwise relate to the relationship or transaction, and/or form the controlling mind or management of any legal entity involved in the funds, and/or who ultimately benefits from any transaction or relationship entered into. See Section IV.</p>
	<p>57. Some customers, by their nature or through what is already known about them by the designated person, may carry a lower money laundering or terrorist financing risk. For example:</p> <ul style="list-style-type: none"> - Customers who are employment-based or with a regular source of income from a known source which supports the activity being undertaken (this applies equally to pensioners or benefit recipients, or to those whose income originates from their partners’ employment); - Customers with a long-term and active business relationship with the designated person; or - Customers represented by those whose appointment is subject to court approval or ratification (such as executors).
	<p>58. For some customers, a comprehensive risk profile may only become evident once the business relationship has begun; making monitoring of customer activities and on-going reviews a fundamental component of a reasonably designed risk-based approach.</p>
	<p>Product Risk</p> <p>59. An overall risk assessment should also include determining the potential money laundering and terrorist financing risks presented by products and/or services offered by a designated person. Designated persons need to be mindful of new or innovative products or services not specifically being offered by designated persons, but that make use of the designated person’s services to deliver the product. Determining the money laundering risks of products and services may need to include a consideration of such factors below but designated persons should consider factors unique to their own sector (see sectoral guidelines in Part 2):</p>

	<ul style="list-style-type: none"> - International correspondent banking services involving transactions such as commercial payments for non-customers (for example, acting as an intermediary bank); - International private banking services; - Services involving banknotes and precious metal trading and delivery; - Services intended to render a customer anonymous; - Products which allow/facilitate use by third parties; or - Internet based products or products that facilitate easy non-face to face access.
	<p>Channel/Distribution Risk</p> <p>60. A further risk factor that may be relevant is the risk arising from the chosen channel of distribution of the product or service. This would include:</p> <ul style="list-style-type: none"> - Non-face-to-face business; - Business originating through introducers or agents, particularly of international origin; - Business introduced via multiple intermediaries; or - Business originating through unregulated, as opposed to regulated counterparties.
	<p>Other variables that may impact risk</p> <p>61. A designated person's risk-based methodology should also take into account risk variables specific to a particular business relationship. These variables may increase or decrease the perceived risk posed by a particular customer and may include:</p> <ul style="list-style-type: none"> - The level of assets to be deposited by a particular customer or the size of transactions undertaken. Unusually high levels of assets, or unusually large transactions, compared to what might reasonably be expected of customers with a similar profile may indicate that a customer not otherwise seen as higher risk may need to be treated as such. Conversely, low levels of assets or low value transactions involving a customer that would otherwise appear to be higher risk might allow for a designated person to treat the customer as lower risk. However, in the latter case, designated persons must be conscious of the fact that in respect of terrorist financing, low value transactions are often a common feature and it is often the repetitive nature of such transactions that is suspicious; - The regularity or duration of the relationship. Long standing relationships involving frequent customer contact throughout the relationship may present less risk from a money laundering and terrorist financing perspective; - The familiarity with a country, including knowledge of local laws, regulations and rules, as well as the structure and extent of regulatory oversight, as the result of a designated person's own operations within the country; or - The use of intermediate corporate vehicles or other structures that have no apparent commercial or other rationale or that unnecessarily increase the complexity or otherwise result in a lack of transparency. The use of such vehicles or structures, without an acceptable explanation, increases the risk.

	F. ASSESSING THE RISK OF TERRORIST FINANCING
	<p>62. In conducting a risk assessment of their business, designated persons must consider any vulnerabilities arising from the nature of their products or services to being abused for purposes of financing of terrorists or terrorism. Controls should be designed and implemented to seek to mitigate such risks and included in the risk policies and procedures.</p>
	<p>63. The application of a risk-based approach to terrorist financing is a difficult concept, as it differs from a risk-based approach that can be applied to detecting and identifying potential money laundering and other suspicious activity. Funds that are used to finance terrorist activities do not necessarily derive from criminal activity and, therefore, activities related to terrorist financing may not exhibit the same traits as conventional money laundering or fraud. Similarly, transactions associated with the financing of terrorists may be conducted in very small amounts, which in applying a risk-based approach may be the very transactions that are frequently considered to be of minimal risk with regard to money laundering. In addition, the actions by terrorists may be overt and outwardly innocent in appearance, such as the purchase of materials and services (i.e. commonly held chemicals, a motor vehicle, etc.) to further their goals, with the only covert fact being the intended use of such materials and services purchased. Should terrorist financing have a connection with other money laundering activity, a risk-based approach should help to suppress terrorist financing by providing the means for designated persons to identify and report such activity to government authorities.</p>
	G. OTHER FACTORS TO CONSIDER IN DESIGNING A RISK BASED APPROACH
	<p>64. While the application of a risk assessment and the development and maintenance of AML/CTF policies and procedures are mandatory under the Act, designated persons have a degree of discretion in determining the extent to which they adopt a risk based approach and the level of its complexity. The guiding principles are that:</p> <ul style="list-style-type: none"> - the risk analysis should be solidly founded on reliable research and provide a true reflection of the inherent risks and relevant mitigants across the business; - the risk criteria and categorisations chosen should be proportionate to the complexity of the business and consistent with the risk analysis; <p>On this basis, having regard to the services they provide, their customer base and their geographical area of operation, designated persons may need to devise a complex basis for assessing and managing the risks or, on the other hand, may determine that a relatively simple approach is appropriate for them. The business of some designated persons, having regard to their services and customer base, could be seen as relatively simple, involving few products or services, with most customers falling into similar categories. In such circumstances, a simple approach to risk management may be appropriate for many customers, with the focus being on those customers who fall outside the</p>

	<p>‘norm’. In this case customers can be easily grouped and allocated to categories without the need for an individual assessment unless there are other risk factors that indicate the contrary.</p>
	<p>65. Other designated persons may have a greater level of business, but large numbers of their customers may be predominantly retail, served through delivery channels that offer the possibility of adopting a standardised approach to many AML/CFT procedures. Here, too, the approach for most customers may be relatively straightforward, building on the product risk. However, in using such a standardised approach, designated persons should take care to ensure that relevant risk factors other than product risk are properly considered.</p> <p>66. By contrast, designated persons may offer a more ‘bespoke’ service to their customers (or to some categories of customer) or some of the other risk factors identified earlier would be relevant (higher-risk customers, product lines, countries and/or channels of distribution). In such cases, the business of assigning the customer to a risk-appropriate category is likely to be more complex and ongoing monitoring of the relationship more onerous. To assist in this regard, designated persons may take into account such additional information as they have already obtained through the business relationship to ensure that they ‘know their customer’ and assess, categorise and monitor the risks appropriately.</p>
	<p>67. How a risk-based approach is implemented will also depend on the designated person’s organisational and operational structure. For example, a designated person that operates through multiple business units will need a different approach from one that operates as a single business. Whatever approach is considered most appropriate to the designated person’s AML/CFT procedures, the broad objective is that the designated person should know who their customers are and understand the purpose and intended nature of the business relationship - what they do, and the risk that they may be involved in money laundering or terrorist financing. The profile of the customer’s behaviour will build up over time, assisting the designated person in identifying activities that may be suspicious.</p>
	<p>H. SECTORAL NOTES</p>
	<p>68. Further guidance on the risk based approach and how it applies to the particular sectors can be found in the sectoral guidelines in Part II.</p>

	SECTION IV: CUSTOMER DUE DILIGENCE
	A. WHAT IS CUSTOMER DUE DILIGENCE?
Art. 8 (1) S.33 (2)	<p>69. The term ‘Customer Due Diligence’ (CDD) refers to the range of measures used by designated persons to comply with their obligations under the Act in respect of: identifying and verifying the identity of their customers and identifying beneficial owners and verifying their identity; obtaining information on the purpose and intended nature of the business relationship; conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution’s knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.</p> <p>Designated persons must also collect and assess such other information as is needed to ensure that it knows its customers and what to expect from doing business with them, having regard to the risks of abuse for purposes of money laundering and terrorist financing. Varying degrees of due diligence measures will be appropriate, as discussed in Section III, depending on the nature of the relationship between the designated person and the customer, the type of business conducted and the perceived risks arising; what is adequate CDD in one case would be inadequate in another higher-risk situation. This section discusses the appropriate levels of CDD to be applied, ranging from those customers and products that qualify under the Act for SCDD up to the enhanced CDD required for compliance with the Act in relation to politically exposed persons (PEPs), correspondent banking and other higher-risk situations identified by designated persons.</p>
S.35 (1) S.35 (3)	<p>70. By reference to the Act, CDD shall comprise the following:</p> <ul style="list-style-type: none"> (a) Identifying the customer, and verifying the customer’s identity on the basis of documents (whether or not in electronic form), or information, that the designated person has reasonable grounds to believe can be relied upon to confirm the identity of the customer, including (i) documents from a government source (whether or not a State government source), or (ii) any prescribed class of documents, or any prescribed combination of classes of documents; (b) Identifying any beneficial owner connected with the customer or service concerned, and taking measures reasonably warranted by the risk of money laundering or terrorist financing (i) to verify the beneficial owner’s identity to the extent necessary to ensure that the person has reasonable grounds to be satisfied that the person knows who the beneficial owner is, and (ii) in the case of a legal entity or legal arrangement of a kind referred to in Sections 26, 27, 28 or 30 of the Act, to understand the ownership and control structure of the entity or arrangement concerned; (c) Obtaining information reasonably warranted by the risk of money laundering or terrorist financing on the purpose and intended nature of the business relationship; and (d) Conducting ongoing monitoring (to the extent reasonably warranted by the risk of money laundering or terrorist financing) of the business relationship including scrutiny of transactions undertaken throughout

	<p>the course of that relationship to ensure that the transactions being conducted are consistent with the designated person's knowledge of the customer, the business and risk profile, including, where necessary, the source of funds or wealth.</p>
<p>Art 20 S.54(3)</p>	<p>71. A designated person must, as part of its CDD process and following the policy it adopts in compliance with the obligations under section 54(3) of the Act, identify and scrutinise complex or large transactions, unusual patterns of transactions that have no apparent economic or visible lawful purpose, and any other activity that the designated person has reasonable grounds to regard as particularly likely, by its nature, to be related to money laundering or terrorist financing. As designated persons should be in a position to demonstrate compliance with this requirement, it is recommended that the background and purpose of such transactions should, as far as possible, be examined and the findings established in writing – see also paragraph 101.</p>
	<p>72. Designated persons should:</p> <ul style="list-style-type: none"> - appropriately verify the customer’s identity and that of any beneficial owner associated with the customer or the service provided (the extent of verification required in respect of beneficial owners will depend on the level of risk), - obtain appropriate information on the purpose and intended nature of the business relationship and conduct ongoing monitoring of the business relationship, - obtain appropriate additional information to understand the customer’s circumstances and business – including, where appropriate, the source of wealth, the purpose of specific activities and the expected nature and level of activities, - keep such information current and valid. <p>This information should be gathered at the outset of the business relationship. However, some of the information will be gathered and kept up-to-date by the designated person through ongoing monitoring of the business relationship which will afford the designated person an increasing understanding of the customer’s activities and the patterns of those activities. From time to time, events are likely to occur which may create doubt as to the veracity or adequacy of CDD information previously relied upon, in which case the designated person has an obligation under section 33(1) (d) to address any deficiencies in the CDD previously conducted. The Act is explicit regarding the veracity of identification documentation for both new and existing customers and this is further outlined in paragraph on existing customers. Designated persons should ensure that personal data is only used for the purpose for which it was obtained as stated in the Data Protection Acts and is not used for other purposes without prior consent. – See Para 19”</p>
	<p>B. IDENTIFICATION AND VERIFICATION OF THE CUSTOMER’S IDENTITY</p>

	<p>73. The Act specifies in section 33(2) (a) that the measures to be applied under section 33(1) of the Act 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, including—</p> <ul style="list-style-type: none"> - 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
	<p>What does identification mean?</p> <hr/> <p><u>Personal customers:</u></p> <p>74. Identification of a personal customer is the process whereby a designated person obtains from a customer the information necessary for it to identify who the customer is. The identity of an individual has a number of aspects at any point in time, all of which must be obtained by the designated person:</p> <ul style="list-style-type: none"> a. name (which may change due to particular events); b. address (which is likely to change from time to time); and c. date of birth (which is a constant). <p>This combination of data elements should be sufficient to identify an individual customer. Other information on an individual accumulates over time e.g., changes in name or address, family circumstances, employment, contacts with the authorities, relationships with other designated persons and physical appearance.</p> <p><u>Legal persons and arrangements:</u></p> <p>75. In the case of a legal person or arrangement, the process of identification is set out in three parts and comprises details on the entity itself, its directors (or equivalent) and the person(s) with signing authority. This is separate to the requirements relating to identification and verification of beneficial ownership dealt with later in this section. Guidance on how to meet the obligations outlined in this section are detailed in section 2 of Appendix 1.</p>
	<p>What does verification mean and what sources of evidence can be used?</p> <hr/> <p>76. Verification is the process through which the designated person establishes that the information obtained in relation to the customer’s identity is correct on the basis of satisfactory evidence provided by the customer or otherwise obtained by the designated person and accepted by the designated person as meeting the obligation in section 33 of the Act as to its veracity and adequacy.</p>
S.33 (2) (a)	<p>77. Evidence of identity can take a number of forms. Documentary evidence of identity can be in paper or electronic format. In respect of individuals, identity</p>

	documents, such as passports and driving licences, often offer the best means of being reasonably satisfied as to someone’s identity. However, in certain circumstances as outlined in Appendix 2 it may be possible to be reasonably satisfied as to a customer’s identity based on other forms of information.
	78. Where the customer is met face to face, the designated person should have sight of the original document(s) and appropriate details should be recorded, preferably by means of a digital copy. Where a member of the designated person’s staff visits the customer at his/her home address, the staff member should make a detailed record of the visit. This would include, for example, taking details of passport or driving licence numbers and relevant reference numbers from address verification documentation. Non face-to-face verification is addressed below under J.
S.33	<p>Use of online sources to verify identity</p> <hr/> <p>79. While a designated person may use online sources during the verification of identity, the requirement remains the verification of 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. A number of commercial agencies which access many data sources are accessible online by designated persons, and may provide designated persons with electronic verification.</p>
	80. Positive information (relating to full name, current address, date of birth) can prove that an individual exists, but some can offer a higher degree of confidence than others. Such information should include data from robust sources - where an individual has to prove their identity, or address, in some way in order to be included, as opposed to others, where no such proof is required.
	81. Before using a commercial agency for electronic verification, a designated person should be satisfied that information supplied by the data provider is considered to be sufficiently extensive, reliable and accurate and they should document the outcome of this assessment.
	82. In addition, a designated person may wish to satisfy itself that a commercial agency has processes that allow the enquirer to capture and store the information they used to verify an identity.
	<p>Information as evidence</p> <hr/> <p>83. Section 33(2)(a) of the Act provides that the identity of a customer can be verified on the basis of documentation or information where the designated person has reasonable grounds to believe that it can be relied upon to confirm the identity of the customer. In circumstances where the money laundering or terrorist financing risk in a product or service is considered to be at its lowest, a payment drawn on an account with an Irish or EU regulated credit institution, or one from a comparable jurisdiction, and which is in the sole or joint name of the</p>

	<p>customer, that contains the necessary information in Appendix 1 may be used as information for the purposes of Section 33(2)(a). Whilst the payment may be made between accounts with regulated designated persons or by cheque or debit card, the accepting designated person should be able to confirm that the payment (by whatever method) is from a bank or building society account in the sole or joint name(s) of the customer. Designated persons will need to be able to demonstrate why they considered it to be reasonable to have regard to the source of funds as suitable information in a particular instance.</p>
	<p>Means of verification</p> <hr/> <p><u>Personal Customers:</u></p> <p>84. It is anticipated that many designated persons will opt to verify the identity of customers by means of one piece of photographic evidence that includes name and date of birth and one piece of evidence of address. This “One plus One” method is set out in the Appendices.</p> <p>The majority of customers will be verified using the ‘standard documentation’ listed in Appendix 1. However where a customer is not in a position, for genuine reasons, to provide documentation listed in Appendix 1 an alternative and non-exhaustive list of ‘non standard documents’ is listed in Appendix 2.</p>

People who cannot reasonably be expected to produce conventional evidence of identity should not be unreasonably denied access to the services of designated persons. Where a customer is not in a position to provide 'standard documentation', a designated person should refer to the documentation and information requirements in Appendix 2 of these Guidelines and ensure that its staff do not cite the requirements of the Act as an excuse for not providing services without giving proper consideration to the evidence available.

A designated person should have robust procedures in place which take into account the requirement of those who may not be able to provide standard identification documentation but who may be able to provide alternative non standard documents.

In particular, designated persons subject to the Central Bank Consumer Protection Code are subject to the following general principle set out in that code:

“A regulated entity must ensure that in all its dealings with customers and within the context of its authorisation it, without prejudice to the pursuit of its legitimate commercial aims, does not, through its policies, procedures or working practices, prevent access to basic financial services” (General Principle 11, Chapter 1).

Designated persons should also consider any similar principle(s) contained in any amendment of the Consumer Protection Code.

Designated persons will also find FATF Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion to be helpful.
<http://www.fatf-gafi.org/dataoecd/62/26/48300917.pdf>

	<p>C. IDENTIFICATION AND VERIFICATION OF THE BENEFICIAL OWNER</p>
<p>S.33 (2) (b)</p>	<p>85. The Act specifies in section 33(2)(b) that the measures to be applied under section 33(1) of the Act include identifying any beneficial owner connected with the customer or service concerned, and taking measures reasonably warranted by the risk of money laundering or terrorist financing—</p> <ul style="list-style-type: none"> (i) to verify the beneficial owner’s identity to the extent necessary to ensure that the person has reasonable grounds to be satisfied that the person knows who the beneficial owner is, and (ii) in the case of a legal entity or legal arrangement of a kind referred to in section 26, 27, 28 or 30 of the Act, to understand the ownership and control structure of the entity or arrangement concerned.
<p>Art 3 (6) S.30 (3)</p> <p>S.26</p> <p>S.27</p> <p>S.28</p>	<p>86. Other than as set out in a) to g) below, the Act defines a beneficial owner as “any individual who ultimately owns or controls a customer or on whose behalf a transaction is conducted.” The Act goes on to define beneficial owner in the following circumstances:</p> <ul style="list-style-type: none"> a) “Beneficial owner”, in relation to a body corporate, is any individual who (other than a company having securities listed on a regulated market) — <ul style="list-style-type: none"> i. ultimately owns or controls, whether through direct or indirect ownership or control (including through bearer shareholdings), more than 25 per cent of the shares or voting rights of the body; or ii. otherwise exercises control over the management of the body. b) “Beneficial owner”, in relation to a partnership, means any individual who— <ul style="list-style-type: none"> i. ultimately is entitled to or controls, whether the entitlement or control is direct or indirect, more than a 25 per cent share of the capital or profits of the partnership or more than 25 per cent of the voting rights in the partnership; or ii. otherwise exercises control over the management of the partnership c) “Trust” means a trust that administers and distributes funds. d) “Beneficial owner”, in relation to a trust, means any of the following: <ul style="list-style-type: none"> i. any individual who is entitled to a vested interest in possession, remainder or reversion, whether or not the interest is defeasible, in at least 25 per cent of the capital of the trust property; ii. in the case of a trust other than one that is set up or operates entirely

	<p>for the benefit of individuals referred to in paragraph (a), the class of individuals in whose main interest the trust is set up or operates;</p> <p>iii. any individual who has control over the trust.</p> <p>iv. For the purposes of and without prejudice to d(i)-(iii) above, an individual who is the beneficial owner of a body corporate that—</p> <ul style="list-style-type: none"> • is entitled to a vested interest of the kind referred to in d(i) above, or • has control over the trust, is taken to be entitled to the vested interest or to have control over the trust (as the case may be). <p>g) “Control”, in relation to a trust, means a power (whether exercisable alone, jointly with another person or with the consent of another person) under the trust instrument concerned or by law, to do any of the following:</p> <ul style="list-style-type: none"> i. dispose of, advance, lend, invest, pay or apply trust property; ii. vary the trust; iii. add or remove a person as a beneficiary or to or from a class of beneficiaries; iv. appoint or remove trustees; v. direct, withhold consent to or veto the exercise of any power referred to in e(i) to (iv) above. <p>An individual does not have control solely as a result of the power exercisable collectively at common law to vary or extinguish a trust where the beneficiaries under the trust are at least 18 years of age, have full capacity and (taken together) are absolutely entitled to the property to which the trust applies.</p> <p>S.29 h) “Beneficial owner”, in relation to an estate of a deceased person in the course of administration, means the executor or administrator of the estate concerned.</p> <p>S.30 i) In all other cases, “beneficial owner” in relation to a legal entity or legal arrangement means –</p> <ul style="list-style-type: none"> i. if the individuals who benefit from the entity or arrangement have been determined, any individual who benefits from at least 25 per cent of the property of the entity or arrangement; ii. if the individuals who benefit from the entity or arrangement have yet to be determined, the class of such individuals in whose main interest the entity or arrangement is set up or operates; and iii. any individual who exercises control over at least 25 per cent of the property of the entity or arrangement. <p>87. For the purposes of, and without prejudice to, the generality of subsection (g) above, any individual “who is the beneficial owner of the customer” that benefits from or exercises control over the property of the entity or arrangement is taken to benefit from or exercise control over the property of the entity or arrangement. “Arrangement or entity” means an arrangement or entity that</p>
--	---

	<p>administers and distributes funds.</p>
	<p>88. In respect of a legal entity or arrangement, the designated person shall verify the identity of the beneficial owner (the extent of this verification will depend on the level of risk) and understand the ownership and control structure of the customer.</p> <p>Appendix 1 Section 2.b. provides guidance on how a designated person should identify and verify beneficial owners for legal persons and arrangements.</p> <p>Money launderers are attracted by the availability of complex products and services that operate internationally within a reputable and secure financial services environment that is familiar with high value or frequent transactions. Designated persons should be alert to customer transactions, relationships and structures that promote or facilitate, whether intentionally or unintentionally, a culture of confidentiality or concealment of the true beneficial owner or beneficiary of funds.</p> <p>The use of concentration accounts or entities – e.g. multi-client pooled/ omnibus type accounts, nominee companies/structures or other arrangements (“Pooling Arrangements”)- used to collect together funds from a variety of sources for onward transmission or investment, is seen as a potential significant risk.</p> <p>It should be noted that, in conducting a risk based assessment of such accounts, a designated person may take into account whether there is a legitimate business reason for the use of the account and whether the account is owned or controlled by a regulated financial entity. The designated person can then exercise its own judgement in the circumstances as to the level of customer due diligence to be applied.</p> <p>Designated persons should also establish whether there are any beneficial owners of the funds contained in such accounts and the necessity to identify and verify same. It is acknowledged that there may be instances where the customer meets the definition of a specified customer as defined in section 34(5) of the Act, in which case SCDD may be applied to the customer.</p> <p>A designated person must know who has ownership or control over the funds which form or otherwise relate to the relationship, transaction or investment, and/or form the controlling mind or management of any legal entity involved in the funds.</p> <p>A designated person’s records should evidence how these risks have been analysed and assessed and how they are being addressed in accordance with Section III.</p>
	<p>89. While there is an obligation to identify and verify the identity of all beneficial</p>

S.30	<p>owners, there may be circumstances where the product or service is of a type where it is obvious that it is being provided in respect of the customer only and that no beneficial owner is involved. In those circumstances, designated persons may, on the basis of an appropriate risk assessment, decide that it is not necessary to enquire any further in that regard. Where this is not clearly established by the designated person, they must verify the beneficial owner's identity to the extent necessary to ensure that the person has reasonable grounds to be satisfied that the person knows who the beneficial owner is. Actions that may assist in verifying the identity of a beneficial owner in this case include securing a statement signed by the customer with respect to the business relationship entered into with the designated person.</p>
S.34	<p>90. It is not necessary for designated persons to identify and verify the identity of beneficial owners of incorporated entities that are admitted to trading on a regulated market within the meaning of Section 24 of the Act. This means regulated markets in the EEA as defined in the European Communities (Markets in Financial Instruments Directive) Regulations 2007 (as amended) or a regulated market outside the EEA, where that place imposes disclosure requirements consistent with legislation of the European Communities on companies admitted to trading on that market. In the case of markets that do not come within the definition of a regulated market in the Act and do not qualify for SCDD treatment, the designated person should apply measures that are warranted by the level of risk, i.e. the identify of any beneficial owner must be established with the extent of verification of any beneficial owner determined according to the risk of money laundering or terrorist financing.</p>
Art 9 (5) S.35 (2) S.33 (8)	<p>91. If the designated person is unable to satisfy itself concerning the identity of the beneficial owner of any customer, on the basis of the verification methods that it considers appropriate given the nature of the customer, no business relationship with the customer may be established nor any service to the customer supplied and the designated person should consider whether to make a report to An Garda Síochána and to the Revenue Commissioners.</p>
	<p>D. WHEN MUST IDENTIFICATION AND VERIFICATION BE UNDERTAKEN?</p>
Art 9 (1) S.33 (1)	<p>92. The identity of the customer must be established in all cases prior to the establishment of a business relationship or the provision of a service. In cases where SCDD exemptions of section 34 apply, the identity of the customer must, of necessity, be established along with the relevant exemption criteria which should be recorded by the designated person. The verification of the identity of the customer or the verification of the identity of the beneficial owner (the extent of verification required is dependent on the level of risk connected with the customer or service concerned), must, subject to the exceptions referred to below, take place prior to the establishment of a business relationship or the carrying out of a transaction or service.</p>

	<p>93. However, provided the designated person takes the necessary steps as soon as practicable, verification of the identity of the customer or beneficial owner may be completed in the course of the establishment of a business relationship where the designated person has reasonable grounds to believe that:</p> <ul style="list-style-type: none"> - doing so prior to the establishment of the relationship would interrupt the normal conduct of business; and - there is no real risk that the customer is involved in, or the service sought by the customer is for the purpose of money laundering or terrorist financing.
Art 9 (3) S.33 (7)	<p>94. The verification of the identity of the beneficiary under a life assurance policy may take place after the business relationship has been established, provided that it takes place before any payout or exercise by a beneficiary of a right vested under the policy.</p>
Art 9 (4) S.33 (6)	<p>95. The verification of the identity of the customer or beneficial owner may take place after a bank account has been opened, so long as the institution ensures that transactions in connection with the account are not carried out by or on behalf of the customer or beneficial owner before carrying out that verification.</p>
	<p>96. The assessment of when it might be appropriate for a designated person to establish a business relationship in accordance with the paragraphs above is a matter for each designated person, according to the nature of the products and the services it provides. However, where a designated person enters into a business relationship in advance of verification of identity, it should consider the legal consequences of making any payments to the customer including the return of any assets transferred by the customer to the designated person prior to the completion of verification. Designated persons should also be mindful that failure to comply with the requirements of section 33 is an offence which carries a penalty of up to five years imprisonment and/or an unlimited fine.</p>
	<p>E. OBTAINING INFORMATION ON THE PURPOSE AND NATURE OF THE BUSINESS RELATIONSHIP</p>
S.35 (1)	<p>97. The obligation to obtain information from a customer on the purpose and nature of the business relationship is one that must be applied to all customers with whom a designated person is entering into a business relationship. In most cases, this will be self evident given the nature of the product or service that the customer is seeking or may be easily clarified by discussing with the customer what they are seeking from the relationship.</p>
	<p>98. Before a designated person enters into a business relationship with a customer, the designated person shall obtain information reasonably warranted by the risk of money laundering or terrorist financing on the purpose and intended nature of the business relationship. The following information may be of assistance to a designated person in this regard:</p> <ul style="list-style-type: none"> - Nature and details of the business/occupation/employment of the customer; - The expected source of funds in relation to the customer's anticipated pattern of transactions;

	<ul style="list-style-type: none"> - The expected source of wealth (particularly for high risk customers); - The various relationships between signatories and with underlying beneficial owners; and - The anticipated level and nature of the activity that is to be undertaken through the business relationship.
	<p>99. Over time, the designated person will develop a greater understanding of the business or nature of the activities undertaken by the customer. While it is necessary to obtain information on the purpose and nature of the business relationship at the outset of the relationship, the reliability of this profile will increase over time as the designated person learns more about the customer.</p>
	<p>F. CONDUCTING ONGOING MONITORING OF THE BUSINESS RELATIONSHIP</p>
S.35 (3)	<p>100. A designated person shall monitor dealings with a customer with whom the person has a business relationship, including (to the extent reasonably warranted by the risk of money laundering or terrorist financing) by scrutinising transactions and the source of wealth or of funds for those transactions, to determine whether or not the transactions are consistent with the person’s knowledge of the customer and the customer’s business and pattern of transactions, and any knowledge that the person may have that the customer may be involved in money laundering or terrorist financing.</p> <p style="padding-left: 40px;">Section 35(3) of the Act refers to “source of funds”. When scrutinising the source of funds a designated person should seek to discover the origin and the means of transfer for funds that are involved in the transaction (for example, occupation, business activities, proceeds of sale, corporate dividends)</p> <p style="padding-left: 40px;">Section 35(3) of the Act refers to “source of wealth”. When scrutinising the source of wealth a designated person should seek to discover the activities that have generated the total net worth of the customer (that is, the activities that produced the customer’s funds and property).</p>
	<p>101. The objective of the ongoing monitoring obligation imposed by the Act is to identify activities of customers during the course of the business relationship which are not consistent with the designated person’s knowledge of the customer, or the purpose and intended nature of the business relationship, and which need to be assessed for the possibility that the designated person may have grounds to report a suspicion of money laundering or terrorist financing. It is recommended that designated persons should pay particular attention to complex or unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose. As designated persons should be in a position to demonstrate compliance, it is recommended that the background and purpose of such transactions should, as far as possible, be examined and the findings established in writing – see also paragraph 71.</p>

	<p>102. Given the large differences between designated persons in terms of customer numbers and the nature and scale of activities entered into by those customers, how monitoring is undertaken will vary considerably. Further guidance on appropriate monitoring is given in the sectoral guidelines.</p>
	<p>G. WHAT IS SIMPLIFIED CUSTOMER DUE DILIGENCE (SCDD)?</p>
<p>Art 11 S.34</p>	<p>103. For certain categories of customer or business defined in the Act, a set of SCDD measures may be substituted for full CDD, to reflect the accepted low risk of money laundering or terrorist financing that could arise from such business. This does not represent a total exemption as, prior to applying SCDD, designated persons have to conduct and document appropriate testing to satisfy themselves that the customer or business qualifies for the simplified treatment, in accordance with the definitions and criteria set out in the Act. Designated persons do not have any discretion to add to the categories specified in the Act to which SCDD may be applied.</p>
<p>Art 11 (3)</p>	<p>104. Legislative basis:</p> <p>The Act provides, in section 34(1), that a designated person is not required to apply the measures specified in section 33(2) of the Act if the customer or product concerned is a specified customer or a specified product, as the case may be. Similarly, section 36(1) of the Act provides that a designated person is not required to comply with section 35(1) of the Act if the designated person has reasonable grounds for believing that the customer or product concerned is a specified customer or specified product, as the case may be.</p> <p>105. In addition, section 34(2) of the Act provides that a credit institution is not required to apply the measures specified in section 33(2)(b) in respect of the beneficial ownership of money held, or proposed to be held, in trust—</p> <ul style="list-style-type: none"> (a) in a client account, within the meaning of the Solicitors (Amendment) Act 1994, or (b) in an account for clients of a person who by way of business, provides legal or notarial services to those clients— <ul style="list-style-type: none"> (i) in a Member State and who is supervised or monitored for compliance with requirements specified in the Third Money Laundering Directive, in accordance with Section 2 of Chapter V of that Directive, or (ii) in a place that is designated under section 31 and who is supervised or monitored in the place for compliance with requirements equivalent to those

	<p>solely because the undertaking provides either foreign exchange services or payment services, or both.</p>
<p>Art 11 (2) (a) S.34 (5) (b)</p>	<p>a. Listed Companies</p> <hr/> <p>109. SCDD may be applied where the customer is a company listed on a Regulated Market as defined in Section 24 of the Act (e.g. the Irish Stock Exchange Official List. However, the Irish Stock Exchange’s IEX market is not a regulated market, neither is the London Stock Exchange’s AIM market). Section 34(5)(b) brings within the definition of specified customer a listed company whose securities are admitted to trading on a regulated market.</p> <p>Markets that do not come within the definition of a Regulated Market in Section 24 of the Act and do not qualify for SCDD treatment, may nevertheless be treated as low risk to the extent warranted by the risk.</p>
<p>Art 11 (2) (c) S.34 (5)(d)</p>	<p>b. Public Body</p> <hr/> <p>110. SCDD may be applied to a public body, or other body as defined below (whether incorporated or unincorporated) that—</p> <ul style="list-style-type: none"> (i) has been entrusted with public functions under a provision of the treaties of the European Communities or under an Act adopted by an institution of the European Communities, (ii) in the reasonable opinion of the designated person concerned, the identity of the body is publicly available, transparent and certain, (iii) in the reasonable opinion of the designated person concerned, the activities of the body and its accounting practices are transparent, and (iv) the body is either accountable to an institution of the European Communities or to a public authority of a Member State. <p>Examples of institutions falling into this category include the European Central Bank, The European Investment Bank, the European Environment Agency etc.</p> <p>A list of EU agencies can be found at: http://europa.eu/agencies/community_agencies/index_en.htm</p>

<p>Art 11 (2) (b) S.34 (2)</p>	<p>Beneficial Owners of Pooled Accounts held by Solicitors and other Legal Professionals</p> <p>111. As solicitors and other legal professionals are subject to the Act, they are obliged to verify the identities of their customers where they open client accounts on their behalf. Designated persons with which such client accounts are held may apply a variation of SCDD to the owners of such funds. It is important to note that the relevant exemption in section 34(2) is from the beneficial owner identification and verification requirements of section 33 (2) (b) only, in other words the customer identification and verification measures required by section 33 (1) (a) still apply. This exemption also applies in relation to notaries and other legal professionals from non EEA countries who are subject to equivalent AML/CFT terrorist requirements to those set out in the Act and they are supervised for compliance with those requirements. In addition, on request they must make the information concerning the identity of the customer available to the designated person.</p>
<p>Art 11 (5) (d) S.34 (7) (d)</p>	<p>Specified Products</p> <p>Electronic Money</p> <p>112. SCDD may be applied in relation to electronic money. ‘Electronic money’ shall mean monetary value as represented by a claim on the issuer which is:</p> <ul style="list-style-type: none"> a) Stored on an electronic device; b) Issued on receipt of funds of an amount not less in value than the monetary value issued; and c) Accepted as means of payment by undertakings other than the issuer. <p>113. If the device cannot be recharged, the maximum amount stored in the device is no more than €250 or €500, if the device cannot be used outside the State. Where the device can be recharged, a limit of €2500 is imposed on the total amount transacted in a calendar year, and no more than €1000 is redeemed in that same calendar year by the issuer of electronic money.</p>
<p>Directive 2006/70/EC Art 3 (3) S.34 (7) (a)</p>	<p>114. SCDD may be applied to a life assurance policy having an annual premium of no more than €1,000 or a single premium of no more than €2,500. Further guidance is provided in the sectoral guidelines on products falling within the criteria set out above.</p>
<p>Art 11 (5) (c) S.34 (7) (c)</p>	<p>Pensions</p> <p>115. SCDD may be applied to pension, superannuation or similar schemes which provide retirement benefits to employees, where contributions are made by an employer, or by way of deduction from an employee’s wages, and the scheme rules do not permit the assignment of a member’s interest under the scheme.</p>

<p>Art 11 (5) (b) S.34 (7) (b)</p>	<p>116. SCDD may also be applied in relation to insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral.</p>
<p>Art 7 (c,d) S.33 (1) (c,d)</p>	<p>117. SCDD may not be applied where the designated person has reasonable grounds to believe that there is a real risk that a customer is involved in, or the service sought involves money laundering or terrorist financing, or where there are doubts about the veracity or accuracy of documents, data or information previously obtained for the purposes of customer verification.</p>
	<p>118. Designated persons may not avail of the SCDD concession where</p> <ul style="list-style-type: none"> (i) the customer concerned is from a place that is designated under section 32 of the Act as a place that does not have adequate procedures in place for the detection of money laundering or terrorist financing, (ii) section 33(1)(c) of the Act relating to reasonable grounds to believe that there is a real risk of involvement in money laundering or terrorist financing applies, (iii) section 33(1)(d) of the Act relating to adequacy of documentation or information applies, (iv) the customer is an individual and section 33(4) of the Act relating to remote identification applies, <p style="text-align: center;">or</p> <ul style="list-style-type: none"> (v) the designated person is required to apply measures under section 37 (where a customer or beneficial owner is a PEP, immediate family member or close associate of PEP)
	<p>I. WHAT IS ENHANCED CUSTOMER DUE DILIGENCE?</p>
	<p>Enhanced Customer Due Diligence Obligations in the Act</p> <p>119. The Act prescribes three circumstances in which enhanced customer due diligence (ECDD) or additional CDD measures must be applied:</p> <ul style="list-style-type: none"> - In respect of a correspondent banking relationship with another credit institution located outside of the EU - In respect of non face-to-face customers under Section 33(4) of the Act; and - In respect of a business relationship or transaction with a non-

	<p style="text-align: center;">resident PEP.</p> <p>120. In addition to these explicit statutory obligations, in any case where designated persons identify other higher risk customers or business scenarios, a risk-proportionate level of ECDD must also be applied. On that basis, in circumstances in which a designated person concludes that a customer presents a higher risk of money laundering or terrorist financing, ECDD measures should be applied at two levels:</p> <ul style="list-style-type: none"> i. Designated persons need to decide whether or not they have obtained adequate information regarding the customer or service to form a basis for a reliable and comprehensive assessment of the risks arising – do they sufficiently know the customer and the risks likely to be presented by the customer’s business? If not, the designated person should seek additional documentation and/or information regarding the customer and/or service, including additional CDD information in any case where the designated person has doubts about the veracity or adequacy of information previously obtained (to comply with section 33(1)(d) of the Act). ii. Designated persons should apply an enhanced level of ongoing monitoring to their business with the customer, as appropriate to their assessment of the risk of money laundering or terrorist financing arising from the business with that customer and should review the level of that monitoring on a regular basis to ensure that it remains risk-appropriate.
	<p>Enhanced Customer Due Diligence for politically exposed persons (PEPs)</p> <p>121. Individuals, residing outside the State, who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to designated persons as their position makes them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates residing outside the State. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put a customer into a higher risk category. Under the definition of a PEP, an individual ceases to be so regarded one year after he or she has left office.</p> <p>122. Section 37 requires a designated person to take steps to determine whether or not a customer (or a beneficial owner connected with the customer or service concerned) who resides in a place outside the State, is a PEP, an immediate family member, or a close associate, of a PEP.</p> <p>The steps to be taken are such steps as are reasonably warranted by the risk that the</p>

customer or beneficial owner is involved in money laundering or terrorist financing.

123. The Act requires, in section 37(4), that, where a designated person knows or has reasonable grounds to believe that a customer residing in a place outside the State is a PEP or an immediate family member or close associate of a PEP, the designated person shall—

- (a) ensure that approval is obtained from any senior management of the designated person before a business relationship is established with the customer, and
- (b) determine the source of wealth and of funds for the following transactions—
 - (i) transactions the subject of any business relationship with the customer that are carried out with the customer or in respect of which a service is sought, or
 - (ii) any occasional transaction that the designated person carries out with, for or on behalf of the customer or that the designated person assists the customer to carry out.

124. Similarly, the Act requires, in section 37(6), that, where a designated person knows or has reasonable grounds to believe that a beneficial owner residing in a place outside the State, and connected with a customer or with a service sought by a customer, is a PEP or an immediate family member or close associate of a PEP, the designated person shall—

- (a) ensure that approval is obtained from any senior management of the designated person before a business relationship is established with the customer, and
- (b) determine the source of wealth and of funds for the following transactions—
 - (i) transactions the subject of any business relationship with the customer that are carried out with the customer or in respect of which a service is sought, or
 - (ii) any occasional transaction that the designated person carries out with, for or on behalf of the customer or that the designated person assists the customer to carry out.

125. Section 37(5) of the Act provides that a credit institution may allow a bank account to be opened with it by a customer before taking the steps referred to in section 37(1) of the Act or seeking the approval referred to in section 37(4)(a), so long as the institution ensures that transactions in connection with the account are not carried out by or on behalf of the customer or any beneficial owner concerned before taking the steps or seeking the approval, as the case may be.

Politically Exposed Persons

Definitions of PEP terminology in the Act.

126. Section 37(10) of the Act defines a PEP as “an individual who is, or has at any time in the preceding 12 months been, entrusted with a prominent public function, including either 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;”

127. The section in turn defines a specified official as “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;
- (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’affaires or high-ranking officer in the armed forces.”

128. The section also states that an immediate family member of a PEP includes any of the following persons:

- (a) any spouse of the PEP;
- (b) any person who is considered to be equivalent to a spouse of the PEP under the national or other law of the place where the person or PEP resides;
- (c) any child of the PEP;
- (d) any spouse of a child of the PEP;
- (e) any person considered to be equivalent to a spouse of a child of the PEP under the national or other law of the place where the person or child resides;

	<p>(f) any parent of the PEP;</p> <p>(g) any other family member of the PEP who is of a class prescribed by the Minister for Justice and Equality under section 37(11) of the Act.</p> <p>129. The section further states that a close associate of a PEP includes any of the following persons:</p> <p>(a) any individual who has joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with the PEP;</p> <p>(b) any individual who has sole beneficial ownership of a legal entity or legal arrangement set up for the actual benefit of the PEP.</p> <p>130. The Act provides at section 37(7) that, for the purposes of section 37(4) and section 37(6), a designated person is deemed to know that another person is a PEP or an immediate family member or close associate of a PEP if, on the basis of—</p> <p>(a) information in the possession of the designated person (whether obtained under section 37(1) to section 37(3) or otherwise),</p> <p>(b) in a case where the designated person has contravened section 37(1) or section 37(2), information that would have been in the possession of the person if the person had complied with that provision, or</p> <p>(c) public knowledge, there are reasonable grounds for concluding that the designated person so knows.</p>
	<p>Points to note in relation to PEPs</p> <p>131. The Act requires designated persons to apply enhanced measures to PEPs (and their immediate family members and close associates) that are resident outside the State but not to PEPs resident in the State. In this context, a designated person must take care to not confuse residency with nationality.</p> <p>132. Where section 37(4)(a) of the Act refers to “any senior management”, this must not be interpreted to permit an individual merely approaching his or her line manager; the approval should be from senior management at the designated person.</p> <p>133. Section 37(4) (b) of the Act refers to “source of wealth and of funds”. When determining the source of wealth, a designated person should look at the activities that have generated the total net worth of the customer (that is, the activities that produced the customer’s funds and property). When determining the source of funds, a designated person should consider the origin and the means of transfer for funds that are involved in the transaction (for example, occupation, business activities, proceeds of sale, corporate dividends)</p>

	<p>134. Although a customer or beneficial owner might not initially (at the commencement of the business relationship) meet the definition of a PEP (or immediate family member or close associate), designated persons should be conscious that this position might change over time. The designated person should, as far as practicable, be alert to public information relating to possible changes in the status of its customer or beneficial owner with regard to political exposure. Where an existing customer or beneficial owner becomes a PEP, immediate family member, or close associate, then the measures required by section 37 should be applied. Although not explicitly required by section 37 (4), it would be advisable to obtain senior management approval to the continuation of a business relationship in light of the provisions of section 37 (8).</p> <p>135. Due to the higher risk of money laundering and terrorist financing posed by PEPs, designated persons should apply an enhanced level of ongoing monitoring to their business relationships with PEPs</p> <p>136. Establishing whether an individual qualifies as a PEP is not always straightforward and can present difficulties. Where designated persons need to carry out specific checks, they may be able to rely on an internet search engine, or consult relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations. If there is a need to conduct more thorough checks, or if there is a high likelihood of a designated person having PEPs for customers, subscription to a specialist PEP database may be the only adequate risk mitigation tool.</p>
	<p>J. ENHANCED CUSTOMER DUE DILIGENCE WHERE A CUSTOMER WHO IS AN INDIVIDUAL DOES NOT PRESENT IN PERSON (NON FACE-TO-FACE)</p>
	<p>Additional Customer Due Diligence Obligations in the Act</p> <p>137. Section 33(4) of the Act contains a supplementary obligation on a designated person where a customer who is an individual does not present in person. This is not an alternative obligation but a supplementary one. The subsection provides that, without prejudice to the generality of section 33(2)(a) of the Act, one or more of the following measures shall be applied by a designated person under section 33(1) of the Act, where a customer who is an individual does not present to the designated person for verification in person of the customer's identity:</p> <ul style="list-style-type: none"> a) verification of 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 are reliable as confirmation of the identity of the customer in addition to any documents or information that would ordinarily have been used to verify the customer's identity if the customer had presented to the designated person for verification in person of the customer's identity;

	<p><u>Examples of a):</u></p> <ul style="list-style-type: none"> - The use of robust anti-fraud and other risk based checks that the firm routinely undertakes as part of its existing procedures; - Telephone contact with the customer prior to the commencement of the business relationship on a home or business number which has been verified (electronically or otherwise), or a “welcome call” to the customer before the business relationship starts, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account; - Communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, might be required to be returned completed or acknowledged without alteration); - Internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail secure delivery to the named individual at a verified address; - Card or account activation procedures where the customer uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail secure delivery to the named individual at a verified address; - Verify information on documents received, e.g. in relation to a utility bill forwarded, cross check against a bank statement narrative relating to entries from the utility bill provided or cross checking salary details appearing on a recent bank or building society statement verifying the individual’s employer as previously notified; and - Electronic verification via a commercial agency where electronic verification has not been used originally to verify the customer. <p>(b) verification of documents supplied, for the purposes of verifying the identity of the customer under this section, to the designated person by the customer;</p> <p>(c) verification of the customer’s identity on the basis of confirmation received from an acceptable institution that the customer is, or has been, a customer of that institution;</p> <p>(d) ensuring that one or more of the following transactions is carried out through an account in the customer’s name with an acceptable institution that is a credit institution:</p> <ul style="list-style-type: none"> (i) the first payment made by the customer to the designated person for the provision of a service; (ii) in the case of a designated person acting for or on behalf of the customer in respect of a financial transaction or a transaction relating to land, the first payment made by the customer in respect of the transaction; (iii) in the case of a designated person that is another credit
--	---

	<p>institution or is a financial institution, the first payment made by the customer to the designated person for the provision of a product;</p> <p>(iv) in the case of a designated person that is another credit institution, the first occasion on which credit is received by the customer from the designated person or on which money is deposited with the designated person by the customer;</p> <p>(v) in the case of a designated person trading in goods in respect of transactions involving cash payments as referred to in section 25(1)(i) of the Act, the first such payment made by the customer to the designated person.</p>
	<p>138. The extent of the CDD in respect of non face-to-face customers will depend on the type of the product or service requested and the assessed money laundering risk presented by the customer. There are some circumstances where the customer is typically not physically present - such as in many wholesale markets, or when purchasing some types of collective investments - which would not in themselves, increase the risk attaching to the transaction or activity. A designated person should take account of such cases in developing their systems and procedures. Where third parties (that are not relevant third parties) are relied upon to carry out CDD and meet the customer this will be viewed as face to face identification for the purposes of the designated person's risk assessment.</p>
	<p>139. Additional measures would also include assessing the possibility that the customer is deliberately avoiding face-to-face contact. It is therefore important to be clear on the appropriate approach in these circumstances.</p>
	<p>SECTION V: RELIANCE ON THIRD PARTIES TO UNDERTAKE DUE DILIGENCE</p>
	<p>A. INTRODUCTION</p>
<p>Art 14 S.40 (3)</p>	<p>140. The Act provides for a designated person to rely on certain 'relevant third parties' to carry out part of the due diligence requirements. In order to meet the requirements of the Act, the designated person relying on the relevant third party must have an arrangement in place confirming that the relevant third party accepts being relied upon and that the relevant third party will provide, to the designated person, any due diligence documents or information obtained, as soon as practicable, upon request.</p>
<p>S.40 (4)</p>	<p><u>Section 40(4) of the Act states:</u></p> <p>A designated person may rely on a relevant third party to apply a measure under section 33 or 35(1) only if –</p> <p>(a) there is an arrangement between the designated person (or, in the case of a designated person who is an employee, the designated</p>

	<p>person’s employer) and the relevant third party under which it has been agreed that the designated person may rely on the relevant third party to apply any such measure, and</p> <p>(b) the designated person is satisfied, on the basis of the arrangement, that the relevant third party will forward to the designated person, as soon as practicable after a request from the designated person, any documents (whether or not in electronic form) or information relating to the customer that has been obtained by the relevant third party in applying the measure.</p> <p>141. A designated person may only rely on the ‘relevant third party’ to carry out the CDD measures required by section 33 and to obtain information on the intended nature of the business relationship as required by section 35 (1). It may not rely on a ‘relevant third party’ to fulfil the on-going monitoring requirements of section 35(3).</p> <p>142. The Act requires there to be a prior arrangement between the parties recognising that one is reliant on the other for the purposes set out above and that the designated person (relying on the relevant third party) is satisfied that the relevant documents and information will be furnished to the designated person, as soon as practicable, on request by the designated person. In the absence of such an arrangement the provisions of section 40(4) do not apply and the designated person must itself carry out the due diligence.</p> <p>143. A designated person relying on such a relevant third party to apply CDD measures remains liable for any failure to apply the measure. Failure to comply with the requirements of section 33 or 35 is an offence under the respective section.</p>
	<p>B. FOR WHAT PURPOSE CAN THIRD PARTIES BE RELIED UPON?</p>
<p>S.40 (5)</p>	<p>144. A designated person may rely upon certain relevant third parties to undertake due diligence measures required under <i>section 33</i> and/or to obtain information required under <i>section 35(1)</i>, in relation to a customer that the relevant third party proposes to introduce to it. However, under the Act, the designated person retains responsibility for ensuring that it’s customer due diligence obligations have been met.</p> <p>145. In addition, a designated person is responsible for ongoing monitoring of all customers and transactions, including where it has relied upon a relevant third party to meet its other customer due diligence obligations.</p>
	<p>146. Examples of circumstances where a designated person might rely on certain relevant third parties to undertake CDD measures and obtain information in relation to a customer include:</p> <ul style="list-style-type: none"> - Where a designated person enters into a business relationship with, or undertakes a transaction for, a customer through an intermediary who is acting as agent for the customer; - Where two designated persons are party to the same transaction with a

	<p>customer - e.g. a loan syndication or where an executing broker and a clearing broker are parties to the same transaction; and</p> <ul style="list-style-type: none"> - Where one member of a group introduces a customer to another member company of the same group. Group introductions are subject to the requirements of the Act and as such there must be an arrangement in place between the two parts of the Group recognising and accepting the fact that one is reliant on the other for the purposes set out above. <p>Section V of these Guidelines only deals with the reliance on relevant third parties as detailed in the Act and does not relate to introduced business, agency or outsourcing arrangements.</p> <p>147. Introduced Business:</p> <p>There is a difference between a relevant third party as detailed in this section and introduced business, where the person introducing may not have (now or in the future) a business relationship with the customer. In this case the designated person is not relying on the introducing party to perform CDD.</p> <p>In these circumstances, the CDD obligations lie with the designated person who is the product/service provider.</p> <p>148. Agency (agent of the designated person) and Outsourcing:</p> <p>A reference in the Act to a relevant third party on whom a designated person may rely to apply a measure under sections 33 or 35(1) does not include a reference to a person who applies the measure as an outsourcing service provider or an agent of the designated person.</p> <p>In such cases, the agent/outsourcee may actually obtain the appropriate verification evidence in respect of the customer but the product/service provider is responsible for specifying what should be obtained, and for ensuring that records of the appropriate verification evidence taken are retained in accordance with the Act. The agent/outsourcee in this case is viewed as an extension of the designated person. However the designated person remains liable for any failure to apply the measures required by section 33 or 35 (1)</p>
C. WHAT PARTIES CAN BE RELIED UPON?	
<p>Art 16</p> <p>S.40 (1)</p>	<p>149. “Relevant third party” means—</p> <ul style="list-style-type: none"> a) A person, carrying on business as a designated person in the State— <ul style="list-style-type: none"> i. that is a credit institution; ii. that is a financial institution (other than an undertaking that is a financial institution solely because the undertaking provides either foreign exchange services, or payment services, or both); iii. who is an external accountant or auditor and who is also a member of a designated accountancy body; iv. who is a tax adviser and who is also a solicitor or a member

	<p>of a designated accountancy body, or of the Irish Taxation Institute;</p> <ul style="list-style-type: none"> v. who is a relevant independent legal professional; or vi. who is a trust or company service provider, and who is also a member of a designated accountancy body a solicitor or authorised to carry on business by the Central Bank of Ireland; or <p>b) A person carrying on business in another Member State who is supervised or monitored for compliance with the requirements specified in the Third Money Laundering Directive, in accordance with Section 2 of Chapter V of that Directive, and is—</p> <ul style="list-style-type: none"> i. a credit institution authorised to operate as a credit institution under the laws of the Member State; ii. a financial institution (other than an undertaking that is a financial institution solely because the undertaking provides either foreign exchange services, or payment services, or both) and authorised to operate as a financial institution under the laws of the Member State; or iii. an external accountant, auditor, tax adviser, legal professional or trust or company service provider subject to mandatory professional registration or mandatory professional supervision under the laws of the other Member State; or <p>c) A person who carries on business in a place designated under <i>section 31</i> of the Act, is supervised or monitored in the place for compliance with requirements equivalent to those specified in the Third EU Money Laundering Directive, and is</p> <ul style="list-style-type: none"> i. a credit institution authorised to operate as a credit institution under the laws of the place; ii. a financial institution (other than an undertaking that is a financial institution solely because the undertaking provides either foreign exchange services, or payment services or both) authorised to operate as a financial institution under the laws of the place; or iii. an external accountant, auditor, tax advisor, legal professional or trust or company service provider subject to mandatory professional registration or mandatory professional supervision under the laws of the place.
	<p>D. WHAT OVERSIGHT OF RELEVANT THIRD PARTIES MUST BE UNDERTAKEN?</p>
	<p>150. The AML/CTF policy should set out the measures that the designated person undertakes to satisfy itself that the relevant third parties in question can be relied upon including:</p> <ul style="list-style-type: none"> - The regulatory status of the relevant third party and any adverse publicly available information regarding its compliance standards; - The experience the designated person has previously had in relying on the

	<p>relevant third party, in particular the promptness with which information relating to the identity of a customer is provided on request; and</p> <ul style="list-style-type: none"> - The designated person may also undertake a review of the relevant third parties' AML/CTF policies and procedures and level of compliance with the Act.
	<p>151. The Act allows for certain relevant third parties to be relied upon provided there is an arrangement between the designated person and the relevant third party. The designated person shall not rely on a relevant third party unless a written arrangement is in place between the designated person and the relevant third party. The arrangement that the designated person makes with the third party should deal with the following:</p> <ul style="list-style-type: none"> - an acknowledgement that the relevant third party is aware that the designated person is relying upon it for CDD purposes other than monitoring. - a confirmation of the group of customers for whom the arrangement is being given. - identification and verification of the identity of all customers introduced to the designated person. - identification of beneficial owners and verification of the beneficial owners identity (the extent of verification required will be dependent on the risk of money laundering and the financing of terrorism) such that the relevant third party can be reasonably satisfied that it knows who the beneficial owners are, as well as the ownership and control structures. - the provision to the designated person, as soon as practicable upon request by the designated person, of any and all documentation used by the relevant third party to identify the customer and beneficial owners as reasonably warranted by the risk of money laundering and the financing of terrorism. - the retention of any and all documentation used by the relevant third party to identify the customer and any beneficial owners for a period of at least five years after the business relationship with the customer has ended. - a commitment on the part of the relevant third party to obtain from the customer information on the purpose and intended nature of the business relationship between the designated person and the customer, and to furnish this information to the designated person, prior to the commencement of any such business relationship. - the designated person should take measures to satisfy itself that the procedures for implementing these measures are effective in a manner warranted by the risk of money laundering or terrorist financing. - where a customer who is an individual does not present to the relevant third party for verification in person ('non Face to Face'), the relevant third party shall address the additional risk presented by this scenario. <p>The manner in which the CDD measures are to be applied can be in compliance with the AML/CTF legislation and regulations which are applicable in the jurisdiction in which the relevant third party is carrying on business. The legislation/regulation applied by the relevant third party</p>

	<p>should be named in the agreement/arrangement with the relevant third party.</p> <p>The above is not an exhaustive list and it is for a designated person to decide if additional content is required in their arrangement.</p> <p>A designated person should consider whether it is appropriate to rely on a relevant third party which has in turn relied upon another relevant third party to meet its CDD obligations. In particular, whether it could oblige the other relevant third party to provide it with copies of identification and verification data where necessary.</p> <p>In instances where the third party is part of the same group of companies as the designated person, and can justifiably be deemed by the designated person to be a relevant third party for the purposes of the Act, the designated person may determine that an arrangement between the parties satisfies the requirements of the Act without necessarily being consistent with the form and content of the written arrangement outlined above. See Part H of this section for further information on group company reliance.</p>
	<p>E. CONDITIONS ATTACHING TO RELIANCE ON RELEVANT THIRD PARTIES</p>
	<p><u>Secrecy Jurisdictions</u></p> <p>152. In certain jurisdictions, banking secrecy and similarly restrictive legislation may prevent a relevant third party from forwarding documentation or information to the designated person, as required by section 40(4) of the Act. Consequently, before placing reliance upon on relevant third parties based in such jurisdictions, the designated person shall ensure that it has fully satisfied itself that, in placing such reliance, it can meet its obligations under the Act.</p> <p><u>Initial Information</u></p> <p>153. Although the Act allows designated persons to rely on certain third parties to apply measures contained within sections 33 and 35(1) of the Act, the requirement remains for the designated person to be in possession of information on the purpose and intended nature of a business relationship with a customer, prior to the establishment of the relationship.</p> <p>Furthermore, as the Act prohibits the establishment of anonymous accounts, the designated person shall ensure that it knows the identity of the customer and, where relevant, any beneficial owners, prior to the commencement of the business relationship, occasional transaction or provision of a service.</p> <p>The initial requirements may be summarised as follows:</p> <ul style="list-style-type: none"> i. The identity of the customer; ii. Confirmation that the relevant third party has verified the identities

	<p>of the customer and the identity of any beneficial owner(s) (the extent of verification required in respect of beneficial owners will depend on the level of risk) it is introducing; and</p> <p>iii. The purpose and intended nature of any proposed business relationship with the customer.</p> <p><u>Politically Exposed Persons (PEPs)</u></p> <p>154. In the case of PEPs, although a designated person may rely on a relevant third party to perform the due diligence measures required under <i>section 33</i>, the designated person may not rely on the relevant third party to perform the enhanced due diligence measures required by <i>section 37</i> of the Act.</p> <p>However, one of the steps a designated person may take to determine whether a customer/beneficial owner is a PEP is to rely on a relevant third party to gather the documentation/information which would allow an appropriate determination to be made by the designated person. Once a customer/beneficial owner is determined as being a PEP, the designated person must take the enhanced CDD measures which are as outlined in section 37(4). The relevant third party may however provide assistance to the designated person in gathering the documentation/information which would assist in determining the source of wealth and source of funds for transactions with the PEP.</p> <p><u>‘Non-Face to Face’ Identification</u></p> <p>155. Where relevant third parties are relied upon to carry out CDD and meet the customer this will be viewed as face to face identification for the purposes of the designated persons risk assessment.</p> <p><u>Jurisdictions Designated under Section 31 of the Act</u></p> <p>156. Although the Minister for Justice and Equality has powers under section 31 of the Act to designate countries not directly subject to the Third Money Laundering Directive but which the Minister is satisfied impose requirements equivalent to the Third Money Laundering Directive, designated persons are still expected to include any such countries in any risk assessment they are required to perform. While the designation pursuant to section 31 is a significant factor, designated persons should have regard to any specific jurisdictional issues that might nonetheless arise. (See Paragraph 55)</p>
	<p>F. ONGOING MONITORING</p>
<p>S.35(3)</p>	<p>157. A designated person is not permitted to rely upon a relevant third party to undertake, on its behalf, ongoing monitoring of customer transactions and the customer relationship.</p> <p><u>Section 35(3) of the Act states:</u></p> <p>158. A designated person shall monitor dealings with a customer with whom the person has a business relationship, including (to the extent reasonably warranted by the risk of money laundering or terrorist financing) by scrutinising</p>

	<p>transactions and the source of wealth or of funds for those transactions, to determine whether or not the transactions are consistent with—</p> <ul style="list-style-type: none"> (a) the person’s knowledge of the customer and the customer’s business and pattern of transactions, and (b) any knowledge that the person may have that the customer may be involved in money laundering or terrorist financing. <p>As a result, the designated person must obtain sufficient information in relation to the customer at the outset to undertake the necessary monitoring according to its assessment of the risk presented by the customer or the products or services being provided to the customer. This information should be sourced by the designated person directly or it may be sourced from relevant third parties. It is also important that a designated person keeps its records and information up to date in relation to the customer in the normal course of business.</p>
	<p>G. RESPONSIBILITY FOR RECORD KEEPING AND PROVISION</p>
<p>S.55(1)&(2)</p>	<p>159. A designated person is required to retain the documents and information used to comply with Chapter 3 of the Act.</p> <p><u>Sections 55(1)&(2) of the Act state:</u></p> <ul style="list-style-type: none"> (1) A designated person shall keep records evidencing the procedures applied, and information obtained, by the designated person under Chapter 3 in relation to— <ul style="list-style-type: none"> (a) each customer, and (b) in the case of a designated person to whom section 38 applies, each correspondent banking relationship. (2) Without prejudice to the generality of subsection (1), a designated person shall take the original or a copy of all documents used by the designated person for the purposes of Chapter 3, including all documents used to verify the identity of customers or beneficial owners in accordance with section 33. <p>Where reliance is placed on a relevant third party to obtain the required due diligence, the designated person relying on such documents and information should ensure that the requirements in relation to this section are embedded in their arrangement with the relevant third party, in order to meet their obligations under the Act. The relevant third party must clearly understand the extent of the reliance on them and the necessity for them to provide, to the designated person, such documents and information, should they be required.</p> <p>Where a designated person places reliance on a relevant third party, whether it be a group company or otherwise, to enable it to meet its</p>

<p>S.40(4)(b)</p>	<p>obligations under <i>sections 33 and 35(1)</i>, the designated person must ensure that it meets its obligations under <i>section 40(4)(b)</i> of the Act.</p> <p><u>Section 40(4)(b) of the Act states:</u></p> <p>“the designated person is satisfied, on the basis of the arrangement, that the relevant third party will forward to the designated person, as soon as practicable after a request from the designated person, any documents (whether or not in electronic form) or information relating to the customer that has been obtained by the relevant third party in applying the measure.”</p> <p>Furthermore, the designated person also needs to remember its obligations under <i>sections 55 and 56</i> of the Act. These Sections of the Act are dealt with in Section VIII of the core guidelines.</p> <p>Specific care should be exercised in setting out how due diligence information and documents collected at the outset by a relevant third party can be passed to the designated person relying on that fact, should a customer relationship cease to exist or should a relevant third party itself cease to operate. A designated person must ensure that they are aware of the specific requirements of the Act when reliance is placed on a relevant third party and such arrangements should not be entered into lightly.</p> <p><u>Section 40(5) of the Act states:</u></p>
	<p>H. GROUP INTRODUCTIONS</p>
	<p>160. Designated persons may rely on a group company to apply measures contained in sections 33 and 35(1), on their behalf, only where that group company meets the definition of a relevant third party contained in section 40(1) of the Act.</p>
	<p>161. Where a customer is introduced to a designated person by a relevant third party within the same group of companies as the designated person, it is not necessary for the customer’s identity to be re-verified, provided that:</p> <ul style="list-style-type: none"> - There is an arrangement between the designated person and the relevant group company, under which it has been agreed that the designated person may rely on the group company to apply such measures; - The identity of the customer has been verified by the introducing part of the group; and - The group entity that carried out the CDD measures meets the definition of a third party that can be relied upon, as set out above.

	<p>The manner in which the CDD measures are to be applied can be in compliance with the AML/CTF legislation and regulations which are applicable in the jurisdiction in which the relevant third party is carrying on business. The legislation/regulation applied by the relevant third party should be named in the agreement/arrangement with the relevant third party.</p>
	<p>I. BUSINESS ACQUISITIONS</p>
<p>S.33(1)(d)</p>	<p>162. Where a designated person acquires the business or an element of the business of another entity, re-verification of its customers will not be necessary if the acquired entity is regulated and supervised:</p> <ul style="list-style-type: none"> (a) in the EU for compliance with the Third EU Money Laundering Directive; or (b) to a standard equivalent to the Third EU Money Laundering Directive in a jurisdiction designated under section 31 of the Act, by the Minister. <p>Notwithstanding this, a designated person must comply with the requirements of section 33(1)(d) of the Act, in relation to doubts about the veracity and adequacy of the documents and information obtained in relation to those customers.</p> <p>Section 33(1)(d) of the Act states:</p> <p>A designated person shall apply the measures specified in subsections (2) and, where applicable, (4), in relation to a customer of the designated person—</p> <p>(d) prior to carrying out any service for the customer if—</p> <ul style="list-style-type: none"> (i) the person has reasonable grounds to doubt the veracity or adequacy of documents (whether or not in electronic form) or information that the person has previously obtained for the purpose of verifying the identity of the customer, whether obtained under this section or section 32 of the Criminal Justice Act 1994 (“the 1994 Act”) prior to its repeal by this Act or under any administrative arrangements that the person may have applied before section 32 of the 1994 Act operated in relation to the person, and (ii) the person has not obtained any other documents or information that the person has reasonable grounds to believe can be relied upon to confirm the identity of the customer. <p>In order to comply with the Act it will be necessary for all underlying records on customer due diligence be passed to the acquiring business.</p> <p>Designated persons should seek a confirmation from the acquired entity, or by the vendor where a portfolio of customers or business has been acquired, that CDD has been carried out. The designated person acquiring the business must be satisfied with the representations made in the confirmation.</p> <p>It is, however, important that the designated person’s due diligence inquiries</p>

	<p>include some sample testing in order to confirm that the customer identification procedures previously followed by the acquired entity (or by the vendor, in relation to a portfolio) have been carried out in accordance with the Act or its equivalent under (a) or (b) above.</p>
--	---

In the event that the sample testing of the customer identification procedures previously undertaken shows that these have not been carried out to the required standard, procedures cannot be examined for completeness or the customer records are not available to the designated person, verification of identity will need to be undertaken as soon as is practicable for all transferred customers who are not existing verified customers of the designated person.

	<p>SECTION VI: INTERNAL POLICIES AND PROCEDURES</p>
	<p>A. INTRODUCTION</p> <p>164. This section provides guidance on the internal controls that will help designated persons meet their obligations in respect of the detection and prevention of money laundering and terrorist financing. Guidance is provided in Section III, D, of the guidelines on the adoption of policies and procedures in respect of AML/CTF and it should be read in conjunction with this section. It should also be noted that there are a range of other legal and regulatory obligations on designated persons to maintain appropriate records and implement controls. This guidance is not intended to replace or interpret such wider obligations.</p>
<p>Art 34 S.54, 55</p> <p>S. 33, 35</p> <p>S. 33(1)(d)</p> <p>S. 37</p>	<p>B. WHAT DOES THE ACT REQUIRE?</p> <p>165. Designated persons are obliged to adopt and implement adequate policies and procedures appropriate to their business to prevent and detect the commission of money laundering and terrorist financing and in particular to address their obligations under all of Part 4 of the Act (sections 24 to 109). At a minimum, the policies and procedures should address the following obligations but readers should consult the relevant sections of these guidelines for further detail on the specific requirements;</p> <ul style="list-style-type: none"> - CDD (Section IV) including; <ul style="list-style-type: none"> o identification and verification of customers and beneficial owners (the extent of verification required in respect of beneficial owners will depend on the risk). o obtaining reasonably warranted information on the purpose and intended nature of the business relationship. o conducting ongoing monitoring of the business relationship with the customer including scrutiny of transactions and the source of wealth or of funds for those transactions. o Keeping CDD information up-to-date o Application of enhanced, additional and simplified customer due diligence. - CDD in respect of existing customers (Section II). - In respect of PEPs (Section IV); <ul style="list-style-type: none"> o steps to be taken to determine whether or not a customer, or a beneficial owner connected with the customer or service concerned, being a customer or beneficial owner residing in a place outside the State, is a PEP or an immediate family member, or a close associate of a PEP. o steps to be taken where the designated person knows or has reasonable grounds to believe that a customer residing in a place outside the State is a PEP or an immediate family member, or close associate of a PEP. o steps to be taken where the designated person knows or has reasonable grounds to believe that a beneficial owner residing in a place outside the State, and connected with a customer or with a service sought by a customer, is a PEP or an immediate family member or close associate of

	a PEP.
S. 54(3)(a)	<ul style="list-style-type: none"> - Identification and scrutiny of complex or large transactions, unusual patterns of transactions that have no apparent economic or visible lawful purpose and any other activity that the designated person has reasonable grounds to regard as particularly likely, by its nature, to be related to money laundering or terrorist financing.
S. 54(3)(b)	<ul style="list-style-type: none"> - Measures to be taken in respect of transactions or products that could favour or facilitate anonymity so as to prevent money laundering or terrorist financing. - Risk Assessment and Management (Section III) including: <ul style="list-style-type: none"> o role of senior management in the design and implementation of a risk based approach. o identification and categorisation of risks of money laundering and or terrorist financing arising from the designated person's business. o mitigation and management of risks identified in an effective and proportionate manner. o maintenance of meaningful records of implementation decisions.
S. 42, 43	<ul style="list-style-type: none"> - Reporting (Section VII) including; <ul style="list-style-type: none"> o Reporting of suspicious transactions to the FIU and Revenue Commissioners. o Reporting of transactions involving places designated under <i>section 32</i>. o Internal and external reporting procedures. o Actioning of directions and orders received from An Garda Síochána and the District Court.
S. 55	<ul style="list-style-type: none"> - Recordkeeping (Section VIII) including; <ul style="list-style-type: none"> o Type of records which must be maintained. o Location at which records must be kept. o Record retention periods. o Formats in which records are to be kept.
S. 40	<ul style="list-style-type: none"> - Reliance on relevant third parties (Section V) including; <ul style="list-style-type: none"> o Commitments to be sought from relevant third parties in terms of; <ul style="list-style-type: none"> - identification and verification of customers and beneficial owners. - provision upon request of CDD documentation obtained. - information to be obtained on the purpose and intended nature of the business relationship with the customer and the provision of such

<p>S. 57</p> <p>S. 54</p> <p>S. 54</p> <p>S. 54</p> <p>S. 54</p> <p>S. 54</p>	<p>information to the designated person.</p> <ul style="list-style-type: none"> ○ procedures to be followed where a relevant third party is based in a jurisdiction subject to secrecy requirements. ○ procedures to be adopted in relation to ongoing monitoring of customers. ○ responsibilities for recordkeeping. <p>- Branches or subsidiaries (Section II.A) including;</p> <ul style="list-style-type: none"> ○ Application of certain requirements to branches and subsidiaries in non-Member States (where applicable). <p>- Training of staff (Section IX) including;</p> <ul style="list-style-type: none"> ○ Identification of “persons involved in the conduct of the designated person’s business” i.e. relevant staff for the purposes of receiving training. ○ Material to be addressed in training. ○ Method and regularity of training. ○ Other awareness raising methods. <p>- Internal controls.</p> <p>- Monitoring and management of compliance with all of the policies and procedures listed above.</p> <p>- Internal communication of all of the policies and procedures listed above.</p>
	<p>166. The implementation of policies and procedures as identified above will necessitate the development and operation of a set of systems and controls by the designated person. The nature and extent of such systems and controls will depend on a variety of factors, including:</p> <ul style="list-style-type: none"> -The nature, scale and complexity of the designated person’s business; -The diversity of its operations, including geographical diversity; -Its customer, product and activity profile; -Its distribution channels; -The volume and size of its transactions; and -The degree of risk associated with each area of its operation.
	<p>167. The systems and controls which are required to be established, implemented and maintained should cover:</p> <ul style="list-style-type: none"> - Adequate procedures for recruitment in accordance with normal business practice to ensure high standards when hiring employees. Such procedures should be appropriate to the level of risk of money laundering or terrorist

	<p>financing associated with the position being filled and also to the level of seniority of the position.</p> <ul style="list-style-type: none"> - Appropriate training on money laundering and terrorist financing to ensure that relevant personnel are aware of, and understand, their legal and regulatory responsibilities and their role in 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. (See Section IX on Training); - Appropriate provision of regular and timely information to senior management relevant to the management of the designated person’s AML-CTF risks; - Appropriate documentation of the designated person’s risk assessment and management policies and procedures; - Appropriate measures to ensure that the risks of money laundering and terrorist financing are taken into account in the day-to-day operation of the designated person, including in relation to: <ul style="list-style-type: none"> 1. the development of new products; 2. the taking-on of new customers; and, 3. changes in the designated person’s business profile. 4. The threats arising from new technologies. - Appropriate documented internal and external reporting procedures to ensure prompt reporting of knowledge, suspicion, or reasonable grounds to suspect money laundering and terrorist financing. - Appropriate documented procedures to ensure that there is validation of AML/CTF policies and procedures including the performance of risk assessment and management processes and of related internal controls. This testing and reporting should be conducted by, for example, the internal audit department, external auditors, compliance monitoring, specialist consultants or other qualified parties who are independent of the implementation or operation of the financial institution’s AML/CTF compliance programme. The testing should reflect the size and complexity of the designated person’s business and focus on the risks inherent in the designated person’s business. It should evaluate the adequacy of the financial institution’s overall AML/CTF programme and the quality of risk management for the financial institution’s operations, departments and subsidiaries. It should also include appropriate and comprehensive testing procedures for all relevant business units. <p>The board of directors (or equivalent) and senior management of the designated person should ensure that there are sufficient resources available to the designated persons’ AML/CTF programme, including appropriate staff and technology.</p>
S.54 (4)	168. The designated person should ensure that appropriate monitoring processes and procedures across the designated person are established and maintained so

	that regular assessments of the adequacy of its systems and controls to ensure that they manage the money laundering risk effectively are undertaken.
	169. As appropriate to the nature and scale of the designated persons activities, an annual report should be given to senior management and the board, if applicable, which assesses the operation and effectiveness of the designated person's systems and controls in relation to managing money laundering and terrorist financing risk.
	C. SENIOR MANAGEMENT's RESPONSIBILITIES AND THE ROLE OF THE MONEY LAUNDERING REPORTING OFFICER (MLRO)
	170. Section III of the guidelines outlines the importance of the role of senior management (and the board of directors or equivalent) in implementing a designated person's AML/CTF policy. While ultimate responsibility will always rest with the board of directors, designated person's may decide to allocate overall responsibility for the establishment and maintenance of effective AML/CTF systems and controls to a member of senior management.
	171. Although the Act does not require designated persons to appoint officers to the role of MLRO, the role of Head of Compliance with responsibility for AML/CTF legislation is a pre-approval controlled function in the context of the Central Bank Reform Act 2010 (Sections 20 and 22) Regulations 2011.
	<p>172. Money Laundering Reporting Officer</p> <p>The MLRO has the role of ensuring communication of reports of suspicious transactions to the FIU and the Revenue Commissioners and acts as a liaison between the designated person and the FIU and the Revenue Commissioners. However, <i>section 41</i> of the Act makes clear that the requirement for designated persons to report suspicious transactions extends to any person acting on behalf of the designated person including any agent, employee, partner, director or other officer of, or any person engaged under a contract for services with, the designated person. Further detail on the reporting obligations of designated persons may be found at Section VII of these guidelines.</p>
	173. The MLRO has a significant degree of responsibility and should be familiar with relevant aspects of the Act and these guidelines. He/she is required to determine whether the information or other matters contained in the suspicious transaction he/she has received via any internal reporting procedure merit the making of a report to the FIU and the Revenue Commissioners. A formal register should be maintained by the MLRO of all suspicious transactions reports, the determinations made, any subsequent reports made to the FIU and the Revenue Commissioners and any further correspondence sent or received. Where the MLRO decides not to make a report to the FIU and Revenue Commissioners, a record of that fact should be recorded together with the reason/s for not making the report.
	174. In order to carry out the role, the MLRO should have sufficient knowledge of the designated person, its products, services and systems. He/she should

	<p>have the authority to act independently and autonomously in carrying out his/her responsibilities. The MLRO should be free to have direct access to the FIU, Revenue Commissioners or to any supervisory body, in order that any suspicious activity can be reported to the appropriate bodies as soon as is practicable after acquiring the relevant knowledge, forming the suspicion or acquiring reasonable grounds to suspect that a person has been or is engaged in money laundering or terrorist financing.</p>
	<p>175. The competent authority should be mindful of the sensitivity of the MLRO position, particularly in smaller designated persons and should take steps to protect the position of the reporter.</p>
<p>SECTION VII: REPORTING OF SUSPICIOUS TRANSACTIONS</p>	
<p>A. INTRODUCTION</p>	
	<p>176. The Act requires that designated persons must report to the Garda Síochána Financial Intelligence Unit (“FIU”) and Revenue Commissioners, known or suspected instances of money laundering or terrorist financing or where they have reasonable grounds to suspect such instances. In addition, designated persons must report any services or transactions provided or carried out by the designated person, which are connected with a place that is designated under section 32 of the Act. The FIU is a national centre for receiving and analysing suspicious transaction reports and other information regarding potential money laundering or terrorist financing.</p> <p>This section addresses the various aspects of the reporting process and the associated offence of tipping off. The various Directions and Orders available to members of the Garda Síochána and the District Court are also addressed in this Section.</p> <p>For a detailed description of the offences of money laundering and terrorist financing please see Section I, C & D of these guidelines.</p>
<p>B. WHAT DOES THE ACT REQUIRE?</p>	
<p>Art 22 (1)(a) S.42 (1) S. 33(8)</p>	<p>177. Designated persons (including agents, employees, partners, directors, other officers or any person engaged under a contract for services with the designated person) who know, suspect or have reasonable grounds to suspect that money laundering or terrorist financing is being, or has been committed or attempted, must report that suspicion to the FIU and Revenue Commissioners.</p> <p>178. Where as a result of any failure on the part of the customer to provide the necessary documents or information, a designated person is not able to;</p> <ul style="list-style-type: none"> - identify and verify a customer/beneficial owner’s identity, or,

<p>Art 9(5) S. 42(4)</p> <p>S. 43</p> <p>S. 42(1) & S. 43(1)</p> <p>S.6 and S.7</p>	<ul style="list-style-type: none"> - obtain sufficient information about the purpose and intended nature of business relationship with a customer, or, - apply enhanced customer due diligence measures in respect of PEPs as specified in <i>section 37</i> of the Act, <p>and this gives rise to a suspicion that money laundering or terrorist financing is being, or has been committed or attempted, then the designated person should consider making a report to the FIU and Revenue Commissioners.</p> <p>179. Designated persons must also report to the FIU and Revenue Commissioners any service or transaction that the designated person provides or carries out, which is connected with a place that is designated under section 32 of the Act.</p> <p>180. The obligation to make a report under section 42 of the Act only applies where the knowledge, suspicion or reasonable grounds for suspicion of the designated person arises on the basis of information obtained in the course of carrying on business as a designated person. Similarly, the service or transaction which is referred to in section 43 of the Act must be provided or carried out by the designated person in the course of carrying on business as a designated person.</p> <p>181. It should be noted that there may be a chain of criminal offences, all of which may be reported to An Garda Síochána. Money laundering is a derivative crime in that the monies being laundered are derived from another criminal activity. The initial criminal activity is known as the predicate offence. Where the designated person is aware of the nature of any predicate offence, it may be reported as normal through the usual channels e.g. to local Garda Síochána and where an act occurs in relation to the proceeds of the predicate offence (which gives rise to a suspicion of money laundering or an attempt to launder money) then that act should be reported by way of suspicious transaction report (STR) to the FIU and the Revenue Commissioners.</p> <p>182. Occasionally, there may be situations where a report should be made through usual channels together with a STR to the FIU and Revenue Commissioners. For example, the designated person may be the subject of a crime e.g. fraud or phishing. In this case, the double reporting may occur where the fraud is reported through the fraud reporting system but there will also be proceeds of crime and should be reported through the STR process.</p>
	<p>C. TIMING OF REPORTS</p>
<p>S. 42(2) & 42(3)</p>	<p>183. The designated person must make the report as soon as practicable after acquiring the knowledge or forming the suspicion, or acquiring reasonable grounds to suspect that money laundering or terrorist financing is being, or has been committed or attempted. However, a designated person is taken not to have reasonable grounds to know or suspect that another person commits an offence on the basis of having received information until the person has scrutinised the information in the course of reasonable business practice (including automated banking transactions).</p>
	<p>D. KNOWLEDGE, SUSPICION AND REASONABLE GROUNDS FOR</p>

	SUSPICION –
	<p>Knowledge</p> <hr/> <p>184. Having knowledge means actually knowing something to be true. In a criminal court, it must be proven that the individual in fact knew that a person was engaged in money laundering or terrorist financing.</p>
<p>Queensland Bacon PTY Ltd V Rees [1966]</p> <p>Da Silva [2006] EWCA Crim 1654</p>	<p>Suspicion</p> <hr/> <p>185. Suspicion is more subjective and falls short of proof based on firm evidence. UK and Australian case law, which may be influential but not binding in an Irish Court, suggests that suspicion is a state of mind more definite than speculation, but falls short of knowledge based on evidence. It must be based on evidence, even if that evidence is tentative – simple speculation that a customer may be money laundering or terrorist financing is not sufficient grounds to form a suspicion. Suspicion has been defined by the courts as being beyond mere speculation and based on some foundation, for example:</p> <ul style="list-style-type: none"> - "A suspicion that something exists is more than mere idle wondering whether it exists or not; it is a positive feeling of actual apprehension or mistrust, amounting to a slight opinion, but without sufficient evidence" and - "It seems to us that the essential element in the word "suspect" and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice" - A transaction which appears unusual is not necessarily suspicious. Even customers with a stable and predictable transactions profile will have periodic transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. So the fact that a transaction appears unusual is, in the first instance, only a basis for further enquiry, which may in turn require judgment as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises. A member of staff who considers a transaction or activity to be suspicious, would not be expected either to know or to establish the exact nature of any underlying criminal offence, or that the particular funds or property were definitely those arising from a crime or terrorist financing.

Reasonable Grounds For Suspicion	
	<p>186. In addition to imposing a legal obligation to make a report when there is a suspicion or actual knowledge of money laundering or terrorist financing, the Act requires a report to be made when reasonable grounds exist for suspecting that a person is engaged in money laundering or terrorist financing. This introduces an objective test of suspicion – designated persons and their directors and personnel will not be able to rely on an assertion of ignorance or naivety where this would not be reasonable to expect of a person with their training and position. The test would likely be met when there are demonstrated to be facts or circumstances, known to the member of staff, from which a reasonable person engaged in a business, subject to the Act, would have formed the suspicion, that another person was engaged in money laundering or terrorist financing. Staff within designated persons need to be able to demonstrate that they took reasonable steps in the particular circumstances, in the context of a risk-based approach (where applicable), to know the customer and the rationale for the transaction, activity or instruction. It is important to bear in mind that, in practice, a court may decide, with the benefit of hindsight, whether the objective test has been met.</p>
	<p>187. “Reasonable grounds” should not be confused with the existence of higher than normal risk factors which may affect certain sectors or classes of persons. For example, cash-based businesses or complex overseas trust and company structures may be capable of being used to launder money, but this capability of itself is not considered to constitute ‘reasonable grounds’.</p>
	<p>188. Existence of higher than normal risk factors require increased attention to gathering and evaluation of customer information, and heightened awareness of the risk of money laundering or terrorist financing in performing professional work, but do not of themselves require a report of suspicion to be made. For ‘reasonable grounds’ to come into existence, there needs to be sufficient information to advance beyond speculation that it is merely possible someone is laundering money or terrorist financing, or a higher than normal incidence of some types of crime in particular sectors.</p>
	<p>189. It is important that staff do not turn a blind eye to information, but make reasonable enquiries such as a professional with their qualifications, experience and expertise would reasonably be expected to make in such a situation within the normal scope of their assignment or client relationship, and draw a reasonable conclusion such as should be expected of a person of their standing. A healthy level of professional scepticism should be maintained, and if unsure of the action that should be taken, consult with the MLRO or other appropriate person in accordance with the designated person’s internal reporting process. If in doubt, personnel should err on the side of caution and make a report to the MLRO or through the designated person’s internal reporting process.</p>

Art 26 S.47	190. Section 47 provides that the disclosure of information by a person in accordance with Chapter 4 shall not be treated, for any purpose as a breach of any restriction imposed by any other enactment or rule of law on disclosure by the person or any other person on whose behalf the disclosure is made.
S.83	191. Similarly, by virtue of section 83, any disclosure or production of information or document by a person in accordance with Chapter 8 of the Act (monitoring of designated persons), shall not be treated as a breach by the person of any restriction under any enactment or rule of law on disclosure or production.
S.112	<p>192. Section 112 of the Act also contains protection from breach of any restriction on the disclosure of information imposed by any enactment or rule of law for disclosures made in good faith to a member of the Garda Síochána (or to any person who is concerned in the investigation or prosecution of an offence of money laundering or terrorist financing) of;</p> <ul style="list-style-type: none"> - a suspicion that any property has been obtained in connection with any such offence, or derives from property so obtained, or, - any matter on which such a suspicion is based. <p>193. However, section 112 does not afford any protection to a person making a report maliciously.</p>
	194. Designated persons should remain vigilant for any additional activities undertaken by, or instructions from, any customer in respect of which a disclosure has been made, and should submit further reports, to the FIU and Revenue Commissioners, as appropriate. The making of such a report should feed into the designated person's risk based assessment of the customer. The Act does not impose a prohibition on providing further products and services for customers about whom a report has been made. However, a designated person must comply with any direction or order received pursuant to section 17 of the Act.
	E. WHEN REPORTS DO NOT HAVE TO BE MADE
Art 9 (5) Art 23 (2) S.46	195. As set out in section 46 of the Act, information that is subject to legal privilege is not required to be disclosed and nor is a relevant professional adviser (as defined in section 24) required to disclose information that he or she has received from or obtained in relation to a client in the course of ascertaining the legal position of the client, so long as he or she did not do so with a criminal purpose. In any case, where the information is not legally privileged, then it must be reported as normal.

	<p>196. Whether or not non-disclosure of legally privileged information is permissible needs to be considered carefully. It is strongly recommended that a careful record is maintained of the status of information considered when a decision is made on the applicability of section 46 of the Act. Section 47 provides that the disclosure of information by a person in accordance with Chapter 4 shall not be treated, for any purpose as a breach of any restriction imposed by any other enactment or rule of law on disclosure by the person or any other person on whose behalf the disclosure is made.</p>
	<p>197. For further reading on the meaning of legal privilege please refer to guidance produced by the relevant competent authorities (e.g. Law Society of Ireland, Irish Taxation Institute etc.) and to leading textbooks on the law of evidence.</p>
<p>F. THE INTERNAL REPORTING PROCESS</p>	
s.44	<p>198. All designated persons should put in place an internal reporting process for the purpose of complying with their obligations under the Act to report suspicious transactions and transactions connected to certain places. The obligation to report is placed upon the designated person which includes any person acting, or purporting to act, on behalf of designated person, including any agent, employee, partner, director or other officer of, or any person engaged under a contract for services with, the designated person. Reports must be made to the FIU and Revenue Commissioners in accordance with the Act. All members of staff should be obliged to make a report via the internal reporting process where they have knowledge or suspicion, or reasonable grounds for suspicion, of money laundering or terrorist financing. Some designated persons may choose to require that such unusual or suspicious transactions be drawn initially to the attention of supervisory management to ensure that there are no known facts that will negate the suspicion before further reporting via the internal reporting process. However, reports must be made to the FIU and Revenue Commissioners as soon as practicable and this should be factored into any such consultations.</p>
s. 44(2)	<p>199. Where, or if, a member of staff consults colleagues, the legal obligation remains with the staff member to decide for him/herself whether a report should be made; he/she should not allow colleagues to decide for him/her. Where a colleague has been consulted, the colleague will then have knowledge on the basis of which he/she must consider whether a report in accordance with the designated person's reporting process is necessary. Once a member of personnel has reported his/her suspicion in an appropriate manner via the internal reporting process he/she has fully satisfied his/her statutory obligation. The Act provides a defence for a person charged with a failure to report, to prove that the person was, at the time of the purported offence, an employee, who made a report in accordance with such an internal reporting procedure to another person.</p>
	<p>200. All suspicions reported via the internal reporting process should be recorded. The report should include appropriate details of the customer who is the subject of concern and as full a statement as possible of the information giving rise to the knowledge or suspicion or the basis for the reasonable grounds of the</p>

	<p>suspicion. All internal enquiries made in relation to the report should also be documented, or recorded electronically. This information may be required to supplement the initial report or as evidence of good practice and best endeavours if, at some future date, there is an investigation and the suspicions are confirmed or disproved.</p>
	<p>201. Further transactions or activity in respect of the customer about whom a STR has been made, whether of the same nature or different from that giving rise to the previous suspicion, should be reported to the MLRO in accordance with the designated person’s internal reporting process as they arise.</p>
	<p>202. The MLRO or any other person(s) charged under a designated person’s internal reporting process with making a report to the FIU and Revenue Commissioners must review each report and determine whether it gives rise to knowledge or suspicion, or reasonable grounds for suspicion. The designated person should permit that relevant individual to have access to any information, including CDD information, in the designated person’s possession which could be relevant. The designated person may also require further information to be obtained, from the customer if necessary, or from an intermediary who introduced the customer to the designated person, to the extent that the introducer still holds the information (bearing in mind his or her own record keeping requirements). Any approach to the customer, third party or to the intermediary should be made sensitively and probably by someone other than a person with a recognised external reporting responsibility, to minimise the risk of alerting the customer or an intermediary that a disclosure to the FIU and Revenue Commissioners is under consideration. To do otherwise could potentially alert the customer to the possibility of a report.</p>
	<p>203. When considering an internal suspicion report, the MLRO or other any person charged under a designated person’s internal reporting process with making a report to the FIU and Revenue Commissioners, taking account of the risk posed by the transaction or activity being addressed, will need to strike the appropriate balance between the requirement to make timely disclosure to the FIU and Revenue Commissioners and any delay that might arise in searching a number of unlinked systems and records that might hold relevant information. But, it is important to bear in mind the requirement to make a report as soon as practicable after acquiring the knowledge or forming the suspicion, or acquiring those reasonable grounds to suspect.</p>
	<p>204. As part of the review, other known connected accounts or relationships may need to be examined. Connectivity can arise commercially (through linked accounts, introducers, etc.), or through individuals (third parties, controllers, signatories etc.). Given the need for timely reporting, it may be prudent to make the report to the FIU and Revenue Commissioners prior to completing a full review of linked or connected relationships but also to notify them that supplemental information may be provided.</p>
	<p>205. If the designated person decides not to make a report to the FIU and Revenue Commissioners, that outcome should be recorded, together with the reasons for not doing so and the record should be retained in an accessible manner. However, if later on further activities by the customer give rise to a heightened</p>

	<p>suspicion of money laundering or terrorist financing then the designated person should ensure that any report made includes the information that was originally considered in the decision not to report at that time, if this information adds sufficient value.</p>
	<p>G. PROCESS FOR REPORTING TO THE FIU AND REVENUE COMMISSIONERS</p>
<p>Art 22 (1)(a) S.42 (1)</p>	<p>206. Any person(s) charged under a designated person’s internal reporting process with making a report to the FIU and Revenue Commissioners, for example the MLRO, must report to the FIU and Revenue Commissioners any transaction or activity that, after his/her evaluation, he/she knows or suspects, or has reasonable grounds to suspect, may be linked to money laundering or terrorist financing. A designated person is taken not to have reasonable grounds to know or suspect that another person commits an offence on the basis of having received information until the person has scrutinised the information in the course of reasonable business practice (including automated banking transactions). The designated person or MLRO shall make the report as soon as practicable after acquiring that knowledge or forming that suspicion, or acquiring those reasonable grounds to suspect, that the other person has been or is engaged in money laundering or terrorist financing.</p>
	<p>207. Reports in relation to money laundering/terrorist financing suspicions are to be made to:</p> <p>Garda Bureau of Fraud Investigation Financial Intelligence Unit Harcourt Square Harcourt Street Dublin 2 Tel +3531 6663712/4 Fax +3531 6663711</p> <p>Office of the Revenue Commissioners Suspicious Transactions Reports Office Block D Ashtowngate Navan Road Dublin 15 Tel: +353 1 8277542 Fax: +353 1 8277484</p>

	<p>208. Reports can be forwarded by post or in urgent cases by facsimile message. However, in some instances, it may be appropriate to make initial telephone contact with the FIU before following up with a written or faxed copy of the report. The FIU of the Garda Bureau of Fraud Investigation and the Suspicious Transaction Reports Office in the Revenue Commissioners also operate an encrypted email system for accepting reports electronically (FIDOL). They do not accept unencrypted emails. Use of the system is not obligatory. Designated persons currently not accessing the system and who wish to, should contact the FIU.</p>
Art 22 (1)(b)	<p>209. Note that where further information is sought from the designated person in relation to a report, the Act requires that designated persons must furnish the FIU and Revenue Commissioners at their request, with all necessary information as soon as possible.</p>
	<p>210. In responding to such information requests, designated persons should:</p> <ul style="list-style-type: none"> - Be satisfied that the request is from an appropriate and bona-fide member of the Garda Síochána or Revenue Commissioners; and - Consider whether the request requires simply a clarification of the content of the original report or whether responding would involve the production of documents or provision of information additional to the information provided in the report.
	<p>211. Where the request involves the production of additional documentation or the provision of additional information, the designated person, before responding, will need to understand:</p> <ul style="list-style-type: none"> - The authority under which the request is made; - The extent of the information requested; - The required timing and manner of production of the information; and - Whether information or documents requested are subject to privilege and therefore cannot be provided. <p>Legal advice may be required in making this assessment.</p>
	<p>H. REPORTING OF SUSPICIOUS TRANSACTIONS</p>
S.42 (6)	<p>212. A designated person who is required to report under this section shall disclose the following information in the report:</p> <ol style="list-style-type: none"> a) The information on which the designated person's knowledge, suspicion or reasonable grounds are based; b) The identity, if the designated person knows it, of the person who the designated person knows, suspects or has reasonable grounds to suspect has been or is engaged in an offence of money laundering or terrorist financing; c) The whereabouts, if the designated person knows them, of the property the subject of the money laundering, or the funds the subject

<p>S.42 (7)</p>	<p>of the terrorist financing, as the case may be; and</p> <p>d) Any other relevant information.</p> <p>213. A designated person shall not proceed with any suspicious transaction or service connected with, or the subject of, a report, prior to the sending of the report to the FIU and the Revenue Commissioners unless—</p> <p>a) It is not practicable to delay or stop the transaction or service from proceeding, or</p> <p>b) The designated person is of the reasonable opinion that failure to proceed with the transaction or service may result in the other person suspecting that a report may be (or may have been) made or that an investigation may be commenced or in the course of being conducted (see section I below).</p> <p>Due to the nature of retail financial services, suspicious transactions are often identified post-occurrence by means of account/transaction monitoring. In such scenarios, the suspicious transaction should be reported as soon as practicable after its identification.</p>
<p>S.42 (8)</p> <p>S.44 (2)</p>	<p>214. Nothing authorises a designated person to proceed with a service or transaction if the designated person has been directed by the Garda Síochána or ordered by the District Court not to proceed with that service or transaction and the direction or order is in force. Therefore, after the STR has been made to the FIU and Revenue Commissioners, the designated person can proceed with the transaction or service if it has not been subject to a direction or other guidance by the Garda Síochána.</p>
<p>S.46</p>	<p>215. In certain cases, disclosures are not required by law (See section VII E):</p> <ul style="list-style-type: none"> - Nothing requires the disclosure of information that is subject to legal privilege. - Nothing requires a relevant professional adviser to disclose information that he or she has received from, or obtained, in relation to a client in the course of ascertaining the legal position of the client.
<p>S.47</p>	<p>216. The disclosure of information by a person in accordance with these requirements shall not be treated, for any purpose, as a breach of any restriction imposed by any other enactment or rule of law e.g. data protection legislation.</p>
<p>I. TIPPING OFF</p>	
<p>Art 28</p> <p>S.49</p>	<p>217. Section 49(1) of the Act provides that 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 of the Act, 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. Moreover, section 49(2) of the Act provides that a</p>

	<p>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. Staff of a designated person asking the customer questions in the normal course of business, including requests for CDD information is not likely to prejudice an investigation.</p>
s. 22	218. In proceedings under section 17 or 19 suspicious transaction reports are not disclosed other than to the judge.
s. 50	219. A designated person has a number of defences regarding the offence of tipping off. A designated person should seek legal advice if they are unsure of any issue.
	220. It is a defence in any proceedings against a person for a tipping off offence, in relation to a disclosure, for the defendant to prove that – <ul style="list-style-type: none"> a) The disclosure was to a person who, at the time of the disclosure was a customer of the defendant or of a designated person on whose behalf the defendant made the disclosure, b) The defendant, or designated person on whose behalf the defendant made the disclosure, was directed or ordered not to carry out any specified service or transaction in respect of the customer, and c) The disclosure was solely to the effect that the defendant, or a designated person on whose behalf the defendant made the disclosure, had been directed by a member of the Gardai Síochána or ordered by a judge of the District Court, not to carry out the service or transaction for the period specified in the direction or order.
s. 51(1)	221. It is a defence in any proceedings against an individual in relation to a disclosure, for the individual to prove that, at the time of the disclosure— <ul style="list-style-type: none"> a) He or she was an agent, employee, partner, director or other officer of, or was engaged under a contract for services by, an undertaking; and b) He or she made the disclosure to an agent, employee, partner, director or other officer of, or a person engaged under a contract for services by, the same undertaking.
s. 51(2)	222. It is a defence in any proceedings against a person in relation to a disclosure, for the person to prove that, at the time of the disclosure— <ul style="list-style-type: none"> (a) The person was a credit institution or financial institution, or made the

	<p>disclosure on behalf of a credit institution or financial institution;</p> <p>(b) The disclosure was to a credit institution or a financial institution,</p> <p>(c) The institution to which the disclosure was made was situated in a Member State or a place designated under section 31 of the Act; and</p> <p>(d) Both the institution making the disclosure, or on whose behalf the disclosure was made, and the institution to which it was made belonged to the same group.</p> <p>223. It is a defence in any proceedings against a person in relation to a disclosure, for the person to prove that, at the time of the disclosure—</p> <p>(a) The person was a legal adviser or relevant professional adviser,</p> <p>(b) Both the person making the disclosure and the person to whom it was made carried on business in a Member State or in a place designated under section 31 of the Act; and</p> <p>(c) Those persons performed their professional activities within different undertakings that shared common ownership, management or control.</p> <p>S.52 224. (1) In relation to a disclosure—</p> <p>(a) By or on behalf of a credit institution to another credit institution;</p> <p>(b) By or on behalf of a financial institution to another financial institution;</p> <p>(c) By or on behalf of a legal adviser to another legal adviser; or</p> <p>(d) By or on behalf of a relevant professional adviser of a particular kind to another relevant professional adviser of the same kind.</p> <p>S.53(1) (2) It is a defence in any proceedings against a person in relation to a disclosure by or on behalf of the categories above, for the person to prove that, at the time of the disclosure –</p> <p>(a) The disclosure related to -</p> <p>(i) A customer or former customer of the person (or an institution or adviser on whose behalf the person made the disclosure) and the institution or adviser to which or whom it was made, or</p> <p>(ii) A transaction, or the provision of a service, involving both the person (or an institution or adviser on whose behalf the person made the disclosure) and the institution or adviser to which or whom it was made,</p> <p>(b) The disclosure was only for the purpose of preventing money laundering or terrorist financing,</p> <p>(c) The institution or adviser to which or whom the disclosure was made was situated in a Member State or in a place designated under the Act, and</p> <p>(d) The institution or adviser making the disclosure, or on whose behalf the disclosure was made, and the institution or adviser to which or whom it was made were subject to equivalent duties of professional confidentiality and the protection of personal data (within the meaning of the Data Protection Acts 1988 and 2003).</p> <p>225. It is a defence in any proceedings against a person for an offence in relation to a disclosure, for the person to prove that—</p> <p>(a) The disclosure was to the authority that, at the time of the disclosure, was the</p>
--	--

	<p>competent authority responsible for monitoring that person, or for monitoring the person on whose behalf the disclosure was made;</p> <p>(b) The disclosure was for the purpose of the detection, investigation or prosecution of an offence (whether or not in the State); or</p> <p>(c) The person did not know or suspect, at the time of the disclosure, that the disclosure was likely to have the effect of prejudicing an investigation into whether an offence of money laundering or terrorist financing had been committed.</p> <p>226. It is a defence in any proceedings against a person for an offence in relation to a disclosure, for the person to prove that—</p> <p>(a) At the time of the disclosure, the person was a legal adviser or relevant professional adviser;</p> <p>(b) The disclosure was to the person’s client and solely to the effect that the person would no longer provide the particular service concerned to the client;</p> <p>(c) The person no longer provided the particular service after so informing the client; and</p> <p>(d) The person made any report required in relation to the client in accordance with the legislation.</p>
	<p>J. DIRECTIONS AND ORDERS</p>
<p>S.17</p>	<p>227. A member of the Garda Síochána not below the rank of Superintendent may, by notice in writing, direct a person not to carry out a specified service or transaction during the period specified in the direction, not exceeding 7 days. If the member is satisfied that, on the basis of the information that the Garda Síochána has obtained or received, such a direction is reasonably necessary to enable the Garda Síochána to carry out preliminary investigations into whether or not there are reasonable grounds to suspect that the service or transaction would, if it were to proceed, comprise or assist in money laundering or terrorist financing.</p> <p>228. The duration of the direction, which should not exceed 7 days, is presumed to be limited to calendar days and automatically expires at the end of the specified duration.</p> <p>229. A judge of the District Court may order a person not to carry out any specified service or transaction during the period specified in the order, not exceeding 28 days, if satisfied by information on oath of a member of the Garda Síochána, that (a) there are reasonable grounds to suspect that the service or transaction would, if it were to proceed, comprise or assist in money laundering or terrorist financing, and (b) an investigation of a person for that money laundering or terrorist financing is taking place.</p> <p>230. The whole account of the customer is likely to be subject to a direction/order even where the investigation centres on a specific transaction or deal.</p>

<p>S.18</p>	<p>231. As soon as practicable after a direction is given or order is made, the member of the Garda Síochána who gave the direction or applied for the order shall ensure that any person who the member is aware is affected by the direction or order is given notice, in writing, of the direction or order unless,</p> <ul style="list-style-type: none"> - It is not reasonably practicable to ascertain the whereabouts of the person; or - There are reasonable grounds for believing that disclosure to the person would prejudice the investigation in respect of which the direction or order is given. <p>The notice shall include the reasons for the direction or order and advise the person to whom the notice is given of the person’s right to make an application for the revocation of the direction or order or arrange an order in relation to the property subject of the direction or order, e.g. for living expenses.</p>
<p>S.19</p>	<p>232. At any time, a judge of the District Court may revoke the direction or order on application of a person affected by the direction. Such an application may be made only if notice has been given to the Garda Síochána in accordance with any applicable rules of the court.</p>
<p>S.20</p>	<p>233. A District Court may, on application by any person affected by the direction or order concerned, make any order in relation to the property concerned for the purposes of enabling the person access to his/her property for:</p> <ul style="list-style-type: none"> - Reasonable living and other necessary expenses; and - To carry on a business, trade, profession or other occupations to which any of the property relates. <p>Such an application may be made only if notice has been given to the Garda Síochána in accordance with any applicable rules of the court.</p>
<p>S.14 [Criminal Assets Bureau Act 1996]</p> <p>S.78</p>	<p>234. Under section 14 (a) of the Criminal Assets Bureau Act 1996, as amended , or under section 105 of the Criminal Justice Mutual Assistance Act 2008, a member of the Garda Síochána can apply to the District Court for materials to be made available. However, it must be shown that there are reasonable grounds for suspicion in order for the court order to be granted. There must be reasonable grounds for suspecting that the material to which the application relates is likely to be of substantial value to the investigation. The MLRO (or other relevant party) is served with the order and must produce the material requested within a timescale of 7 days, unless the District judge decides otherwise.</p> <p>In certain circumstances, a judge of the District Court may grant a warrant to authorised officers of the Central Bank to enter a premises in order to obtain access to materials. It is recommended that anyone required to hand over materials under this section should keep a copy of the materials that are supplied to the authorities.</p>

s.22	235. A suspicious transaction report shall not be disclosed, in the course of proceedings under section 17 or 19, to any person other than the judge of the District Court concerned.
s.23	236. A member of the Garda Síochána, not below the rank of superintendent may, by notice in writing, authorise a person to proceed with an act that would otherwise comprise of money laundering, if the member is satisfied that the act is necessary for the purposes of an investigation into an offence.
	237. Any act or omission by a person in compliance with a direction or order under the Act shall not be treated, for any purpose, as a breach of any requirement or restriction imposed by any other enactment or rule of law.
SECTION VIII: RECORDKEEPING	
A. INTRODUCTION	
	238. Recordkeeping is an essential component of the evidentiary trail that must be established in order to assist in any investigation with a view to the detection and confiscation of criminal funds by the authorities. Designated persons must retain records concerning customer identification and transactions as evidence of the work they have undertaken in complying with their legal and regulatory obligations, as well as for use as evidence in any investigation conducted by relevant authorities. In addition, designated persons should retain such other records as they deem necessary to show their compliance with the provisions of the Act in relation to internal systems, compliance management and training.
	<p>239. Section 55 of the Act provides that a designated person –</p> <ol style="list-style-type: none"> 1. shall keep records evidencing the procedures applied, and information obtained, by the designated person. 2. shall take the original or a copy of all documents used by the designated person for the purposes of CDD. 3. shall keep records evidencing the history of services and transactions carried out in relation to each customer. <p>The document and other records referred to in subsections (1) to (3) shall be retained by the designated person, at an office or other premises in the State, for a period of not less than 5 years, as appropriate, after-</p> <ol style="list-style-type: none"> (a) the date on which the designated person ceases to provide any service to the customer concerned or the date of the last transaction (if any) with the customer, whichever is the later, (b) the date on which the correspondent banking relationship concerned ends, (c) the date on which the particular transaction is completed or discontinued, (d) the date on which a series of transactions is completed or discontinued, or (e) the date on which the particular service is completed or discontinued.
	240. The requirements imposed by this section are in addition to, and not in substitution for, any other requirements imposed by any other enactment or rule of law with respect of the retention of records by a designated person.

--	--

	B. WHAT RECORDS SHOULD BE MAINTAINED
<p>Art 30 S.55</p>	<p>241. Designated persons are obliged to keep the following documents and information for use in any investigation into, or analysis of, possible money laundering or terrorist financing by the FIU or Revenue Commissioners, or by other competent authorities in accordance with national law:</p> <p>Statutory;</p> <ul style="list-style-type: none"> - In the case of the CDD procedures applied, an original or an original copy of the documents used to verify identity of the customer which is required to be retained for a period of not less than 5 years (section 55(2)); - In the case of business transactions or services, the supporting evidence and records, consisting of the original documents or copies admissible in court proceedings under the applicable national legislation for a period of not less than 5 years (section 55(3)); - Documents or information used to verify identity of beneficial ownership (<i>section 33(2)(b)</i>); - Information on purpose and intended nature of a business relationship with a customer <i>section (35(1))</i>; - Records of ongoing monitoring (<i>section 35(3)</i>); - Documents or information on PEPs (<i>section 37</i>); - Documents or information on correspondent banking relationships (<i>section 38</i> and <i>section 55(1)(b)</i>); - Documentation in relation to reliance on third parties (<i>section 40</i>); - Records of decisions made on risk policy and the risk based approach applied (<i>section 54(2)</i>); - Records of decisions made on veracity or adequacy of previously obtained documents (<i>section 33(1) (d)</i>); <p>Other records;</p> <ul style="list-style-type: none"> - Evidence of training and compliance monitoring; - Annual (and other) reports on the designated persons AML/CTF systems and controls; - Records of decisions on filing/ not filing STRs. - Records of complete information on the payer which accompanies the transfer of funds as required by Regulation (EC) No. 1781/2006 if required.
<p>Art 32 S.56</p>	<p>242. Designated persons are also obliged to have processes in place to respond to enquiries from the Garda Síochána or Revenue Commissioners or other authorities as to whether they maintain or maintained a business relationship during the previous 6 years with a specified individual or company. They must also be able to provide details on the nature of that relationship. In responding to any enquiries from the Garda Síochána or Revenue Commissioners designated persons should also adhere to the criteria in sections 211 and 212 of these guidelines.</p>

<p>S57 (1)</p>	<p>243. A designated person is ultimately responsible for their recordkeeping irrespective of whether the records are kept by an agent, third party, branch or subsidiary. When a designated person has an agent, it should ensure that the agent complies with the record keeping obligations under the Act. This principle would also apply where the record keeping is delegated in any way to a third party, see Section V Reliance on third parties to undertake due diligence.</p> <p>A credit institution or financial institution that is a designated person and incorporated in the State shall ensure that any branch of the institution, or any subsidiary of the institution that is also a credit institution or financial institution, in a place other than a Member State, applies requirements equivalent to those specified in Chapters II (Customer Due Diligence) and Chapters IV (Record Keeping) of the Third Money Laundering Directive.</p>
<p>S.55 (2)</p>	<p>Customer information</p> <hr/> <p>244. A designated person shall take the original or a copy of all documents used by them for the purposes of CDD, including all documents used to verify the identity of customers or beneficial owners. A designated person shall keep records evidencing the history of services and transactions carried out in relation to each customer of the designated person.</p> <p>245. Certain sectors of the population or individuals may not be in a position to provide designated persons with the types of documentation considered as standard in order to fulfil its CDD obligations. When a designated person has concluded that it should treat a customer in accordance with requirements in relation to those without standard documentation, it should keep a record of the reasons for doing so. Appendix 2 of these guidance notes details alternative verification documents to facilitate financial inclusion.</p>
	<p>246. The designated person’s procedures must ensure that when a customer presents to the designated person face to face, or at one of its branches, the customer should produce the necessary identity proof(s), for the designated person to take and retain copies. However in circumstances (such as where verification is carried out at a customer’s home and photocopying facilities are not available) where it would not be possible to take a copy of the identity proof, a record should be made of the type of document, e.g. its reference number, date and place of issue, so that, if necessary, the document may be re-obtained from its source of issue. In such circumstances, the designated person must have had sight of the original document. Designated persons should ensure that personal data is only used for the purpose for which it was obtained as stated in the Data Protection Acts and is not used for other purposes without prior consent. – See Para 19”</p>

S.55 (3)	<p>Transactions</p> <hr/> <p>247. All transactions carried out on behalf of, or with a customer, in the course of relevant business, must be recorded within the designated person's records. A designated person shall keep records evidencing the history of services and transactions carried out in relation to each customer. The documents and other records shall be retained by the designated person, at an office or other premises in the State, for a period of not less than 5 years. Physical evidence of transactions may be of benefit to support a suspicious transaction.</p>
	<p>Internal and external reports</p> <hr/> <p>248. It is recommended that designated persons retain records of actions taken under internal and external reporting requirements as follows: When information or other material concerning possible money laundering has been considered by the MLRO, but a report has not been made to the FIU or Revenue Commissioners, a record of the other material that was considered should be retained; In addition, copies of any reports made to the FIU and Revenue Commissioners should be retained for 5 years from when the report was made; and Records of all internal and external reports should be retained for 5 years from when the report was made or the decision was made, by the MLRO not to make a report to the authorities.</p>
	<p>Other records</p> <hr/> <p>249. The obligations that are imposed on a designated person continue to apply to a person who has been a designated person, but has ceased to carry on business as a designated person.</p> <p>250. A designated person's records should include, details of its training programme (see Section IX Training) including for example;</p> <ul style="list-style-type: none"> - Dates AML training was given; - The nature of the training; - The names of the staff who received training; and - The results of the tests undertaken by staff, where appropriate. <p>251. In relation to documents or information on PEPs (see Section IV Customer Due Diligence) the following should be maintained;</p> <ul style="list-style-type: none"> - A record of written procedures detailing the designated person's policy and systems on how they identify PEPs. - All reports to senior management detailing PEPs and actions taken regarding PEPs. <p>252. In relation to documents or information on risk policy and risk based</p>

	<p>approach (see Section III The Risk Based Approach) the following should be maintained;</p> <ul style="list-style-type: none"> - A record of the steps taken to identify and analyse the risks to which the designated person is exposed in relation to money laundering and terrorist financing. - A record of the implementation procedures of the methods used for the risk based approach. - Records of how the risk based policy and approach are monitored and reviewed. <p>253. In relation to compliance monitoring, the following should be maintained;</p> <ul style="list-style-type: none"> - Reports to senior management; and - Records of any action taken as a consequence
	C. POSSIBLE FORMATS IN WHICH RECORDS MAY BE KEPT
S55(7)	254. A designated person may keep such records wholly or partially in an electronic, mechanical or other non-written form only if they are capable of being reproduced in a written form.
	D. LOCATION
S.55(4)	255. The documents and other records evidencing the procedures applied and information obtained, shall be retained by the designated person, at an office or other premises in the State, for a period of not less than 5 years.
	SECTION IX: TRAINING
	A. INTRODUCTION
	256. The detection and prevention of money laundering and terrorist financing is unlikely to be successful without the cooperation of well trained staff. It is essential that staff are aware of and alert to the risks of money laundering and terrorist financing and well trained in the various components of the designated person’s systems and controls. To facilitate this, designated persons must implement adequate staff awareness and training programmes. AML training should include reference to the Data Protection requirements and how they are relevant to the AML requirements.
Art 35 (1) S.54 (6-10)	B. WHAT DOES THE ACT REQUIRE?
	257. Designated persons are required by the Act to ensure that persons involved in the conduct of a designated person’s business are aware of the law relating to money laundering and terrorist financing. The Act also requires that such persons partake in programmes to help them identify transactions or other activity that may be related to money laundering and terrorist financing and to instruct them on the actions to take in such circumstances. If the employer has failed to provide the training, this is an offence on the part of the employer which carries a penalty of imprisonment for up to five years and/or an unlimited fine.

C. WHAT SHOULD DESIGNATED PERSONS DO?

Education and training programmes

258. There is no universal solution when determining how to deliver training, a mix of training methods may be appropriate. For example, the training may be delivered by way of online learning systems or through focussed classroom training. The timing and content of training will need to be adapted by individual designated persons for their own needs and according to the specific roles of individual members of staff.

Regardless of the approach taken towards training, it is important that designated persons retain records to monitor;

- i) who has been trained;
- ii) when they received the training;
- iii) the nature of the training given; and
- iv) the outcome of the training e.g. results of any tests undertaken by staff, where appropriate.

259. In respect of certain categories of staff, the following is recommended:

New Staff

A general appreciation of the background to money laundering and terrorist financing, and the subsequent need for reporting of any suspicious activities to the MLRO should be provided to relevant new staff. They should be made aware of the importance placed by the management of the designated person on the reporting of suspicions, that there is a legal requirement to report, and that there is a personal statutory obligation in this respect.

Customer-Facing Staff

Those dealing directly with customers are the first point of contact with potential money launderers and terrorist financiers and their efforts are therefore vital in the fight against money laundering and terrorist financing. They should be made aware of their legal responsibilities and the organisation's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious. This training will also include CDD procedures in addition to procedures for customers who cannot provide standard documentation. Training should also include the following:

- The designated person's policies and procedures on assessment and management of money laundering and terrorist financing risks;
- Staff are made aware of the range of acceptable documentation and information (from reliable and independent sources) that can be used to identify the customer and verify their identity;

- Staff should not unduly deny access to the financial system by only accepting limited types of ID documentation [i.e. that they would be breaching the rule outlined in Chapter 2.7 of the Consumer Protection Code; *A regulated entity must take into consideration the provisions of the relevant anti-money laundering guidelines....., and in particular any guidance in such notes on how to establish identity, in order to ensure that a person is not denied access to financial services solely on the grounds that that person does not possess certain specified identification documentation*]; Designated persons should also consider any similar principle contained in any amendment of the Consumer Protection Code.
- That if in doubt about whether a document is acceptable (on its own or taken together with a number of other documents), staff should speak to their manager or contact the MLRO who will be familiar with this aspect of the Act;
- “Front-line” staff should be made aware of the organisation’s policy for dealing with occasional customers, particularly where large cash transactions are involved, and the need for extra vigilance in these cases; and
- Details of the designated person’s systems for ongoing monitoring of customer business relationships and the role the individual plays in the functioning of that system.

Money Laundering Reporting Officers

Training concerning the Act and internal policies and procedures is required for MLRO’s (see Section VI: B). In addition, the MLRO will require on-going instruction on the validation and reporting of suspicious transactions to the FIU and the Revenue Commissioners and on the feedback arrangements and new trends and patterns of criminal activity. The FIU and Revenue Commissioners may, but are not required to provide such feedback and the MLRO should ensure that this service is availed of where provided. It is also possible that much knowledge may be obtained through reading of relevant publications by standard setters in the area of AML/CTF and from other reliable sources e.g. FATF, World Bank, the International Monetary Fund, Transparency International, United Nations Office on Drugs and Crime etc. Additional materials available on the internet and less formal discussions within networks will add to the MLRO’s knowledge.

260. Personal legal responsibilities of Staff

All relevant staff should be made aware of their personal responsibilities under the Act and the possible sanctions should they fail to comply with their obligations. Staff should also know at all times how, when and where/to whom a suspicious transaction report should be made.

	<p>261. Refresher Training/Ongoing Training</p> <p>It will also be necessary to make arrangements for refresher training to ensure that relevant staff are kept aware of their responsibilities and are provided with updates on any changes. It is recommended that refresher training should take place at least on an annual basis. However, individual designated persons may decide to adopt a more flexible approach to such training depending on the size or nature of their business.</p>
	<p>D. ADDITIONAL ISSUES FOR CONSIDERATION BY STAFF</p>
	<p>262. Sufficient training will need to be given to all relevant staff to enable them to recognise when a transaction is unusual or suspicious, or when they should have reasonable grounds to know or suspect that money laundering or terrorist financing is taking place. The set of circumstances giving rise to an unusual transaction or arrangement, and which may provide reasonable grounds for concluding that it is suspicious, will depend on the customer and the product or service in question. Examples of the type of situation that may be unusual, and which in certain circumstances might give rise to reasonable grounds for suspicion in accordance with a designated person's risk based approach include:</p> <ul style="list-style-type: none"> - Unusual patterns of transactions that have no apparent economic or visible lawful purpose; - The use of non-resident accounts, companies or structures in circumstances where the customer's circumstances do not indicate any reasonable need for their use; and - Where the activities being undertaken by the customer, or the size or pattern of transactions, is, without reasonable explanation, out of the ordinary range of services normally requested or is inconsistent with the experience of the designated person in relation to the particular customer.
	<p>263. Issues around the CDD process that may raise concerns include such matters as the following:</p> <ul style="list-style-type: none"> - Has the customer refused, or appeared reluctant, to provide the information requested without reasonable explanation? - Do you understand the legal and corporate structure of the customer entity, and its ownership and control, and does the structure appear to make sense? - Is the designated person aware of any inconsistencies between locations linked to the customer arising in the course of the business relationship and other information provided? - Is the area of residence given consistent with other profile details, such as employment? - Does an address appear vague or unusual – e.g., an accommodation agency, a professional 'registered office' or a trading address? - Does it make sense for the customer to be opening the account or

	<p>relationship in the jurisdiction that he is asking for?</p> <ul style="list-style-type: none"> - Does the supporting documentation add validity to the other information provided by the customer? - Does the customer want to conclude arrangements unusually urgently, against a promise to provide information at a later stage, which is not satisfactorily explained? - Has the customer suggested changes to a proposed arrangement in order to avoid providing certain information?
	<p>264. Staff awareness and training programmes should also address the issue of terrorist financing in order that staff may be conscious of customer transactions or activities that might be terrorist-related. Examples of activity that might suggest to staff (where such information is available) that there could be potential terrorist related activity include;</p> <ul style="list-style-type: none"> - Use of wire transfers and internet banking facilities to move funds to and from high-risk jurisdictions. - Media and official reports on suspected/arrested terrorists or groups. - Frequent and unexplained address changes. - Incompatibility of transactions with known sources of income.
	<p>265. It is important that staff are appropriately made aware of changing behaviour and practices amongst money launderers and those financing terrorism. A range of useful publications are available from public sources which will generally reflect the latest research into such behaviours and practices together with guidance on how best to detect and prevent its occurrence. Amongst the array of material freely available on the internet, the FATF website is relevant for all Designated Persons. Other bodies which may have relevant information include:</p> <ul style="list-style-type: none"> - World Bank (www.worldbank.org) - International Monetary Fund (www.imf.org) - United Nations Office on Drugs and Crime (www.unodc.org) - Bank for International Settlements (www.bis.org) - European Union (www.europa.eu) - Council of Europe (www.coe.int) - Transparency International (www.transparency.ie) - Egmont Group of Financial Intelligence Units (www.egmontgroup.org) - Wolfsberg Group of Banks (www.wolfsberg-principles.com)

SECTION X: ENFORCEMENT

266. Readers should note that Section X does not list every offence under the Act; readers should refer to the Act for a full list of offences.

The Act contains a number of offence provisions of relevance to credit and financial institutions.

The offence provisions in part 2 of the Act prescribe the substantive activities of money laundering and terrorist financing and provide for personal liability for individuals in respect of an offence.

The offence provision in Part 3 of the Act prescribes non-compliance by a person with a direction or order issued under Section 17 of the Act and provides for personal liability for individuals in respect of an offence.

The offence provisions in part 4 of the Act prescribe failures by credit and financial institutions (and other designated persons) to take preventative measures to diminish the risk of their businesses being used to launder monies or finance terrorism and provides for the liability of the relevant credit institution or financial institution.

The table below provides a brief synopsis of the principal offence provisions in parts 2, 3 and 4. To understand the offence in its entirety this synopsis must be read in conjunction with the full detail of the requirements in the legislation.

Part 2 – Money Laundering Offences

Offence	Sanction
<p>Money Laundering – includes; engaging, in relation to the proceeds of criminal conduct, in acts such as:</p> <p>(i) concealing or disguising the true nature, source, location, disposition, movement or ownership of the property, or any rights relating to the property;</p> <p>(ii) converting, transferring, handling, acquiring, possessing or using the property;</p> <p>(iii) removing the property from, or bringing the property into, the State,</p>	<p>On summary conviction, a fine not exceeding €5000 or imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 14 years or to both.</p>

S.7

S.8, 9, 10	<p>where the person knows or believes (or is reckless as to whether or not) the property is the proceeds of criminal conduct.</p>							
	<p>Money laundering outside the State with links to the State; attempts outside the State to launder within the State; aiding, abetting, counselling or procuring, from outside the State, the commission of laundering within the State or any other form of money laundering, attempted money laundering or aiding, abetting, counselling or procuring in respect of money laundering covered under Sections 8,9 and 10 of the Act.</p>	<p>On summary conviction, a fine not exceeding €5000 or imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 14 years or to both.</p>						
S. 17	<table border="1"> <thead> <tr> <th colspan="2" data-bbox="415 882 1382 1003">Part 3 – Offence of non-compliance with Section 17 Direction or Order</th> </tr> <tr> <th data-bbox="415 1003 899 1037">Offence</th> <th data-bbox="906 1003 1382 1037">Sanction</th> </tr> </thead> <tbody> <tr> <td data-bbox="415 1037 899 1713"> <p>Failure to comply with;</p> <p>a) a direction issued by a member of the Garda Síochána not below the rank of Superintendent not to carry out any specified service or transaction for a specified period not exceeding 7 days, or,</p> <p>b) an order issued by a judge of the District Court not to carry out any specified service or transaction for a specified period not exceeding 28 days.</p> </td> <td data-bbox="906 1037 1382 1713"> <p>On summary conviction, a fine not exceeding €5000 or imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 5 years or to both.</p> </td> </tr> </tbody> </table>		Part 3 – Offence of non-compliance with Section 17 Direction or Order		Offence	Sanction	<p>Failure to comply with;</p> <p>a) a direction issued by a member of the Garda Síochána not below the rank of Superintendent not to carry out any specified service or transaction for a specified period not exceeding 7 days, or,</p> <p>b) an order issued by a judge of the District Court not to carry out any specified service or transaction for a specified period not exceeding 28 days.</p>	<p>On summary conviction, a fine not exceeding €5000 or imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 5 years or to both.</p>
Part 3 – Offence of non-compliance with Section 17 Direction or Order								
Offence	Sanction							
<p>Failure to comply with;</p> <p>a) a direction issued by a member of the Garda Síochána not below the rank of Superintendent not to carry out any specified service or transaction for a specified period not exceeding 7 days, or,</p> <p>b) an order issued by a judge of the District Court not to carry out any specified service or transaction for a specified period not exceeding 28 days.</p>	<p>On summary conviction, a fine not exceeding €5000 or imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 5 years or to both.</p>							

		Part 4 – Controls Failure Offences by Designated Persons	
		Offence	Sanction
S.33(9)		<p>Failure to identify and verify customers or beneficial owners connected with customers when and as required by the Act or failure to comply with the other requirements under S.33, except as provided for in Section 34 of the Act.</p>	<p>On summary conviction, a fine not exceeding €5000 or to imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 5 years or to both</p> <p>Breach of section 33 of the Act, except as provided for in Section 34 of the Act, may also be a prescribed contravention and form the basis for administrative sanction under Part IIIC of Central Bank Act 1942.</p>
S.35(4)		<p>Failure to obtain information on the purpose and intended nature of a business relationship with a customer prior to the establishment of the relationship or failure to comply with the other requirements in Section 35 of the Act, except as provided for under Section 36 of the Act.</p> <p>Failure to conduct ongoing monitoring of dealings with customers</p>	<p>On summary conviction, a fine not exceeding €5000 or to imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 5 years or to both</p> <p>Breach of section 35 of the Act, except as provided for in Section 36 of the Act, may also be a prescribed contravention and form the basis for administrative sanction under Part IIIC of Central Bank Act 1942.</p>
37(9)		<p>Failure to take steps to determine whether or not a customer, or a beneficial owner connected with a customer, is a PEP or failure to comply with the other requirements in Section 37 or the Act.</p> <p>Failure includes having reasonable grounds to believe a customer is a PEP and failing to seek senior management approval before establishing a business relationship or to determine the source of wealth and of funds for certain transactions involving PEPs.</p>	<p>On summary conviction, a fine not exceeding €5000 or to imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 5 years or to both.</p> <p>Breach of section 37 of the Act may also be a prescribed contravention and form the basis for administrative sanction under Part IIIC of Central Bank Act 1942.</p>

<p>38(2)</p>	<p>Failure to apply specified ECDD measures required by Section 38 of the Act prior to commencing a correspondent banking relationship with a respondent institution situated in a place other than a Member State or failure to comply with the other requirements in Section 38 of the Act.</p>	<p>On summary conviction, a fine not exceeding €5000 or to imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 5 years or to both.</p> <p>Breach of section 38 of the Act may also be a prescribed contravention and form the basis for administrative sanction under Part IIIC of Central Bank Act 1942.</p>
<p>s.42(9)</p>	<p>Failure to report to the Garda Síochána and the Revenue Commissioners a Designated Person's knowledge or suspicion (on reasonable grounds) that another person has been or is engaged in an offence of money laundering or terrorist financing or failure to comply with the other requirements in section 42 of the Act except as provided by Section 46 of the Act.</p>	<p>On summary conviction, a fine not exceeding €5000 or to imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 5 years or to both.</p> <p>Breach of section 42 of the Act, except as provided by Section 46 of the Act, may also be a prescribed contravention and form the basis for administrative sanction under Part IIIC of Central Bank Act 1942.</p>
<p>s.43(2)</p>	<p>Failure to report to the Garda Síochána and the Revenue Commissioners transactions connected with places designated by the Minister as having inadequate procedures for detection of money laundering or terrorist financing under section 32.</p>	<p>On summary conviction, a fine not exceeding €5000 or to imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 5 years or to both.</p>

<p>S.49(3)</p>	<p>When knowing or suspecting, 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, making any disclosure that is likely to prejudice an investigation that may be conducted following the making of a report under that Chapter.</p> <p>When knowing or suspecting, on the basis of information obtained 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, making any disclosure that is likely to prejudice such an investigation.</p>	<p>On summary conviction, a fine not exceeding €5000 or to imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 5 years or to both.</p> <p>Breach of section 49 of the Act may also be a prescribed contravention and form the basis for administrative sanction under Part IIIC of the Central Bank Act 1942.</p>
<p>S.54(8)</p>	<p>Failure to adopt policies and procedures, in relation to the designated person's business, to prevent and detect the commission of money laundering and terrorist financing or failing to comply with any other requirement of Section 54 of the Act, such as providing training and legal instruction.</p> <p>The policies and procedures should include policies and procedures dealing (inter alia) with the identification and scrutiny of complex or large transactions, unusual patterns or transactions that have no apparent economic or visible lawful purpose and any other activity likely, by its nature, to be related to money laundering or terrorist financing. The policies and procedures should also set out measures to be taken to prevent the use, for money laundering or terrorist financing, of transactions or products that could favour or facilitate anonymity.</p>	<p>On summary conviction, a fine not exceeding €5000 or to imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 5 years or to both.</p> <p>Breach of section 54 of the Act may also be a prescribed contravention and form the basis for administrative sanction under Part IIIC of Central Bank Act 1942.</p>

<p>S.55(12)</p>	<p>Failure to keep records evidencing the procedures applied, and information obtained, by a designated person to verify the identity of customers or beneficial owners in accordance with section 33 and to evidence the history of services and transactions carried out in relation to customers or failure to comply with any other requirements of Section 55 of the Act.</p>	<p>On summary conviction, a fine not exceeding €5000 or to imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 5 years or to both.</p> <p>Breach of section 55 of the Act may also be a prescribed contravention and form the basis for administrative sanction under Part IIIC of Central Bank Act 1942.</p>
<p>S.56(2)</p>	<p>Failure by credit or financial institutions to establish systems to retrieve information relating to business relationships and to respond fully and promptly to enquiries from the Garda Síochána in that regard or failure to comply with other requirements in Section 56 of the Act.</p>	<p>On summary conviction, a fine not exceeding €5000 or to imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 5 years or to both.</p> <p>Breach of section 56 of the Act may also be a prescribed contravention and form the basis for administrative sanction under Part IIIC of Central Bank Act 1942.</p>

<p>S.57(4)</p>	<p>Failure by credit institution or financial institution to apply certain requirements to branches and subsidiaries in non- Member States or failure to comply the other requirements under S.57 of the Act.</p> <p>Failure by a credit institution or financial institution to inform the competent authority when places concerned do not permit application of requirements equivalent to those specified in the Third Money Laundering Directive, in order to apply measures, determined in consultation with the competent authority, to deal with the risk of money laundering or terrorist financing arising from the absence of those requirements or failing to comply to any other requirements under S.57 of the Act.</p> <p>Failure by a credit institution or financial institution to communicate policies and procedures adopted under section 54 to branches or subsidiaries in places other than a Member State – or failing to comply to any other requirements under S.57 of the Act.</p>	<p>On summary conviction, a fine not exceeding €5000 or to imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 5 years or to both.</p> <p>Breach of section 57 of the Act section may also be a prescribed contravention and form the basis for administrative sanction under Part IIIC of Central Bank Act 1942.</p>
<p>S.58(3)</p>	<p>Credit or financial institutions setting up, providing to customers or maintaining in existence anonymous accounts.</p>	<p>On summary conviction, a fine not exceeding €5000 or to imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 5 years or to both.</p> <p>Breach of section 58 of the Act may also be a prescribed contravention and form the basis for administrative sanction under Part IIIC of Central Bank Act 1942.</p>

<p>S.59(5)</p>	<p>Credit or financial institutions entering into or maintaining correspondent banking relationships with shell banks</p> <p>Failure to adopt measures to ensure that such relationships are not entered into or maintained or failure to comply with the other requirements under S.59 of the Act.</p>	<p>On summary conviction, a fine not exceeding €5000 or to imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 5 years or to both.</p> <p>Breach of section 59 of the Act may also be a prescribed contravention and form the basis for administrative sanction under Part IIIC of Central Bank Act 1942.</p>
<p>S.67(2)</p> <p>S.67(6)</p>	<p>Failure to comply with a direction (in writing) from the State competent authority to provide information or documents without reasonable cause.</p> <p>Failure, knowing the whereabouts of documents subject to a direction, to furnish to the relevant State competent authority a statement, verified by a statutory declaration, identifying the whereabouts of the documents without reasonable cause.</p> <p>Failure to comply with any other requirements under S.67 of the Act.</p>	<p>On summary conviction, a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both).</p>
<p>S.68(3)</p>	<p>Failure to comply with a direction (in writing) from the State competent authority to furnish an explanation of documents in the manner specified by the authority without reasonable cause.</p> <p>Failure to comply with any other requirement under S.68 of the Act.</p>	<p>On summary conviction, to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months (or both).</p> <p>Breach of section 68 of the Act may also be a prescribed contravention and form the basis for administrative sanction under Part IIIC of Central Bank Act 1942.</p>
<p>S.71(3)</p>	<p>Failure to comply with a direction (in writing) from the State competent authority to discontinue, or refrain</p>	<p>Will be treated as an aggravating factor in the event the designated person is subsequently found guilty</p>

	from engaging in, specified conduct that, in the opinion of the authority constitutes a breach of any specified provision of Part 4 of the Act.	of an offence.
S.80(3)	<p>Failing to comply with a requirement, or request made by an authorised officer.</p> <p>Or</p> <p>Obstructing or interfering with an authorised officer in the exercise of the officer’s powers under this Chapter 8 (<i>Monitoring of designated persons</i>) of the Act.</p> <p>Or</p> <p>Failure to meet any other requirement under S.80 of the Act.</p>	<p>On summary conviction, a fine not exceeding €5000 or to imprisonment for a term not exceeding 12 months or to both</p> <p>On conviction on indictment, a fine or to imprisonment for a term not exceeding 5 years or to both.</p> <p>Breach of section 80 of the Act may also be a prescribed contravention and form the basis for administrative sanction under Part IIIC of Central Bank Act 1942.</p>
S.13(8) 2005 Act	Criminal Justice (Terrorist Offences) Act, 2005 (“2005 Act”)	
	A person guilty of an offence under this section is liable—	<p>On summary conviction, to a fine not exceeding €3,000 or imprisonment for a term not exceeding 12 months or both, or</p> <p>On conviction on indictment, to a fine or imprisonment for a term not exceeding 20 years or both.</p>
Authorised Officers and Enforcement		
S.72(1)	267. State Competent Authorities are empowered to appoint officers or other suitably qualified persons as Authorised Officers to monitor compliance by designated persons for whom they are the competent authority under the Act	
S. 75(1) S.77(1)	<p>268. Authorised officers are empowered to do all, or any of the following, for the purposes of carrying out an investigation:</p> <ul style="list-style-type: none"> - At all reasonable times, enter any premises at which there are reasonable grounds to believe that the business of a designated person is, or has been, carried on, or that relevant records are on the premises; 	

	<ul style="list-style-type: none"> - Search and inspect the premises referred to in subparagraph (a) and any relevant records on the premises; - Secure for later inspection the premises, or any part of the premises, in which relevant records are kept or in which the officer has reasonable grounds for believing the relevant records are kept; - Require any person who carries on the business of a designated person and any person employed in connection therewith to produce to the officer relevant records, and if the information is in a non-legible form, to reproduce it in a legible form or to give to the officer such information as the officer reasonably requires in relation to entries in the relevant records; - Inspect and take copies of relevant records inspected or produced under the Scheme (including, in the case of information in a non-legible form, a copy of all or part of the information in a permanent legible form); - Remove and retain any of the relevant records inspected or produced under the Scheme for such period as may be reasonable to facilitate further examination; - Require a person to give to the officer information (including information by way of a written report) that the officer reasonably requires in relation to activities covered by the Scheme and to produce to the officer any relevant records that the person has or has access to; - Require a person by whom or on whose behalf data equipment is or has been used, or any person who has charge of, or is otherwise concerned with the operation of, the data equipment or any associated apparatus or material, to give the officer all reasonable assistance in relation thereto; and - Require a person to explain entries in any relevant records.
<p>S.78(1)</p>	<p>269. Authorised officers may make an application to a judge of the District Court for a warrant to enter any premises from which it has been prevented from entering or where he has reasonable grounds for believing there are relevant records in a private dwelling and to be accompanied by a Garda if necessary.</p>
<p>S.114(4)</p>	<p>270. Failures to take the preventative measures required by Part 4, may simultaneously constitute a criminal offence under the 2010 Act and a “prescribed contravention” for the purpose of the Central Bank’s administrative sanctions procedure.</p> <p>271. By operation of law, the ‘credit institutions’ and ‘financial institutions’ i.e. ‘designated persons’ for the purpose of the 2010 Act, become ‘regulated financial service providers’ for the purposes of (administrative sanctions) Part IIIC of the Central Bank Act 1942 and thus become subject to a range of administrative sanctions, such as:</p>

	<ul style="list-style-type: none"> a. caution or reprimand; b. direction to refund or withhold all or part of an amount of money charged or paid. c. a direction to pay to the Central Bank a monetary penalty (not exceeding a prescribed amount of €5,000,000 for a corporate, or €500,000 for a natural person); d. if the financial service provider is a natural person, a direction disqualifying the person from being concerned in the management of a regulated financial service provider for such period as is specified in the order; e. if the financial service provider is found to be still committing the contravention, a direction ordering the financial service provider to cease committing the contravention; f. a direction to pay to the Central Bank all or a specified part of the costs incurred by that Authority in holding an inquiry and in investigating the matter to which an inquiry relates. <p>272. The administrative sanctions regime is also applicable to “persons concerned in management” of credit and financial institutions and so if the Central Bank makes a finding that “a person concerned in the management” of a credit or financial institution is participating or has participated in the commission by the financial service provider of one of the prescribed contraventions listed above and in part 4 of the Act, it may impose:</p> <ul style="list-style-type: none"> (a) a caution or reprimand; (b) a direction to pay to the Central Bank a monetary penalty not exceeding €500,000; (c) a direction disqualifying the person from being concerned in the management of a regulated financial service provider for such period as is specified in the order; (d) if the person is found by the Central Bank to be still participating in the commission of the contravention, a direction ordering the person to cease participating in the commission of the contravention; (e) a direction to pay to the Central Bank all or a specified part of the costs incurred by the Bank in holding an inquiry and in investigating the matter to which an inquiry relates. <p>The level of sanction imposed by the Central Bank will depend on a variety of factors, such as:</p> <ul style="list-style-type: none"> (a) The gravity of the contravention, e.g. whether it was deliberate, its
--	--

duration, whether it reveals serious or systemic weaknesses of the management systems or internal controls relating to all or part of the business, and so on.

(b) The conduct of the regulated financial service provider or person concerned in its management after the contravention, for example how quickly, effectively and completely the credit or financial institution, or person concerned in its management brought the contravention to the attention of the Central Bank or to the attention of any other relevant Central Bank; the degree of co-operation with the Central Bank or other agency provided during the examination of the contravention.

(c) The previous record of the credit or financial institution, or of the person concerned in its management, for example, whether the Central Bank has taken any previous action resulting in a settlement, sanctions or whether there are relevant previous criminal convictions; whether the credit or financial institution, or the person concerned in its management has previously been requested to take remedial action

Suspected prescribed contraventions may be dealt with by the Central Bank in a number of ways as illustrated below.

Any potential or pending criminal proceedings in respect of the contravention will be prejudiced or barred if a monetary penalty is imposed pursuant to the Administrative Sanction Procedure.

```

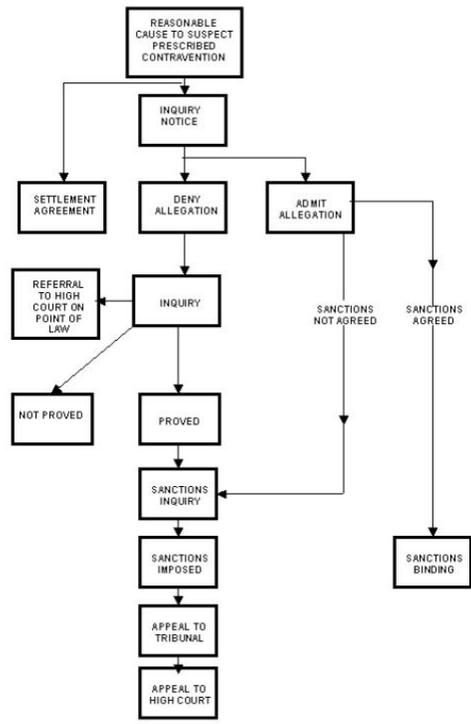
graph TD
    A[SUSPICION] --> B[EXAMINATION]
    B --> C[NO FURTHER ACTION]
    B --> D[SUPERVISORY ACTION]
    B --> E[ADMINISTRATIVE SANCTIONS INQUIRY]
    B --> F[ADMINISTRATIVE SANCTIONS SETTLEMENT AGREEMENT]
    B --> G[CRIMINAL PROSECUTIONS]
    B --> H[REFERRAL TO OTHER AUTHORITY OR ENFORCEMENT BODY]
  
```

Figure 1 - Enforcement options

The procedure can be graphically presented as follows:

ASP Guidelines
Rule 14(1)(j)

S. 33AT
CBA 1942



Detailed guidance on the operation of the Central Bank’s administrative sanctions procedure is available on the Central Bank’s website www.centralbank.ie under [Financial Regulation Homepage](#).

APPENDIX 1

GUIDANCE ON IDENTIFICATION AND VERIFICATION PROCEDURES

Scope:

This appendix provides guidance on identification and verification procedures but does not provide a basis for satisfying other CDD obligations such as obtaining information on the purpose and nature of the business relationship and the requirement to monitor ongoing relationships including the scrutiny of transactions, or where the customer is acting on his/her own behalf rather than on behalf of another beneficial owner. Therefore, Appendix 1 should be read in conjunction with Section IV on Customer Due Diligence. Designated persons should also ensure that personal data is only used for the purpose for which it was obtained as stated in the Data Protection Acts and is not used for other purposes without prior consent. – See Para 19”

Authenticity of Documentation

It is important for Designated Persons to have regard to the validity and authenticity of documentation or information received:

- Passports, national identity cards and driving licences must be current (i.e., unexpired) and valid.
- Letters or statements (of official origin or from financial institutions) should be of a recent date, i.e. no greater than 6 months, except in the case of an official document known to be issued only or typically at fixed intervals of more than 6 months, in which case such documents may be accepted during that period, to a maximum of 12 months e.g. car tax. The table below contains a list of documents which are considered to be generally acceptable. It is for each Designated Person to decide on a risk basis which of these types of documents it considers appropriate to its business, in the light of any other due diligence procedures it applies and other information available in relation to the customer at the commencement of the business relationship, having regard also to the principle of avoiding unduly excluding prospective customers from access to financial services.
- Designated persons should take reasonable care to check that documents offered are genuine and valid (showing no apparent evidence of forgery). For face-to-face customers, where documents incorporate photographs, Designated Persons should ensure that these bear a reasonable likeness to the presenter.
- In relation to copy documentation, the Designated Person should satisfy themselves as to the validity of any copy documentation received from or on behalf of non face-to-face customers where warranted by the risk. These additional risks may be mitigated by one or more of the following :
 - o Obtaining additional documentation to that obtained for face to face customers. These additional documents can be in electronic form;
 - o Verification of the customer’s identity on the basis of confirmation received from an acceptable institution e.g. their bank, credit union, An Post etc, that the customer is, or has been, a customer of that institution;
 - o Ensuring that the transaction is carried out through an account in the customer’s name with an acceptable institution that is a credit institution; or
 - o Certification of the documents received.

To the extent that copy documentation is certified, the following, and potentially their equivalents in other jurisdictions, are considered suitable persons to certify documentation, where they are willing to do so:

- Garda Siochana/ Police Officer

- Practising Chartered & Certified Public Accountants
- Notaries Public / Practising solicitors
- Embassy/Consular Staff
- Regulated financial or credit institutions
- Justice of the peace
- Commissioner for oaths
- Medical professional

Designated persons may determine that other persons with equivalent status to the persons in this list in the relevant jurisdiction might be suitable to certify documentation and should document their reasons for this determination.

Before accepting certification by such persons in jurisdictions other than Ireland, Designated Persons should have regard to any additional risks relating to the jurisdiction and satisfy themselves as to the validity and acceptability of the certification and the status and standing of the category of person in that jurisdiction. The level of verification of the certifier will depend on the risk of that jurisdiction and may not require application to the certifier of the full identification and verification requirements in this Appendix. The results of this risk analysis should be documented and retained. The contact details (to include name address and where applicable professional registration) of the certifier should be made available to the Designated Person accepting the document so that a follow up confirmation may be requested, if required. In general, certification of documents should include a statement to the effect that the original of the document was sighted. The document should also be signed and dated. Where available a stamp should be used by the certifier. In cases where there is doubt regarding the validity of documents or certification a designate person is required to investigate further prior to accepting such documents. A business relationship must not be entered into where the doubts regarding the validity of documents have not been clarified by the Designated Person.

Section 1. Individuals

In accordance with best practice, the standard approach of Designated Persons should be to obtain and verify the following information in order to uniquely identify individual customers:

- Name, Date of Birth and Current Address

Designated persons may exercise a degree of risk-based discretion³, where they are prepared to accept responsibility for their decision, made on reasonable grounds, that verification of (1) the name and (2) one of the other elements above (Date of Birth or Current Address) definitively confirms the identity of the customer. The basis for any such decisions should be documented and retained.

Where an account is a joint account, identification and verification must be obtained and undertaken in relation to all parties.

Documentary Verification

Where identification information is verified using documentary evidence, whether or not in electronic form, the verification should be based upon one or more of the documents listed below, having regard to the perceived risk of the customer. It is anticipated that many Designated Persons will opt to identify their customers by means of one piece of photographic evidence that includes name and date of birth and one piece of evidence of address. It is important to note that documents differ in their integrity, reliability and independence. Some are issued after due diligence on an individual's identity has been undertaken, others

³ particularly for customers or product lines regarded as lower risk (where not already qualifying for Simplified Customer Due Diligence)

are issued on request, without any such checks being carried out. In its risk analysis, a Designated Person should also have regard to the jurisdiction that issued the documentation on which it chooses to place reliance. A broad hierarchy of documents can be defined, as follows, commencing with documents with the highest probative value:

- Documents that include a photograph and that are issued by government departments and agencies, or by a court;
- Documents without a photograph that are issued by government departments and agencies, or by a court;
- Certain documents issued by other public sector bodies or local authorities;
- Certain documents issued by regulated Designated Persons in the financial services sector;
- Those issued by other credit or financial institutions subject to legislative obligations transposing the EU Third Directive or comparable legislation; and
- Corroborative documentation from other sources e.g. including internet printouts. However, such corroborative documents should be used with caution as, for example, internet printouts offered by a customer may be relatively easy to falsify.

The following table defines a set of standard documentation which may be used for the purposes of verifying identity. The list is not intended to be exhaustive and Designated Persons may apply a measure of risk based discretion in deciding on their own policy and procedures in relation to identity verification. Designated persons should not apply the verification measures in such a manner as to unduly exclude persons from access to the financial system and be so rigid in their implementation of the requirements so as to unreasonably restrict the choice of the customer in providing a valid means of verification of identity.

Standard Documentation

“One plus One” approach – one item from the list of photographic IDs (typically to verify name and date of birth) and one item from the list of non-photographic IDs (typically to verify address). Depending on the risk assessment of the customer additional ID verification may be required. This does not prevent the use of two documents under the heading “Photographic ID” for the identification of name, date of birth and address.

In using these lists, Designated Persons should also refer to the discussion above of the relative probative value and risks arising from each category. The Designated Person should have sight of original documentation whenever feasible. For non face to face customers please refer to the section above re additional measures which may be taken to mitigate the risk. A Designated Person should exercise particular caution before deciding to accept documentation printed from the internet.

The documentation which is requested by the designated person should be relevant and not excessive.

- The documentation outlined in this Appendix may contain sensitive personal data, and, as a result, designated persons data security measures should take account of this and such sensitive personal data should not be further processed for separate unrelated purposes. *“All documentation requested should be relevant to the CDD process and not excessive; otherwise data protection issues may arise.”*

Photographic ID:

- Current valid Passport
- Current valid driving licence;
- Current valid National Identity Card;

Non Photographic ID:

- Official documentation/cards issued by the Revenue Commissioners and addressed to the individual;
- Official documentation/cards issued by the Department of Social Protection and addressed to the individual;
- Instrument of a court appointment (such as liquidator, or grant of probate);
- Current local authority document e.g. refuse collection bill, water charge bill (including those printed from the internet);
- Current statement of account from a credit or financial institution, or credit/debit card statements (including those printed from the internet);
- Current utility bills; (including those printed from the internet);
- Current household/motor insurance certificate and renewal notice; and

In cases where a plausible explanation is offered by a customer as to why the above non photographic documentation cannot be provided, a Designated Person may choose the following to assist in confirming the identity of the customer, having regard to any data protection requirements:

- Examination of the electoral register (including online version)
- Examination of a local telephone directory or available street directory;
- Confirmation of identity by a known/recognisable employer;
- Search of a relevant agency that can confirm identity.

The above identification and verification procedures may usefully be supplemented (on a risk basis to be decided by the Designated Person) by media searches and use of internet search engines.

The above is not an exhaustive list. It is up to each institution to decide on a risk based approach whether they will accept other forms of customer ID. However, the documentation set out above should be considered the standard expected to be applied in most cases to meet the obligation in section 33 of the Act to confirm the identity of the customer. Where it is not feasible, on reasonable and documented grounds, to expect the customer to meet the documentation standards set out above, Designated Persons should consider whether it is appropriate to instead adopt the alternative approach to facilitate financial inclusion set out in Appendix 2, including for purposes of financial inclusion.

The basis for such decisions and level of cases should be monitored on an ongoing basis by the Designated Person to ensure that:

- the decisions to set aside the standard identification and verification procedures are warranted and reasonable in the circumstances; and, on the other hand,

- the Designated Person is not unduly restricting access to the financial system.

Verification using electronic information database services:

Where verification is to be undertaken using electronic verification, a Designated Person must ensure the requirements outlined above are met by carrying out electronic checks either directly, or through a supplier that provides a reasonable assurance that the customer is who he or she claims to be. Note, that given the higher risk of exposure to impersonation when using electronic verification, one or more of the checks should be undertaken to ensure the information obtained can uniquely identify individual customers.

It is the Data Protection Commissioner's view that where a designated person (data controller) enters into a contract with a third party (data processor) to undertake a search, this can be done in line with the Data Protection Acts without a requirement for consent because the information remains under the control of the data controller. It would not be acceptable for the designated person to pass data to the third party to conduct a search and for that third party to retain that information in relation to the customer for its own purposes.

Section 2. Identification and Verification where it relates to customers that are legal persons or arrangements:

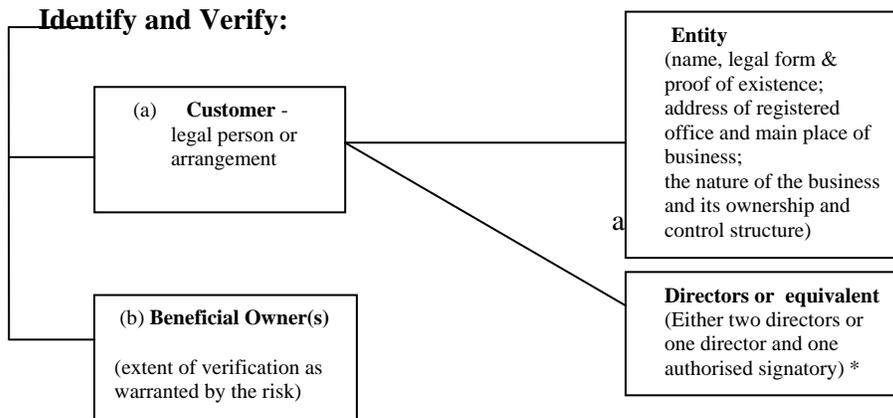
Under section 33 of the Act a Designated Person is required to identify;

- (a) the customer, and
- (b) any beneficial owner.

The extent to which a Designated Person should 'verify' the information obtained at (a) and (b) above is set out in the tables below. The tables should be adapted where necessary depending on the nature of the legal person or arrangement to ensure that the beneficial owner/controller has been identified and verified in all cases (the extent of verification required will depend on the risk). It is important that Designated Persons understand the nature of the business and the ownership and control structure of their customer, including links with the persons in the management that control the operations of the customer. The purpose of the requirements set out in (a) and (b) below regarding the identification and verification of the customer and the beneficial owner (the extent of verification of the identity of the beneficial owner is dependent on the risk) is to prevent the unlawful use of legal persons and arrangements, and to gain a sufficient understanding of the customer to be able to properly assess the potential money laundering and

terrorist financing risks associated with the business relationship and to take appropriate steps to mitigate the risks.

In the case of a legal person or arrangement, the process of identifying is set out in two parts and comprises details of the entity itself and its directors (or equivalent). This is separate to the requirements relating to identification and verification of beneficial ownership (the extent of verification required will depend on the risk). This section should be read in conjunction with section IV of these guidelines.



* In line with risk assessment, one or more signatories may need to be identified and verified.

Note in relation to (a) and (b) below: Where one document provides the verification of more than one category of principals (e.g. both directors and beneficial owners) there is no requirement to obtain separate verifications for each.

(a) Identify the customer and verify that customer’s identity using reliable, independent source documents, data or information.

Identify and verify	Who to identify:	How to identify:	How to verify:
Customer - legal person or arrangement	Legal person or arrangement	Obtain information from the customer or from reliable, independent source on: i) name, legal form and proof of existence; ii) the powers that bind and regulate the legal person or arrangement; iii) the address of the registered office (where applicable) and main place of	This could generally be satisfied by either ✓ A search of the relevant company or other registry (where the necessary information is publicly accessible and considered by the Designated Person to be current and reliable); or ✓ A copy, as appropriate to the nature of the entity, of the certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other official

		business; and iv) the nature of the business and its ownership and control structure.	documentation proving the name, form and current existence of the customer. ✓ In cases regarded by the Designated Person as higher risk, use of more than one source of information may be warranted.
	Directors (or the equivalent in for example; Partnerships and unincorporated businesses, Clubs, Societies, Public Sector bodies.)	Identify the directors of the legal person or trustees of a trust (or other equivalent persons for other forms of legal entity or arrangement). This information can be provided by the customer or obtained from a reliable, independent source.	This could generally be satisfied by either ✓ obtaining a copy of the annual audited accounts listing directors (where the necessary information is publicly accessible and considered by the Designated Person to be current and reliable); or ✓ relevant and up-to-date legal opinion from a reliable source documenting due diligence conducted, including in relation to information on directors; or ✓ obtaining information from relevant company or other registry such as the CRO or known foreign equivalent; or ✓ as warranted by the risk, verify one or more directors in line with requirements for personal customers
	Authorised signatory	Identify the signatories by reference to the duly-approved mandate provided by the customer in relation to the operation of the business relationship.	In accordance with normal business practice and as warranted by the risk of money laundering or terrorist financing, verify the personal identity of one or more of the signatories in line with the requirements for personal customers . Verification of

			authorised signatories may not be required where a sufficient number of directors have been verified in accordance with this appendix.
--	--	--	--

- (b) Identify the beneficial owner, and to the extent warranted by the risk, take reasonable measures to verify the identity of the beneficial owner such that the Designated Person is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include Designated Persons taking reasonable measures to understand the ownership and control structure of the customer. It is not possible to cover all scenarios across all jurisdictions and it is for a Designated Person to be satisfied that the decisions taken and information relied upon to verify the beneficial owner's identity was reasonable for the Designated Person to be satisfied that it verified the identity of the beneficial owner and that the extent of that verification is in accordance with the risk.

Identify and verify	How to identify:	How to verify:
Beneficial Owner	<p>Identify any beneficial owner connected with the customer or service concerned. This information can be provided by the customer (or on the customer's behalf by the customer's duly authorised representative) or obtained from a reliable, independent source. This should include Designated Persons taking reasonable measures to understand the ownership and control structure of the customer.</p> <p>This would comprise:</p> <p>i) Any natural person who owns or controls more than 25% of the shares or voting rights in the legal person or arrangement; or</p> <p>ii) Any natural person who exerts ultimate control over the legal person through its management or otherwise.</p> <p>If, exceptionally, due to the nature or structure of the legal person or arrangement, it is not feasible to identify any natural person who</p>	<p>Verify the identity of the natural persons who own or control more than 25% of the shares or voting rights or otherwise exercises control over the management of the legal person or arrangement. The extent of this verification is dependent on the relevant risks.</p> <ul style="list-style-type: none"> ➤ This would be satisfied by verifying identity in line with the requirements for individuals. ➤ This could also be satisfied by one or more of the following alternative approaches in line with the risk policy of the Designated Person. In high risk scenarios a designated person should use more than one source to verify information. ✓ obtaining a copy of the annual audited accounts listing shareholders, directors or other persons exercising control over the customer (where the information is considered by the Designated Person to be current and reliable), or

⁴ Examples might include a professional firm operating as a partnership with multiple partners.

	<p>meets either of the definitions at i) or ii) above, the Designated Person may treat as exercising control the directors (or equivalent) or other persons having the power to legally bind the customer.⁴</p> <p>The Designated Person must record the basis for their decision in reaching the conclusions it has in relation to the ownership/control of the customer.</p>	<ul style="list-style-type: none"> ✓ for complex structures, (particularly where a company is registered abroad) a relevant and up-to-date legal opinion⁵ from a source on which the Designated Person is prepared to rely, documenting due diligence conducted, including in relation to information on the shareholding/control structure and directors (or equivalent); or ✓ placing reliance on information provided/certified by counterparties/agents (e.g. in syndicated deals) where such persons are regulated credit or financial institutions or are legal or accountancy professionals subject to equivalent AML/CTF obligations; or ✓ having a notary public (or equivalent) certify the validity of the information provided by or on behalf of the customer; or ✓ placing reliance on information provided/certified by a Company Secretary (or equivalent) - e.g.: copies of constitutional documentation (e.g., Memo & Articles/Certificates of Incorporation / Trust Deed) and shareholder certification. ✓ In line with the Designated Person's risk assessment the process may include verifying a beneficial owner's personal identity (the extent of verification required will depend on the risk) in line with the requirements for personal customers. Such verification should be considered the norm for any customer regarded by the designated person as higher risk.
--	---	--

⁵ From a law firm in or with knowledge of the legal system of the jurisdiction of the product.

Where additional information is needed, the following secondary sources/methods, while not endorsed by these guidelines can be useful:

- Independent commercial databases such as C6 intelligence, Complanet, Dow Jones, LexisNexis, Worldcheck, International Chamber of Commerce or similar services;
- Site Visits / meetings with Principals (where necessary to obtain information and/or where warranted by the risk).

It is recommended as good practice to also make use of the internet and other available information sources to further test the reliability and completeness of customer information. This includes reference to:

- Media articles; and
- Internet search engines

Designated persons should satisfy themselves that any person representing the entity is legally entitled to do so and where met face to face that they are who they say they are. Receipt of a properly authorised mandate or equivalent from the directors, empowering the individual to open/operate an account or establish the business relationship should be obtained, e.g. authorised signatories list.

Additional requirements for an entity incorporated/established outside Ireland

Company registration documentation and procedures differ from country to country which can create an additional challenge for Designated Persons to ensure that they have been provided with the appropriate constitutive documentation. Where the Designated Person does not have the necessary local knowledge of the jurisdiction appropriate additional measures should be taken to be sure of the veracity or adequacy of documentation provided (for example, one approach is to obtain appropriate legal opinions from lawyers practising in the country of incorporation/establishment or international law firm as to the status and meaning of the documents, together with verification of incorporation/establishment). If the designated person has concerns they should also obtain a translation if this is appropriate given the customer.

Bearer Shares or other Bearer Instruments

Designated Persons may encounter bearer shares or other bearer instruments. Extra care must be taken in the case of companies with capital in the form of bearer shares, because in such cases it is difficult, if not impossible in some cases, to reliably identify the beneficial owner(s). Designated persons should consider the risks involved before entering into business relationships that rely on bearer shares or instruments and, if they consider the risks acceptable, adopt procedures to establish the identities of the holders and beneficial owners of such shares/instruments and to ensure that they are notified whenever there is a change of holder and/or beneficial owner. In developing such procedures, Designated Persons should be conscious of the difficulty of mitigating the inherent risk of bearer instruments unless there are robust controls requiring the dematerialisation of the bearer instruments or their being held in custody by a trusted party, with strong controls over any change in holder or beneficial owner(s).

Depending on its risk assessment of the client, the Designated Person may require that the bearer shares/instruments be held by a named custodian, with an undertaking from that custodian that the Designated Person will be notified of any changes to records relating to these shares/instruments or of any change in custodian.

Section 3 Pension schemes

Occupational pension schemes are deemed to be low risk primarily due to the long-term nature of the product. The following is a list (although not exhaustive) of suitable identification evidence for pension schemes:

- A letter of registration issued by the Pensions Board and the accompanying Scheme Trace Report may also suffice as it will detail the names and addresses of the trustees involved. Such reports are available at short notice via email from the Pensions Board;
- For domestic pension schemes, a copy of the original approval from the Revenue Commissioners is considered a satisfactory verification of identity; and
- For non-domestic pension schemes, where SCDD is not applicable or procurement of a confirmation of registration from the relevant tax authority or Pensions Board is not obtainable, it is recommended that confirmation of identity may be obtained as follows as warranted by risk:
 - o Full name of pension scheme
 - o Registered office address of the pension scheme
 - o Dependent on the legal form identify the details of controllers (Trustees/Directors/Board Members or equivalent)
 - o Verification of the identity of two controllers in accordance with Section 2 of Appendix I;
 - o Constitutional/Formation Document (e.g. Trust Deed)

Section 4 Charities

Non-profit organisations and charities have been used to divert funds for terrorist and other criminal activities and as a result, Designated Persons should be mindful of the risks that charities can present, particularly in the case of unregistered charities.

Charities should be treated for AML/CTF purposes according to their legal form, e.g. if they are an incorporated body then they should be treated as per section 2 above. Where they are formed as trusts, refer to the due diligence obligations appropriate to trusts. In addition, in all cases, the following information must be provided:

Obtain information from the customer or from reliable, independent source on:

- Full name of the charity;
- Nature and purpose of the charity and scope.
- Principal business address of activities;
- Country of establishment;
- A properly authorised mandate to open an account and conferring authority on those who will operate it;
- Identification of the principals controlling the charity and any beneficial owners.

Verification of information may be obtained as follows (the extent of verification will depend on the risk):

- By documented reference to an official publicly-accessible register of charities, where such is available for the country of authorisation or registration of the charity concerned; or
- By documented reference to such register of charities maintained by the Revenue Commissioners, or equivalent tax authority in another jurisdiction, for tax exempt status purposes, where the register is publicly accessible; or
- In accordance with normal business practice and as warranted by the risk of money laundering or terrorist financing, verify the personal identity of signatories and principals in line with the requirements for personal customer.

Section 5 Trusts, foundations and similar entities.

In this section, “trust” means a trust that administers and distributes funds. For convenience, this section will use the term “trusts” to refer to all such arrangements. There is a wide diversity in terms of size, purpose, transparency, accountability and geographical scope in relation to trusts. A Designated Person’s due diligence in relation to trusts should be based on the outcome of the assessment of the potential risk of money laundering or terrorist financing arising from the business relationship with or operations of the trust.

In this part “beneficial owner” in relation to a trust means any of the following as set down in section 28 (2) of the Act

- (a) any individual who is entitled to a vested interest in possession, remainder or reversion, whether or not the interest is defeasible, in at least 25 per cent of the capital of the trust property;
- (b) in the case of a trust other than one that is set up or operates entirely for the benefit of individuals referred to in paragraph (a), the class of individuals in whose main interest the trust is set up or operates;
- (c) any individual who has control over the trust.

In this section “control”, in relation to a trust, means a power (whether exercisable alone, jointly with another person or with the consent of another person) under the trust instrument concerned or by law to do any of the following:

- (a) dispose of, advance, lend, invest, pay or apply trust property;
- (b) vary the trust;
- (c) add or remove a person as a beneficiary or to or from a class of beneficiaries;
- (d) appoint or remove trustees;
- (e) direct, withhold consent to or veto the exercise of any power referred to in *paragraphs (a) to (d)*.

For trusts where the risk is determined as standard, the following information should be obtained:

- Full name of the trust;
- Nature and purpose of the trust (e.g., discretionary, testamentary, bare);
- Country of establishment;
- Names of all trustees;
- Names of any protector or controller or settlor;
- Names of beneficiaries of 25% or more;
- Relevant part of the trust deed setting out all parties to the trust;
- Designated persons should undertake procedures to satisfy themselves that any person representing the trust is legally entitled to do so;
- In accordance with the documentation requirements for individuals (set out in previous section 1 of Appendix 1), the Designated Person should (in accordance with normal business practice and as warranted by the risk of money laundering) verify the identity of trustees (and an authorised signatory if performed in conjunction with authorisation of one trustee) who are empowered to give instructions to the Designated Person or to operate accounts.

Where a trustee is itself a regulated entity, or a company listed on a regulated market, simplified due diligence may apply as set out in Section IV (G).

Trusts with less transparent and more complex structures, may pose a higher money laundering or terrorist financing risk. Some trusts established in jurisdictions with favourable tax regimes have in the

past been associated with tax evasion and money laundering. In respect of trusts in the latter category, the Designated Person's risk assessment may lead it to require additional information on the purpose, funding and beneficiaries of the trust.

Designated persons should make appropriate distinction between those trusts that have a limited range of activities or serve a limited purpose (such as inheritance tax planning) and those where the activities and connections are more sophisticated, or are based in and/or have financial links to other countries.

Other information that might be appropriate to ascertain for higher than standard risk situations includes:

- Donor/settlor/grantor of the funds (except where there are large numbers of small donors);
- Domicile of business/activity;
- Nature of business/activity; and
- Location of business/activity (operating address).

Following its assessment of the money laundering and terrorist financing risk presented by the trust, the Designated Person may be required to verify the identities of additional trustees, and/or of the settlor(s) and the beneficiaries in accordance with the requirements for individual customers.

APPENDIX 2

Alternative documentation supporting financial inclusion

Most prospective customers will be able to provide the standard documents to verify identity as set out in Appendix 1. Where an individual is genuinely not in a position to provide standard evidence of identity it is important that he/she is not prevented from access to the financial system solely due to not being able to produce particular documentation.

This appendix is a non-exhaustive and non-mandatory list of alternative documents that can be used to verify identity in circumstances where a prospective customer cannot, for justifiable reasons, meet the standard identification and verification requirements, or has experienced difficulties in the past when seeking to open accounts. The documents below are not restricted to the categories outlined but arranged in this manner to assist identifying the types of documents that might be available. While a legal foundation is provided for this alternative approach by section 33(3) of the Act, designated person must ensure that the combination of documents received is sufficient to confirm identity as required for the purposes of the Act.

The documentation outlined in this Appendix may contain sensitive personal data, and, as a result, designated persons data security measures should take account of this and such sensitive personal data should not be further processed for separate unrelated purposes. In the event that an individual is unable to provide the documentation sought, designated persons should advise consumers of the relevant bodies that can assist in gathering the required information e.g. Department of Social Protection, Revenue Commissioners etc.

These alternative documents and approaches include:

Customer	Document(s)
Social Welfare recipients	<p>It may be possible to apply standard identification procedures. Otherwise combinations of current versions of the following may be used to verify name, address and date of birth:</p> <ul style="list-style-type: none">- Entitlement letter from the Department of Social Protection;- Identity Confirmation Letter issued by the Department of Social Protection;- Social welfare card issued by the Department of Protection;- Garda Age card (where considered appropriate); or- A letter on headed paper signed and stamped by statutory or non-statutory sectors such as employers, community welfare officers, social welfare officers, social workers, Money Advice and Budgeting Service (MABS), minister of religion, teacher, community employment scheme supervisor, money advisor, justice of the peace, peace commissioner, managers of community development and voluntary organisations, Community

Customer	Document(s)
	Employment Schemes, etc.
Pensioner	Travel Pass
Non Standard Identification	ML-10 Form
Those in care homes/sheltered accommodation/refuge	<p>It may be possible to apply standard identification procedures. Otherwise:</p> <ul style="list-style-type: none"> - Letter from care home manager/manager of sheltered accommodation or refuge confirming name and address (i.e. of care home) and name and date of birth of the customer; - Letter from a known/recognisable employer if the person is in employment, confirming that the individual is in paid employment or - A letter on headed paper signed and stamped by statutory or non-statutory sectors such as employers, community welfare officers, social welfare officers, social workers, Money Advice and Budgeting Service (MABS), managers of community development and voluntary organisations, Community Employment Schemes, etc.
Those on probation	<p>It may be possible to apply standard identification procedures. Otherwise:</p> <ul style="list-style-type: none"> - A letter from the customer's probation officer confirming name and address and date of birth.
Prisoners	<p>It may be possible to apply standard identification procedures. Otherwise, a letter from the governor of the prison confirming name, home address and date of birth.</p>
Economic migrants <i>[here meaning those working temporarily in Ireland, whose lack of banking or credit history precludes their being offered other than a basic bank service]</i>	<p>It may be possible to apply standard identification procedures. Otherwise:</p> <ul style="list-style-type: none"> - Temporary Residency Card; - National Immigration Bureau Card or foreign documentation (e.g. National ID card); - A letter on headed paper signed and stamped by statutory or non-statutory sectors such as employers, community welfare officers, social welfare officers, social workers, Money Advice and Budgeting Service (MABS), minister of religion, teacher, community employment scheme supervisor, money advisor, justice of peace, peace commissioner, managers of community development and voluntary organizations, Community Employment Schemes etc.

Customer	Document(s)
	<p>Further information on work permits for non-EEA nationals can be found at: http://www.entemp.ie/labour/workpermits/ and http://www.citizensinformation.ie</p>
<p>Refugees/Asylum seekers (Programmed Refugees only)</p>	<p>It may be possible to apply standard identification procedures. Otherwise:</p> <ul style="list-style-type: none"> - GNIB card⁶ accompanied by a letter from Government department coordinating resettlement programme (Office of the Minister for Integration). The letter should state the date the person was admitted as a programmed refugee and should have a copy of a photograph printed on the letter (all current applications include a photograph). The letter and photo copy should be stamped with an official stamp of the Department and signed by a person at HEO or above level. Requirement for a photo should be waived for persons admitted to the State prior to 2007; or - A copy of an International Committee of the Red Cross or other travel document issued by the Government of the country of origin (many refugees admitted under the resettlement programme use these documents) accompanied by a letter from the Office of the Minister for Integration stating it is a true copy of the document. The copies should be signed and stamped by the official copying them. - Official letters issued to the person from Government Departments.
<p>Members of the Travelling Community</p>	<p>Members of the Travelling Community should be able to produce standard identification evidence; if not, the following may assist with verification</p> <ul style="list-style-type: none"> - A check with the local authority, which has to register travellers' sites, may be used as appropriate address verification. - A letter on official paper signed and stamped by a person in a position of responsibility from a financial institution, practicing solicitor, accountant, doctor, minister of religion, teacher, social worker, community employment scheme supervisor, money advisor, justice of peace, peace commissioner, etc, confirming identity

⁶ While a GNIB(Garda National Immigration Bureau) card is not proof of identity, it is evidence of the name used by the person when granted permission to remain in the country and the stamp number identifies their rights under Section 3 of the Refugee Act (1996) as amended (Office of the Minister for Integration).

Customer	Document(s)
Students and young people	<p>It should be possible to apply the standard identification procedures in Appendix 1 in the vast majority of cases when opening accounts or transacting with students, young people or minors. However, there may be instances where this category of customer does not possess standard identification documentation. In such instances the following may assist with verification:</p> <ul style="list-style-type: none"> - Students may have student identity cards which can assist in the verification process along with confirmation of identity and address from a known college/university/schools. - CAO letters and confirmations of places sent to the individual. - National age card. - A letter from the school confirming the students identity and address, in respect of 1st level and 2nd level students, who will not have student identity cards. Parental consent should be obtained in the case of minors. <p>Where other young people and minors do not possess relevant documentation, a birth certificate may be provided. The parent/guardian/adult must be identified and verified in accordance with the requirements of Appendix 1.</p> <p>A Designated Person should ensure in such cases that any other beneficial owner of an account is identified and verified in line with standard procedures.</p>
Those without the capacity to manage their financial affairs	<p>It should be possible to apply standard identification procedures. Otherwise:</p> <ul style="list-style-type: none"> - Current medical cards for over 18s with an intellectual disability; - Current entitlement letters/statements/benefit books from Government departments (e.g. Department of Social Protection/Revenue Commissioners); or - Electoral Register Search for those registered. <p>For under 18s, the parent and/or guardian should also be identified and verified in accordance with the requirements of Appendix 1.</p>