Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Anti-Money Laundering and Countering the Financing of Terrorism Guidelines for the Financial Sector

in conjunction with Consultation Paper CP 128

Revision History

Date	Version	Description
21st December 2018	1.0	Consultation Version

Table of Contents

1. Introduction 7
1.1 Purpose and Scope 7
1.2 Status 7
1.3 Data Protection 8
1.4 Glossary 8
2. Legal and Regulatory Framework 10
2.1 Legislative Framework 10
2.2 Regulatory Framework 10
2.3 International Framework 10
3. Money Laundering and Terrorist Financing 11
3.1 Money Laundering 11
3.2 Terrorist Financing 12
4. Risk Management 13
4.1 Risk-Based Approach 13
4.2 Business-wide Risk Assessment 13
4.3 Risk Factors 14
4.4 Customer Risk 14
4.4.1 Customer's Business or Professional Activities 14
4.4.2 Customer's Reputation 16
4.4.3 Customer's Nature and Behaviour 16
4.5 Country or Geographic Risk 18
4.5.1 Nature and Purpose of the Business Relationship within the Jurisdiction 18
4.5.2 Effectiveness of Jurisdiction's AML/CFT Regime 19
4.5.3 Level of Jurisdiction's Predicate Offences 19
4.5.4 Level of Jurisdiction's TF Risk 20
4.5.5 Level of Jurisdiction's Transparency and Tax Compliance 20
4.6 Products, Services and Transactions 20
4.6.1 Transparency of Products, Services or Transactions Risk 21
4.6.2 Complexity of Products, Services or Transactions 21
4.6.3 Value and Size of Products, Services or Transactions 21
4.7 Channel/Distribution Risk 22
4.7.1 How the Business Relationship is Conducted 22
4.7.2 Channels used to introduce Customer to the Firm 22
4.7.3 Use of Intermediaries 23

4.8 Assessing ML/TF risk 23
4.8.1 Weighting Risk Factors 23
4.8.2 Categorising Business Relationships and Occasional Transactions 24
4.8.3 Monitoring and Review of Risk Assessment 24
4.8.4 Emerging ML/TF risks 25
4.8.5 Updating of ML/TF Risk Assessment 26
5. Customer Due Diligence 27
5.1 Application of Risk Assessment 27
5.2 Customer Due Diligence (CDD) 28
5.2.1 Documentation and Information 29
5.2.2 Beneficial Ownership 30
5.2.3 Establishment of a Business Relationship 31
5.2.4 Purpose and Nature of the Business Relationship 31
5.2.5 Use of Innovative Solutions 32
5.2.6 Reliance on Other Parties to carry out CDD 33
5.3 Ongoing Monitoring 35
5.3.1 Monitoring Complex or Unusual Transactions 36
5.4 Simplified Due Diligence (SDD) 37
5.4.1 SDD measures which Firms may apply to Business Relationships or Transactions 37
5.5 Enhanced Customer Due Diligence (EDD) 39
5.6 EDD in relation to Politically Exposed Persons (PEPs) 40
5.6.1 Policies and Procedures in relation to PEPs 41
5.6.2 Senior Management Approval of PEPs 42
5.6.3 Source of Wealth / Source of Funds of PEPs 42
5.6.4 Enhanced On-going monitoring of PEPs 43
5.7 EDD in Relation to Correspondent Relationships 43
5.7.1 Risk Assessment of Correspondent Relationships – 44
5.7.2 Senior Management Approval of Respondent Relationships 45
5.7.3 Responsibilities of each Party regarding Respondent Relationships 45
5.7.4 Correspondent Relationships in connection with Shell Banks 45
5.7.5 Liaison with Respondent Institutions 45
5.7.6 Screening of Respondent Institutions 46
5.7.7 Information Requirements for Correspondent Relationships 46
5.7.8 Ongoing monitoring of Correspondent Relationships 46
5.7.9 Unusual Transactions in Correspondent Relationships 47

5.8 EDD in relation to Complex or Unusual Transactions....47
5.9 EDD in relation to High-Risk Third Countries and other High-Risk Situations..48
6. Governance....51
6.1 Governance....51
6.2 Role and Responsibilities of Senior Management....51
6.2.1 Governance and Oversight....51
6.3 Roles and Responsibilities of the MLRO....53
6.3.1 MLRO Reporting to Senior Management....53
6.4 Three Lines of Defence Model....54
6.5 External Audit....54
6.6 Policies and Procedures....54
6.6.1 Group wide policies and procedures....55
7. Reporting of Suspicious Transactions....56
7.1 Requirement to Report....56
7.2 Identifying suspicious transactions....56
7.3 Timing of Suspicious Transaction Reports ('STRs')....57
7.4 Internal Reporting of Suspicious Transactions....57
7.5 Making Suspicious Transaction Reports....58
7.6 Tipping Off....59
8. Training....61
8.1 AML/CFT Training....61
8.2 Role Specific and Tailored Training....61
8.3 Frequency of training....62
8.4 Training Governance....62
8.5 Training of Outsource Service Providers....62
8.6 Training Channels....63
8.7 Training Records....63
8.8 Training Assessment....63
8.7 Management Information on Training....63
9. Record Keeping....64
9.1 Obligation to retain records....64
9.2 Records a firm should retain....64
9.2 1 Business-wide Risk Assessments....64
9.2.2 Customer Information....65
9.2.3 Transactions....65
9.2.4 Internal and External Suspicious Transaction Reports....65

9.2.5 Reliance on Third Parties to Undertake CDD 66
9.2.6 Minutes of Senior Management Meetings 66
9.2.7 Training 66
9.2.8 Ongoing Monitoring 66
9.3 Assurance Testing of Record Retention 67
10. International Financial Sanctions 68
10.1 Financial Sanctions Framework 68
10.1.1 UN Sanctions 68
10.1.2 EU Sanctions 68
10.2 Role of the Central Bank 69
10.3 Financial Sanctions Obligations on Firms 69
10.3.1 Financial Sanctions Governance 69
10.3.2 Financial Sanctions Risk Assessment 69
10.3.3 Screening Customers against Sanctions Lists 70
10.3.4 Matches and escalation 70

1. Introduction

1.1 Purpose and Scope

The purpose of the Anti-Money Laundering and Countering the Financing of Terrorism Guidelines for the Financial Sector ('the Guidelines') is to assist firms that are credit and financial institutions ('firms') in understanding their AML/CFT obligations under Part 4 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended) ('CJA 2010').

The Guidelines set out the expectations of the Central Bank of Ireland ('Central Bank') regarding the factors that firms should take into account when identifying, assessing and managing ML/TF risks.

1.2 Status

The Guidelines do not constitute secondary legislation and firms must always refer directly to the CJA 2010 when ascertaining their statutory obligations. The Guidelines do not replace or override any legal and/or regulatory requirements. In the event of a discrepancy between the Guidelines and the CJA 2010, the CJA 2010 will apply. The Guidelines are not exhaustive and do not set limitations on the steps to be taken by firms to meet their statutory obligations.

The Guidelines should not be construed as legal advice or legal interpretation. It is a matter for firms to seek legal advice if they are unsure regarding the application of the CJA 2010 to their particular set of circumstances.

For convenience to the user, from time to time, certain text from the CJA 2010 may be directly quoted in italics or otherwise summarised in the Guidelines. For the avoidance of doubt, such quotes or references are contained in blue text boxes. If any inconsistencies occur between the text in the Guidelines and the CJA 2010, the CJA 2010 prevails. References to sections of legislation within the Guidelines should be taken as references to the CJA 2010 unless otherwise stated.

Where the Guidelines have not provided guidance on a specific section from Part 4 of the CJA 2010, it is because that section of the CJA 2010 already provides clear and detailed information on the obligations of firms and further guidance is unnecessary. The guidance also highlights where the CJA 2010 has been materially amended by the 2018 legislative amendments.

Where lists or examples are included in the Guidelines, such lists or examples are non-exhaustive and represent the minimum matters to be covered. The examples present some, but not the only ways, in which firms might comply with their obligations. The Guidelines do not take the place of a firm performing its own assessment of the manner in which it shall comply with its statutory obligations. The Guidelines are not a checklist of

things that all firms must do or not do in order to reduce their ML/TF risk, and should not be used as such by firms.

The Guidelines are not the only source of guidance on ML/TF risk. Firms are reminded that other bodies produce guidance that may also be relevant and useful.

Nothing in the Guidelines should be read as providing an express or implied assurance that the Central Bank would defer or refrain from using its enforcement powers where a suspected breach of the CJA 2010 comes to its attention.

The Central Bank will update or amend the Guidelines from time to time, as appropriate.

1.3 Data Protection

Firms shall comply with their obligations under Part 4 of the CJA 2010 having regard to their obligations under data protection legislation.

1.4 Glossary

The following terms are used throughout the Guidelines:

AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
CDD	Customer Due Diligence
CJA 2010	Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended by the Criminal Justice Act 2013 and the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018
CJA 2005	Criminal Justice (Terrorist Offences) Act 2005
EDD	Enhanced Due Diligence
EEA	European Economic Area
ESAs	European Supervisory Authorities (comprising the European Banking Authority, European Insurance and Occupational Pensions Authority and European Securities and Markets Authority)
EU	European Union
FATF	Financial Action Task Force, the global AML/CFT standard-setting body
firm(s)	Credit or financial institution(s) subject to the CJA 2010
FS	International Financial Sanctions (restrictive measures)

FTR	**Funds Transfer Regulation** Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds as supplemented by S.I. No. 608/2017 - European Union (Information Accompanying Transfers of Funds) Regulations 2017
FIU Ireland	State Financial Intelligence Unit
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
Risk Factors GL	Guidelines issued by the ESAs in accordance with Articles 17 and 18(4) of 4AMLD on simplified and enhanced due diligence and the factors which credit and financial institutions should consider when assessing the ML/TF risk associated with individual business relationships and occasional transactions
Relevant Third Party	Those persons identified in Section 40. (1) (a) – (c) of the CJA 2010
SDD	Simplified Due Diligence
TF	Terrorist Financing
3AMLD	Third EU AML Directive (Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005)
4AMLD	Fourth EU AML Directive (Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015)

Any term used in the Guidelines should be construed in accordance with its definition under the CJA 2010.

2. Legal and Regulatory Framework

2.1 Legislative Framework

The Irish AML/CFT legislative framework is set out in the CJA 2010. This framework was updated with the transposition of 4AMLD into Irish law in *2018 pursuant to the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018*.

Part 4 of the CJA 2010 obliges firms to put in place an effective, risk-based AML/CFT framework, which includes the application of a risk based approach, customer due diligence ("CDD") measures, reporting of suspicious transactions, governance, policies and procedures, record keeping and training.

2.2 Regulatory Framework

The Central Bank is the competent authority for the monitoring of credit and financial institutions' compliance with the CJA 2010 and is responsible for taking reasonable measures to secure such compliance. The Central Bank is also the competent authority for monitoring compliance with the Funds Transfer Regulation.

2.3 International Framework

The FATF is the global standard setting body in the area of AML/CFT. It has set out standards or recommendations, which include the preventative (compliance) measures to be put in place to combat money laundering and terrorist financing. The FATF publishes guidance on the risk based approach to AML/CFT (including sector specific guidance)[1].

The European Union enacts AML/CFT legislation (directives and regulations), which are either transposed or directly effective in national laws. The ESAs play an important role in taking steps to ensure that competent authorities and firms apply European AML/CFT legislation effectively and consistently[2]. Guidelines are published by the ESAs and the Central Bank complies with ESA guidelines by incorporating them into supervisory processes and, where relevant, into these Guidelines.

As the Guidelines do not replace the guidance published by ESAs and FATF, firms should ensure that they are familiar with and have regard to the guidance published by these bodies.

[1] http://www.fatf-gafi.org/publications/?hf=10&b=0&s=desc(fatf_releasedate)

[2] http://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money

3. Money Laundering and Terrorist Financing

3.1 Money Laundering

Money Laundering means an offence as set out under Section 7 of the CJA 2010. It involves the intentional or reckless conversion of property, generated from "criminal conduct", so that the criminal origin of the property is difficult to trace.

Section 7(1) of the CJA 2010 provides that a person commits a [Money Laundering] offence in the State if:

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

(i) concealing or disguising the true nature, source, location, disposition, movement or ownership of the property, or any rights relating to the property;
(ii) converting, transferring, handling, acquiring, possessing or using the property;
(iii) removing the property from, or bringing the property into, the State,

and

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

Section 7(2) of the CJA 2010 provides that a person who attempts to commit an offence under subsection (1) commits an offence.

"Criminal conduct" is defined in Section 6 of the CJA 2010. This definition encompasses all offences whether minor or serious, summary or indictable.

Section 6(b) of the CJA 2010 defines Criminal Conduct 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*"

"Proceeds of Criminal Conduct" is defined in Section 6 of the CJA.

Section 6 of the CJA 2010 defines Proceeds of Criminal Conduct as:

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

3.2 Terrorist Financing

Terrorist Financing means an offence under Section 13 of the Criminal Justice (Terrorist Offences) Act 2005 (CJA 2005).

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

" in or outside the State, the person by any means, directly or indirectly, unlawfully and wilfully provides, collects or receives funds intending that they be used or knowing that they will be used, in whole or in part in order to carry out—

a) an act that constitutes an offence under the law of the State and within the scope of, and as defined in, any treaty that is listed in the annex to the Terrorist Financing Convention, or

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

(i) That is intended to cause death or serious bodily injury to a civilian or to any other person not taking an active part in the hostilities in a situation of armed conflict, and
(ii) The purpose of which is, by its nature or context, to intimidate a population or to compel a government or an international organisation to do, or abstain from doing, any act."

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

4. Risk Management

4.1 Risk-Based Approach

Section 30A and 30B of the CJA 2010 require firms to apply a risk-based approach when applying AML/CFT compliance measures.

Sections 30A and 30B provide for the application of appropriate measures to higher risk customers or areas of business to combat ML/TF. However, it is recognised that resources are finite and must be allocated on a risk sensitive basis. Firms are obliged to understand the level of risk presented by a customer and to be in a position to apply a risk-based approach in their compliance programs.

In applying a risk-based approach to their AML/CFT obligation, firms should be cognisant of the importance and benefits of financial inclusion. A "zero tolerance" approach, or wholesale termination of business relationships with entire categories of customers, without an individual assessment of their risk, is not consistent with the risk-based approach.

4.2 Business-wide Risk Assessment

Section 30A of the CJA 2010 requires firms to conduct a business-wide risk assessment

Section 30B of the CJA 2010 requires firms to identify and assess risk in applying customer due diligence

A risk assessment should consist of two distinct but related steps:

- Identifying ML and TF risks relevant to a firm's business; and
- Assessing the identified ML and TF risks in order to understand how to mitigate those risks.

Firms should rely on their assessment of the risks inherent in their business to inform their risk-based approach to the identification and verification of an individual customer. This in turn should drive the level and extent of due diligence appropriate to that customer. A business-wide risk assessment should assist firms to understand where they are exposed and which areas they should prioritise to combat ML/TF.

4.2.1 Sources

Firms should use various relevant sources when carrying out their business-wide risk assessment, including (but not limited to):

- The National Risk Assessment for Ireland on Money Laundering and Terrorist Financing;
- European Commission's Supra-national Risk Assessment;
- National Risk Assessment of the other jurisdiction(s) in which the firm operates or customers of a firm are located;
- Communications issued by FIU Ireland;
- Risk Factors contained in Schedule 3 and 4 of the CJA 2010;
- Guidance, circulars and other communication from the Central Bank and other relevant regulatory bodies;
- Information from industry bodies;
- Information from international standard setting bodies such as Mutual Evaluation Reports (MERs) or thematic reviews;
- Guidelines, Regulatory Technical Standards and Opinions issued by the ESAs;
- EU Measures, including financial sanctions and designation of high risk countries;
- Information from international institutions and standard setting bodies relevant to ML/TF risks (e.g. UN, IMF, Basel, FATF, Wolfsberg); and
- Other credible and reliable sources that can be accessed individually or through commercially available databases or tools that are determined necessary by a firm on a risk-sensitive basis.

4.3 Risk Factors

Section 30A.(1) of the CJA 2010 sets out the risk factors firms are required to take into account when conducting their business-wide risk assessment. The risk factors must be relevant to the firm's business and include consideration of at least the following; customer; products and services; types of transaction carried out; countries or geographic areas and delivery channels.

Firms should take a holistic view of the risk associated with any given situation and note that unless required by the CJA 2010 or EU legislation, the presence of isolated risk factors does not necessarily move a relationship into a higher or lower risk category.

4.4 Customer Risk

When identifying the risk associated with their customers, including their customers' beneficial owners, firms should consider the risk related to:

- The customer's and the customer's beneficial owner's business or professional activity;
- The customer's and the customer's beneficial owner's reputation; and
- The customer's and the customer's beneficial owner's nature and behaviour.

4.4.1 Customer's Business or Professional Activities

Firms should consider the risk factors associated with a customer's or their beneficial owner's business or professional activity including for example, whether the customer or its beneficial owner:

- Has links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, arms trade and defense, extractive industries, and public procurement;

- Has links to sectors that are associated with higher ML or TF risk, for example certain Money Service Businesses, casinos or dealers in precious metals;

- Has links to sectors that involve significant amounts of cash;

- Is a legal person or a legal arrangement and if so, the purpose of their establishment and the nature of their business;

- Has political connections, for example:
  - the customer or its beneficial owner is a Politically Exposed Person (PEP) or has any other relevant links to a PEP; or
  - One or more of the customer's directors are PEPs and if so, these PEPs exercise significant control over the customer or beneficial owner[3];

- Holds another prominent position or enjoys a high public profile that might enable them to abuse this position for private gain. For example, they are:
  - Senior local or regional public officials with the ability to influence the awarding of public contracts;
  - Decision-making members of high profile sporting bodies;
  - Individuals that are known to influence the government and other senior decision-makers; or

- Is a public body or state owned entity from a jurisdiction with high levels of corruption.

Other risk factors that firms may consider in relation to a customer's business or professional activity include, for example, whether:

- The customer is a legal person subject to enforceable disclosure requirements that ensure that reliable information about the customer's beneficial owner is publicly available. For example, a public company listed on a regulated market or other trading platform that makes such disclosure a condition for listing and/or admission to trading;

- The customer is a credit or financial institution acting on its own account from a jurisdiction with an effective AML/CFT regime. For example whether:
  - It is supervised for compliance with local AML/CFT obligations; and
  - If so supervised, there is no evidence that the customer has been subject to supervisory sanctions or enforcement for failure to comply with AML/CFT

[3]Where a customer or their beneficial owner is a PEP, firms must always apply enhanced due diligence measures in line with Section 37 of the CJA 2010.

obligations or wider conduct requirements in recent years; or

- The customer's background is consistent with what the firm knows about it. For example:
  - Its former, current or planned business activity;
  - The turnover of the business;
  - Its source of funds; and
  - The customer's or beneficial owner's source of wealth.

4.4.2 Customer's Reputation

Risk factors that firms should consider when assessing the risks associated with a customer's or their beneficial owner's reputation include, for example whether:

- There are adverse media reports or other relevant information sources about the customer or its beneficial owner. For example, there are reliable and credible allegations of criminality or terrorism against the customer or their beneficial owners. Firms should determine the credibility of allegations inter alia based on the quality and independence of the source data and the persistence of reporting of these allegations. Firms should note that the absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing;

- The customer, beneficial owner or anyone publicly known to be closely associated with them has currently, or had in the past, their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing;

- The customer or beneficial owner has been the subject of a suspicious transactions report by the firm in the past; or

- The firm has in-house information about the customer's or their beneficial owner's integrity, obtained for example, in the course of a long-standing business relationship.

4.4.3 Customer's Nature and Behaviour

Risk factors that firms should consider when assessing the risk associated with a customer's or their beneficial owner's nature and behaviour[4] include, for example, whether:

- The customer is unable to provide robust evidence of their identity[5];

[4] Firms should note that not all of these risk factors will be apparent at the outset but may emerge only once a business relationship has been established

[5] Firms should note that there may be legitimate reasons that a customer may be unable to provide robust evidence of their identity, for example if the customer is an asylum seeker, the EBA has issued an 'Opinion on the application of Customer Due Diligence Measures to customers who are asylum seekers from higher risk third countries and territories', see https://eba.europa.eu/documents/10180/1359456/EBA-Op-2016-07+%28Opinion+on+Customer+Due+Diligence+on+Asylum+Seekers%29.pdf

- The firm has doubts about the veracity or accuracy of the customer's or beneficial owner's identity;

- There are indications that the customer is seeking to avoid the establishment of a business relationship. For example, the customer wishes to carry out a number of separate wire transfers, or other service, without opening an account, where the opening of an account with a firm might make more economic sense;

- The customer's ownership and control structure appears unnecessarily complex or opaque and there is no obvious commercial or lawful rationale for such structures;

- The customer has nominee shareholders, where there is no obvious reason for having these;

- The customer is a special purpose vehicle (SPV) or structured finance company;

- There are frequent or unexplained changes to a customer's legal, governance or beneficial ownership structures (e.g., to its board of directors);

- The customer requests transactions that are complex, unusually or unexpectedly large or have an unusual or unexpected pattern without apparent economic or lawful purpose or a sound commercial rationale;

- There are grounds to suspect that the customer is trying to evade specific thresholds such as those set out under the definition of "occasional transaction" under the CJA 2010;

- The customer requests unnecessary or unreasonable levels of secrecy. For example, the customer is reluctant to share CDD information, or appears to disguise the true nature of its business;

- The customer's or beneficial owner's source of wealth or source of funds cannot be easily and plausibly explained. For example through its occupation, inheritance or investments;

- The customer does not use the products and services it has taken out as expected when the business relationship was first established;

- The customer is a non-resident and its needs could be better serviced elsewhere. For example, there is no apparent sound economic and/or lawful rationale for the customer requesting the type of financial service sought in this jurisdiction[6];

[6] *Article* 16 of Directive 2014/92/EU creates a right for customers who are legally resident in the European Union to obtain a basic payment account, but this right applies only to the extent that credit institutions can comply with their AML/CFT obligations . See, in particular, Articles 1(7) and 16(4) of Directive 2014/92/EU

- The customer is a non-profit organisation whose activities put them at a heightened risk of being abused for terrorist financing purposes; or
- The customer is insensitive to price or significant losses on investments.

4.5 Country or Geographic Risk

Country or Geographic Risk relates to:

- Jurisdictions in which the customer and beneficial owner is based;
- Jurisdictions which are the customer´s and beneficial owner's places of business; and
- Jurisdictions to which the customer and beneficial owner appear to have relevant personal links, of which the firm should reasonably have been aware.

When identifying the risk associated with countries and geographic areas, firms should consider for example the risk factors related to:

- The nature and purpose of the business relationship within the jurisdiction;
- The effectiveness of the jurisdiction's AML/CFT regime ;
- The level of predicate offences relevant to money laundering within the jurisdiction;
- The level of ML/TF risk associated with the jurisdiction;
- Any economic or financial sanctions against a jurisdiction; and
- The level of legal transparency and tax compliance within the jurisdiction.

4.5.1 Nature and Purpose of the Business Relationship within the Jurisdiction

The nature and purpose of the business relationship will often determine the relative importance of individual country and geographic risk factors. Risk factors firms should consider, include for example:

- Where the funds used in the business relationship have been generated abroad, the level of predicate offences relevant to money laundering and the effectiveness of a country's legal system;
- Where funds are received from or sent to jurisdictions where groups committing terrorist offences are known to be operating, the extent to which this is expected or might give rise to suspicion is based on what the firm knows about the purpose and nature of the business relationship;
- Where the customer is a credit or financial institution, the adequacy of the country's AML/CFT regime and the effectiveness of AML/CFT supervision; or

- For customers other than natural persons, the extent to which the country in which the customer (and where applicable, the beneficial owner/s) is registered, effectively complies with international tax transparency standards.

4.5.2 Effectiveness of Jurisdiction's AML/CFT Regime

Risk factors that firms should consider when assessing the risk associated with the effectiveness of a jurisdiction's AML/CFT regime include, for example, whether:

- The country has been identified by the European Commission as having strategic deficiencies in their AML/CFT regime, under *Article* 9 of 4 AMLD[7]; or

- There is information from one or more credible and reliable sources about the quality of the jurisdiction's AML/CFT controls, including information about the quality and effectiveness of regulatory enforcement and oversight. Examples of possible sources include:
  - Mutual Evaluations of the FATF or FATF-style Regional Bodies (FSRB)[8];
  - The FATF's list of high risk and non-cooperative jurisdictions;
  - International Monetary Fund assessments; and
  - Financial Sector Assessment Programme reports (FSAPs).

Firms should identify lower risk jurisdictions in line with the ESA's Risk Factor GLs and Schedule 3 of CJA 2010.

4.5.3 Level of Jurisdiction's Predicate Offences

Risk factors that firms should consider when assessing the risk associated with the level of predicate offences relevant to money laundering in a jurisdiction include, for example, whether:

- There is information from credible and reliable public sources about the level of predicate offences relevant to money laundering, for example corruption, organised crime, tax crime or serious fraud. Examples include corruption perceptions indices; OECD country reports on the implementation of the OECD's anti-bribery convention; and the UNODC World Drug Report; or

- There is information from more than one credible and reliable source about the capacity of the jurisdiction's investigative and judicial system effectively to investigate and prosecute these offences.

---

[7] Article 18 (1) of 4AMLD provides that if firms deal with natural or legal persons resident or established in third countries that the European Commission has identified as presenting a high money laundering or terrorist financing risk, firms must always apply enhanced due diligence measures

[8] Firms should note that membership of the FATF or an FSRB, e.g. MoneyVal, does not, of itself, mean that the jurisdiction's AML/CFT regime is adequate and effective.

4.5.4 Level of Jurisdiction's TF Risk

Risk factors that firms should consider when assessing the level of TF risk associated with a jurisdiction include, for example, whether:

- There is information, for example, from law enforcement or credible and reliable open media sources, suggesting that a jurisdiction provides funding or support for terrorist activities or that groups committing terrorist offences are known to be operating in the country or territory; or

- The jurisdiction is subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued, for example, by the United Nations and the European Union.

4.5.5 Level of Jurisdiction's Transparency and Tax Compliance

Risk factors that firms should consider when assessing the jurisdiction's level of transparency and tax compliance include, for example, whether:

- There is information from more than one credible and reliable source that the country has been deemed compliant with international tax transparency and information sharing standards and there is evidence that relevant rules are effectively implemented in practice. Examples of possible sources include:
  - Reports by the OECD's Global Forum on Transparency and the Exchange of Information for Tax Purposes, which rate jurisdictions for tax transparency and information sharing purposes;
  - Assessments of the jurisdiction's commitment to automatic exchange of information based on the Common Reporting Standard;
  - Assessments by the FATF of the jurisdiction's compliance with FATF Recommendations 9, 24 and 25 and Immediate Outcomes 2 and 5[9]; or
  - FSRB or IMF assessments (for example IMF staff assessments of Offshore Financial Centres);

- The jurisdiction is committed to, and has effectively implemented, the Common Reporting Standard on Automatic Exchange of Information, which the G20 adopted in 2014; and

- The jurisdiction has put in place reliable and accessible beneficial ownership registers.

4.6 Products, Services and Transactions

Risk factors that firms should consider when assessing the risk associated with their products, services or transactions, include, for example:

- The level of transparency, or opaqueness, the product, service or transaction afford;

[9] http://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate)

- The ability to transfer ownership of assets;
- The complexity of the product, service or transaction; and
- The value or size of the product, service or transaction.

4.6.1 Transparency of Products, Services or Transactions Risk

Risk factors that firms should consider when assessing the risk associated with the transparency of products, services or transactions include, for example:

- The extent to which products or services facilitate, or allow anonymity or opaqueness of customer, ownership or beneficiary structures that could be used for illicit purposes, for example:
  - pooled accounts, bearer shares, fiduciary deposits, offshore and certain trusts;
  - legal entities structured in a way to take advantage of anonymity; and
  - dealings with shell companies or companies with nominee shareholders;
- The extent to which is it possible for a third party that is not part of the business relationship to give instructions, for example, certain correspondent banking relationships.

4.6.2 Complexity of Products, Services or Transactions

Risk factors that firms should consider when assessing the risks associated with a product, service or transaction's complexity include, for example:

- The extent that the transaction is complex and involves multiple parties or multiple jurisdictions, for example, certain trade finance transactions;
- Conversely, the extent that the transaction is straightforward, for example, regular payments into a pension fund;
- The extent that the products or services allow payments from third parties or accept overpayments. Where third party payments are permitted, the extent to which:
  - The firm can identify the third party and understands their relationship with the customer, for example a state welfare body; and
  - Products and services are funded primarily by fund transfers from the customer's own account at another financial institution that is subject to AML/CFT standards and oversight comparable to those required under 4AMLD;
- The risks associated with new or innovative products or services, in particular where this involves the use of new technologies or payment methods.

4.6.3 Value and Size of Products, Services or Transactions

Risk factors that firms should consider when assessing the risk associated with the value or size of a product, service or transaction include, for example:

- The extent that products or services may be cash intensive, for example, certain types of payment services and current accounts; and

- The extent that products or services facilitate or encourage high value transactions, for example there are no caps on certain transaction values or levels of premium that could limit the use of the product or service for money laundering or terrorist financing purposes.

4.7 Channel/Distribution Risk

When identifying the risk associated with Channel/ Distribution, firms should consider the risk factors related to:

- The extent that the business relationship is conducted on a non-face to face basis; and

- Any introducers or intermediaries the firm utilises and the nature of their relationship to the firm.

4.7.1 How the Business Relationship is Conducted

Risk factors that firms should consider when assessing the risk associated with how the business relationship is conducted, include for example, whether:

- The customer is physically present for identification purposes. If they are not,
  - Whether the firm uses reliable forms of non-face to face CDD; and
  - The extent that the firm has taken steps to prevent impersonation or identity fraud.

4.7.2 Channels used to introduce Customer to the Firm

Risk factors that firms should consider when assessing the risk associated with customers introduced to the firm, include for example, whether:

- The customer has been introduced from other parts of the same financial group and if so,
  - The extent that the firm can rely on this introduction as reassurance that the customer will not expose the firm to excessive ML/TF risk; and
  - The extent that the firm has taken measures to satisfy itself that the group entity applies CDD measures to EEA standards in line with Section 57 of the CJA 2010;

- The customer has been introduced from a third party, for example a bank that is not part of the same group. In such instances, whether that third party is a financial institution or their main business activity is unrelated to financial service provision;

- Where the customer has been introduced by a third party, the extent of the measures that the firm has undertaken to be satisfied that:

  - the third party applies CDD measures and keeps records equivalent to EEA standards and that it is supervised for compliance with comparable AML/CFT obligations in line with Section 40 (1) of the CJA 2010;

- the third party will provide, immediately upon request, relevant copies of identification and verification data, among others in line with Section 40 (4) (b) of the CJA 2010; and
- the quality of the third party's CDD measures is such that it can be relied upon.

4.7.3 Use of Intermediaries

Risk factors that firms should consider when assessing the risk associated with the use of intermediaries, include for example, whether the intermediary is:

- A regulated person subject to AML obligations that are consistent with those of the 4AMLD;

- Subject to effective AML supervision and there are no indications that the intermediary's level of compliance with applicable AML legislation or regulation is inadequate, for example because the intermediary has been sanctioned for breaches of AML/CFT obligations;

- Involved on an ongoing basis in the conduct of business and whether this affects the firm's knowledge of the customer and ongoing risk management;

- Based in a jurisdiction associated with higher ML/TF risk. Where a third party is based in a high risk third country that the European Commission has identified as having strategic deficiencies, firms should not rely on that intermediary. Reliance may be placed on an intermediary where it is a branch or majority-owned subsidiary of another firm established in the EU, and the firm is confident that the intermediary fully complies with group-wide policies and procedures.

4.8 Assessing ML/TF risk

Firms should take a holistic view of the ML/TF risk factors they have identified that, together, will determine the level of ML/TF risk associated with a business relationship or transaction.

4.8.1 Weighting Risk Factors

As part of this assessment, firms should consider whether to weigh risk factors differently depending on their relative importance.

When weighting risk factors, firms should make an informed judgment about the relevance of different risk factors in the context of a business relationship or transaction. The weight given to each of these factors is likely to vary from product to product and customer to customer (or category of customer) and from one firm to another. When weighting risk factors firms should ensure that:

- Weighting is not unduly influenced by just one factor;

- Economic or profit considerations do not influence the risk rating;

- Weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk;

- Situations identified by 4AMLD or national legislation as always presenting a high money laundering risk cannot be over-ruled by the firm's weighting, for example a correspondent relationship with a firm outside of the EEA; and

- Firms are able to override any automatically generated risk scores where necessary. The rationale for the decision to override such scores should be governed and documented appropriately.

Where firms use automated IT systems to allocate overall risk scores to categorise business relationships or transactions and does not develop these in house, rather purchases them from an external provider, they should ensure that:

- The firm fully understands the risk rating methodology and how it combines risk factors to achieve an overall risk score;

- The methodology used meets the firm's risk assessment requirements and legislative obligations; and

- The firm is able to satisfy itself that the scores allocated are accurate and reflect the firm's understanding of ML/TF risk.

4.8.2 Categorising Business Relationships and Occasional Transactions

Following their risk assessment, firms should categorise their business relationships and occasional transactions according to the perceived level of ML/TF risk.

Firms should decide on the most appropriate way to categorise risk[10]. This will depend on the nature and size of the firm's business and the types of ML/TF risk to which it is exposed.

The steps firms take to identify and assess ML/TF risk across their business should be proportionate to the nature and size of each firm.

4.8.3 Monitoring and Review of Risk Assessment

Section 30A.(4) of the CJA 2010 provides that a firm :

"…. shall keep the business risk assessment, and any related documents, up to date in accordance with its internal policies, controls and procedures"

[10]For example firms may categories risk as high, medium and low, or variations of the similar ratings

Firms should keep their business wide risk assessment and assessments of the ML/TF risk associated with individual business relationships and occasional transactions as well as of the underlying factors under review to ensure their assessment of ML/TF risk remains up to date and relevant. Where the firm is aware that a new risk has emerged, or an existing one has increased, this should be reflected in business wide risk assessment as soon as possible.

Firms should assess information obtained as part of their ongoing monitoring of a business relationship and consider whether this affects the risk assessment.

4.8.4 Emerging ML/TF risks

Firms should ensure that they have systems and controls in place to identify emerging ML/TF risks and that they can assess these risks and, where appropriate, incorporate them into their business-wide and individual risk assessments in a timely manner.

Examples of systems and controls firms should put in place to identify emerging risks include:

- Processes to ensure that internal information is reviewed regularly to identify trends and emerging issues;

- Processes to ensure that the firm regularly reviews relevant information from sources such as:

    - The Irish National Risk Assessment;
    - The European Commission's Supra-national Risk Assessment;
    - National Risk Assessment of the jurisdiction(s) in which the firm operates or customers of a firm are located;
    - Communications issued by FIU Ireland;
    - Guidance, circulars and other communication from the Central Bank and other relevant regulatory bodies ;
    - Information obtained as part of the initial CDD process;
    - The firm's own knowledge and expertise;
    - Information from industry bodies;
    - Information from international standard setting bodies such as Mutual Evaluation Reports (MERs) or thematic reviews;
    - Changes to terror alerts and sanctions regimes as soon as they occur, for example by regularly reviewing terror alerts and looking for sanctions regime updates;
    - Information from international institutions and standard setting bodies relevant to ML/TF risks (e.g. UN, IMF, Basel, FATF, Wolfsberg); and
    - Other credible and reliable sources that can be accessed individually or through commercially available databases or tools that are determined necessary by a firm on a risk-sensitive basis;

- Processes to capture and review information on risks relating to new products;

- Engagement with other industry representatives, competent authorities and FIU (e.g. round tables, conferences and training providers), and processes to feed back any findings to relevant staff; and

- Establishing a culture of information sharing and strong ethics within the firm.

4.8.5 Updating of ML/TF Risk Assessment

Firms should put in place systems and controls to ensure their individual and business-wide risk assessments remain up to date. Examples include:

- Setting a timeline on which the next risk assessment update will take place annually, to ensure changing, new or emerging risks are included in risk assessments. Where the firm is aware that a new risk has emerged, or an existing one has increased, this should be reflected in risk assessments as soon as possible;

- Carefully recording issues throughout the year that could have a bearing on risk assessments, such as:

    - Internal suspicious transaction reports;
    - Compliance failures and intelligence from front office staff; or
    - Any findings from internal/external audit reports;

Like the original risk assessments, any update to a risk assessment and adjustment of accompanying CDD measures should be documented, proportionate and commensurate to the ML/TF risk.

5. Customer Due Diligence

5.1 Application of Risk Assessment

Section 30B.(1) of the CJA 2010 requires firms to identify and assess the ML/TF risk in relation to a customer or particular transaction in order to determine the level of customer due diligence required under Sections 33 and 35 .

In carrying out the determination, Section 30B.(1) requires firms to have regard to:

"(a) the relevant business risk assessment,

(b) the matters specified in Section 30A(2),

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

(i) the purpose of an account or relationship;

(ii) the level of assets to be deposited by a customer or the size of transactions undertaken;

(iii) the regularity of transactions or duration of the business relationship;

(iv) any additional prescribed risk variable,

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

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

(f) any additional prescribed factor suggesting potentially higher risk"

Firms should document their determination under Section 30B.(1) in writing and retain the determination in accordance with the firm's record keeping policies and procedures. Where a firm does not document their determination under Section 30B. (1), the Central Bank may direct them to do so.

5.2 Customer Due Diligence (CDD)

Sections 33 to 39 of the CJA 2010 provide the CDD measures which a firm must take in order to comply with its obligations in respect of identifying and verifying customers, persons purporting to act on behalf of customers and beneficial owners.

In accordance with Section 33(1) of the CJA 2010, firms are required to identify and verify customers and where applicable, beneficial owner(s):

- prior to the establishment of a business relationship with a customer;
- prior to carrying out an occasional transaction or service for a customer;
- prior to carrying out any service for a customer where the firm has reasonable grounds to doubt the veracity or adequacy of documents; and
- at any time, including where the relevant circumstances of a customer have changed

The level of CDD measures which a firm is required to apply under Sections 33 to 39 depends upon the nature of the relationship between the firm and its customer, the type of business conducted and the perceived ML/TF risks arising.

Section 33(8)(a) of the CJA 2010 prohibits firms that are unable to identify and verify a customer due to the failure of that customer to provide the necessary documentation or information, from providing any service or carrying out any transactions sought by that customer while the documentation or information required remains outstanding.

Section 33(8)(b) of the CJA 2010 provides that firms must separately and distinctly take action to discontinue the business relationship with the customer in such circumstances.

CDD involves more than just verifying the identity of a customer. Firms should collect and assess all relevant information in order to ensure that the firm:

- Knows its customers, persons purporting to act on behalf of customers and their beneficial owners, where applicable;
- Knows what it should expect from doing business with them; and
- Is alert to any potential ML/TF risks arising from the relationship.

Firms should consider the following steps when conducting CDD measures in relation to new and existing customers, products or services. The list is non-exhaustive and it is for each firm to demonstrate its compliance with the obligations set out under the CJA 2010.

- Where CDD is completed during the establishment of the business relationship, the policies and procedures should specify the defined timeframe in which CDD must be completed. The duration of this defined timeframe should minimise the risk of being unable to contact the customer or return the funds to the original source, should there be a requirement to discontinue the business relationship;

- Ensuring that contractual arrangements for new customers adhere to the statutory obligations as prescribed by Section 33 (8) (a) and (b) of the CJA 2010. In relation to the circumstances that would result in the discontinuance of the business relationship and the subsequent effect of such discontinuance, customer consent should be obtained by the firm in advance as part of the on-boarding process; and

- Implement processes that allows the firm to return funds directly to the source from which they came. Firms should exercise caution when considering the means of doing this, so as not to appear to convert or legitimise such funds. Firms should also consider whether there is any cause for suspicion of ML/TF in circumstances where CDD is not forthcoming, and ensure suspicious transaction reporting obligations are fulfilled as required. It is important that at all times, firms act in the best interest of the customer (or prospective customer) and exhaust all possible avenues before taking any actions that might disadvantage customers.

5.2.1 Documentation and Information

Evidence of identity can take a number of forms. Firms should set out in their policies and procedures the documents and information which they are willing to accept and the circumstances under which they are willing to accept them in order to identify and verify the identity of a customer[11].

Firms should retain records evidencing identity in either paper or electronic format.

[11] Where appropriate, firms should also document their approach to accepting alternative documentation to support financial inclusion.

5.2.2 Beneficial Ownership

Section 33(2)(b) of the CJA 2010 requires firms to:

- identify any beneficial owner(s) connected with a customer or service; and
- take measures reasonably warranted due to the ML/TF risk to verify the beneficial owner's identity

to the extent necessary to ensure that the firm has reasonable grounds to be satisfied that the firm knows who the beneficial owner is and in the case of certain legal structures, to understand the ownership and control structure of the entity or arrangement concerned.

With regard to Section 33(2)(b), firms should:

- Compile detailed, documented assessments determining scenarios where beneficial ownership may be a factor with regard to the provision of products and services offered by the firm; and

- Assess and document the circumstances under which it would be reasonably warranted due to the ML/TF risk to verify the identity of any beneficial owners and procedures to be applied in these circumstances.

Firms should note that while there is an obligation to identify all beneficial owners and verify the identity of beneficial owners on a risk based approach, 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, firms may, on the basis of an appropriate risk assessment, determine that it is not necessary to enquire any further regarding the beneficial owner.

In all other instances, firms are required to verify the beneficial owner's identity in accordance with Section 33(2) to ensure that they are satisfied that they know who the beneficial owner is.

5.2.3 Establishment of a Business Relationship

Section 33(1)(a) of the CJA 2010 requires firms to to identify and verify the identity of a customer or beneficial owner prior to establishing a business relationship with the customer.

However, Section 33(5) of the CJA 2010 allows firms to identify and verify the identity of a customer or beneficial owner during the establishment of a business relationship:

"*…where a firm reasonably believes that:*

(a) Verifying the identity of the customer or beneficial owner prior to the establishment of the relationship would interrupt the normal conduct of business; and

(b) There is no real risk that the customer is involved in, or the service sought is for the purposes of money laundering or terrorist financing".

In such circumstances, firms must take reasonable steps to verify the identity of the customer or beneficial owner as soon as practicable.

Where firms avail of the provisions of Section 33(5), they should document and retain their reasons for doing so. Where they are unable to take reasonable steps to verify the identity of the customer or beneficial owner, firms should be aware of their obligations under Section 33(8) in this regard.

5.2.4 Purpose and Nature of the Business Relationship

Section 35(1) of the CJA 2010, requires firms to obtain information reasonably warranted by the ML/TF risk on the purpose and intended nature of the business relationship with a customer prior to the establishment of the relationship.

Firms are required to obtain sufficient information about their customers in order to adequately monitor their activity and transactions and to satisfy themselves that the account is operating in line with the intended purpose.

Firms should identify the most appropriate information necessary to satisfy their obligations under Section 35(1). Depending on the type of customer, the information might include, for example:

- Information concerning the customer's or beneficial owner's business or occupation/employment;
- Information on the types of financial products or services which the customer is looking for;
- Establishing the source of funds in relation to the customer's anticipated pattern of transactions;
- Establishing the source of wealth of the customer (particularly for high risk customers);
- Copies of the customer's most recent financial statements;
- Establishing any relationships between signatories and underlying beneficial owners;
- Any relevant information pertaining to related third parties and their relationships with / to an account for example, beneficiaries; or
- The anticipated level and nature of the activity that is to be undertaken through the business relationship, which may include the number, size and frequency of transactions that are likely to pass through the account.

While firms are obliged under Section 35(1) to obtain information on the purpose and nature of the business relationship at the outset of the relationship, the reliability of this profile should increase over time as the firm learns more about the customer, their use of products/accounts and the financial activities and services that they require.

Firms should ensure they review any known information on the customer and monitor their transactions/activity, in order to ensure they understand the potentially changing purpose and nature of the business relationship.

5.2.5 Use of Innovative Solutions

Firms should note that the CJA 2010 is technology neutral with regard to the sources which a firm can use in order to comply with its CDD obligations under the CJA 2010.

Where a firm utilises such innovative or so called "RegTech" solutions (collectively referred to here as 'RegTech solution') to assist with their AML/CFT obligations the firm should:

- fully understand the impact the RegTech solution has on the firm's regulatory compliance;
- ensure that the RegTech solution can achieve compliance for the firm with its relevant AML/CFT obligations when the RegTech solution goes live;

- ensure that the RegTech solution is capable of being audited by an independent third party; and

- undertake a compliance risk assessment of the RegTech solution on an annual basis either independently of, or incorporated into, the firm's annual AML/CFT risk assessment.

Firms remain responsible at all times for ensuring that the utilisation of the RegTech solution complies with the firm's regulatory obligations. Firms utilising such RegTech solutions should also have regard to the Joint Committee of the ESAs *Opinion on the use of innovative solutions by credit and financial institutions* when complying with their CDD obligations[12].

5.2.6 Reliance on Other Parties to carry out CDD

Section 40(3) of the CJA 2010, provides that firms can rely on certain relevant third parties ("Third Party" or "Third Parties") as set out under Section 40 subsections (1) (a) to (d) to complete CDD measures required under Section 33 or 35(1) of the CJA 2010.

Section 40(3) of the CJA 2010 provides that firms may rely on a Third Party to apply the measures under Section 33 or 35(1) only if:

- there is an arrangement in place between the firm and the Third Party confirming that the third party accepts being relied upon; and

- the firm is satisfied, either that the third party is a person that is supervised or monitored for compliance with the requirements specified under 4AMLD, or requirements equivalent to those under 4AMLD, or on the basis of the arrangement, the Third Party will forward to the firm, as soon as practicable after a request from the firm, any CDD documents or information obtained.

Section 40(5) of the CJA 2010 provides that firms that rely on a Third Party to apply measures under Section 33 or 35(1) of the CJA 2010 remain liable for any failure to apply the measure.

When placing reliance on Third Parties to undertake CDD, firms should ensure that:

- There is a signed agreement in place between the firm and the Third Party, where the Third Party has formally consented to being relied upon and the firm is satisfied, either that the Third Party is a person that is supervised or monitored for compliance with

12 http://www.eba.europa.eu/documents/10180/2100770/Opinion+on+the+use+of+innovative+solutions+by+credit+and+financial+institutions+in+the+customer+due+diligence+process+%28JC-2017-81%29.pdf

the requirements specified under 4AMLD, or requirements equivalent to those under 4AMLD, or on the basis of the arrangement, the Third Party will provide the firm with the underlying CDD documentation or information, in a timely manner upon request. In the absence of such an arrangement, the provisions of Section 40(4) do not apply and the firm should itself carry out the necessary CDD;

- The signed agreement should have clear contractual terms in respect of the obligations of the Third Party to obtain and maintain the necessary records, and to provide the firm with CDD documentation or information upon request. The signed agreement should not contain any conditional language, whether explicit or implied, which may result in the inability of the Third Party to provide the underlying CDD documentation or information upon request. Examples of such conditional language include (but are not limited to) terms such as 'to the extent permissible by law', 'subject to regulatory request' etc.;

- The firm's policies and procedures set out an approach with regard to the identification, assessment, selection and monitoring of Third Party relationships, including the frequency of testing performed on such Third Parties;

- The firm only relies on the Third Party to carry out CDD measures required by Section 33 and 35(1). Firms may not rely on the Third Party to fulfil the on-going monitoring requirements, which they are obliged to conduct as warranted by the risk of their underlying customers, as prescribed by Section 35(3). Firms should note that they cannot rely on the third party to perform the EDD measures or provide Senior Management approval. However, the relevant third party may provide assistance to the firm in gathering the necessary documentation or information to establish the source of wealth and source of funds;

- The firm conducts regular assurance testing to ensure documentation can be retrieved without undue delay, and that the quality of the underlying documents obtained is sufficient; and

- The firm ensures that it has fully satisfied itself that, in placing such reliance, it can meet its obligations under the CJA 2010 prior to placing reliance upon a Third Party based in jurisdictions known for banking secrecy or similarly restrictive legislation.

Firms should note that placing reliance on a Third Party in accordance with Section 40(3) of the CJA 2010 does not include a situation where a firm has appointed another entity to apply the necessary measures as an outsourcing service provider, intermediary, or an agent of the firm. In such cases, the outsourced service provider, intermediary, or agent may actually obtain the appropriate verification evidence in respect of the customer but the firm remains responsible for ensuring compliance with the obligations contained with the CJA 2010.

See also Section 5.6.1.C of the Guidelines regarding Third Party Reliance for PEPs.

5.3 Ongoing Monitoring

Section 35(3) of the CJA 2010, requires firms to monitor any business relationship that it has with a customer to the extent reasonably warranted by the risk of ML/TF.

Section 54(3) of the CJA 2010 requires firms to adopt internal policies, controls and procedures dealing with:

- the monitoring of transactions and business relationships;
- the identification and scrutiny of complex or large transactions, unusual patterns of transactions that have no apparent economic or visible lawful purpose and any other activity that the firm has reasonable grounds to regard as particularly likely, by its nature, to be related to money laundering or terrorist financing;
- measures to be taken to keep documents and information relating to risk assessments by the firm up to date.

When assessing CDD obligations in relation to the on-going monitoring of customers, firms should ensure that they have effective and appropriate on-going monitoring policies and procedures that are in place, in operation and adhered to by all staff. Such policies and procedures should include at a minimum:

- Full review and consideration of all trigger events associated with their customers. Clear examples of trigger events[13] that are understood by staff and targeted training should be provided for staff on how to identify possible trigger events and interpret these. Trigger events should also be reviewed on a regular basis by the firm and examples revised where appropriate;

- A well-documented and well-established monitoring programme, which is demonstrative of a risk-based approach, where high-risk customers are reviewed on a frequent basis;

- Periodic reviews of all customers, the frequency of which is commensurate with the level of ML/TF risk posed by the customer. Firms should also ensure that staff are provided with specific training on how to undertake a periodic review;

[13] Definitive lists of trigger events may lead to complacency within the firm, as staff may not be open to suspicious activity outside of the listed triggers. Rather firms should list examples of trigger events which should provoke staff to 'think outside the box'.

- Reassessment and, if applicable, re-categorisation of customers upon material updates to CDD information and/or other records gathered through a trigger event or periodic review;
- Re-categorisation of customers as high risk subject to Senior Management approval and the completion of Enhanced Due Diligence[14] before a decision is taken to continue the relationship;

- Screening undertaken of all customers to identify new and on-going PEP relationships. The frequency of such screening should to be determined by the firm, commensurate with the firm's business wide risk assessment;

- Clear instruction for staff regarding the action required where appropriate CDD documentation or information is not held on file. Such instruction should include the steps that may be taken to locate or obtain such documentation or information[15]; and

- Proactive utilisation of customer contact as an opportunity to update CDD information.

5.3.1 Monitoring Complex or Unusual Transactions

Section 36A.(1) CJA 2010, requires firms to examine the background and purpose of all complex or unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose

Section 36A.(2) CJA 2010 requires firms to increase the degree and nature of monitoring of a business relationship in order to determine whether transactions referred to in Section 36A.(1) appear suspicious.

Firms should attempt to establish the rationale for changes in behaviour and take appropriate measures, for example conducting additional due diligence or if warranted, submitting a suspicious transaction report to FIU Ireland and the Revenue Commissioners.

See also Section 5.8 of the Guidelines below regarding complex or unusual transactions

[14] Enhanced Due Diligence is discussed further in section 5.5 of the Guidelines

[15] Where it is necessary to write to customers to seek relevant documentation or information, such communications must clearly detail what is being requested and why, as well as the potential consequences for the customer of failure to provide such documentation or information, as specified in Section 33(8) of the CJA 2010 which are discussed in further detail in section 4.11 below.

5.4 Simplified Due Diligence (SDD)

Firms can no longer avail of the exemptions previously contained in Section 34 and 36 of the Act, as these sections have been repealed. A new section 34 (A) has been introduced.

Section 34A(1) of the CJA 2010 provides that firms may take SDD measures to such extent and at such times as is reasonably warranted by the lower ML/TF risk in relation to a business relationship or transaction where they have :

- *"identified in their business risk assessment an area of lower risk into which the business relationship or transaction falls; and*
- *considers that the relationship or transaction presents a lower degree of risk".*

Section 34A(2) of the CJA 2010 provides that prior to applying the measures under Section 34A (1), firms are required to conduct appropriate testing to satisfy themselves that the customer or business qualifies for the simplified treatment,

Section 34A(3) of the CJA 2010 provides that where a firm has applied SDD measures in accordance with Section 34A(1), it is required to:

- *"Retain a record of the reasons for its determination and evidence upon which it was based; and*
- *Carry out sufficient monitoring of the transactions and business relationships to enable the firm to detect unusual or suspicious transactions."*

5.4.1 SDD measures which Firms may apply to Business Relationships or Transactions

Firms should identify the most appropriate SDD measures to apply to business relationships or transactions in accordance with their policies and procedures. SDD measures which firms may apply, include but are not limited to:

- Adjusting the timing of CDD where the product or transaction sought has features that limit its use for ML/TF purposes, for example by:
    - Verifying the customer's or beneficial owner's identity during the establishment of the business relationship; or
    - Setting defined thresholds or reasonable time limits, above or after which the identity of the customers or beneficial owners must be verified. In such circumstances, firms should make sure that:
        - This does not result in a de facto exemption from CDD. Firms should ensure that the customer's or beneficial owner's identity will ultimately be verified;

- They have systems or processes[16] in place to detect when the threshold or time limit has been reached; and
- They do not defer CDD or delay obtaining relevant information about the customer where applicable legislation, for example FTR or provisions in national legislation, require that this information be obtained at the outset;

- Adjusting the quantity of information obtained for identification, verification or monitoring purposes, for example by:
  - Verifying identity on the basis of information obtained from one reliable, credible and independent document or data source only; or
  - Assuming the nature and purpose of the business relationship because the product is designed for one particular use only, such as a company pension scheme;
- Adjusting the quality or source of information obtained for identification, verification or monitoring purposes, for example by:
  - Accepting information obtained from the customer rather than an independent source when verifying the beneficial owner's identity (note that this is not permitted in relation to the verification of the customer's identity);
  - Relying on the source of funds to meet some of the CDD requirements, where the risk associated with all aspects of the relationship is very low, for example where the funds are state benefit payments;
  - Adjusting the frequency of CDD updates and reviews of the business relationship, for example carrying these out only when trigger events occur such as the customer looking to take out a new product or service or when a certain transaction threshold is reached; or
  - Adjusting the frequency and intensity of transaction monitoring, for example by monitoring transactions above a certain threshold only. Where firms choose to do this, they should ensure that the threshold is set at a reasonable level and that they have systems in place to identify linked transactions that, together, would exceed that threshold.

When applying SDD measures, firms should obtain sufficient information to enable them to be reasonably satisfied that their assessment that the ML/TF risk associated with the relationship is low is justified. Firms should obtain sufficient information about the nature of the business relationship to identify any unusual or suspicious transactions. Firms should note that SDD does not exempt it from reporting suspicious transactions to the FIU Ireland and the Revenue Commissioners.

[16] Such systems and processes may be manual or automated in nature.

If firms adjust the amount, timing or type of each or all of the SDD measures undertaken, then such adjustment should be commensurate with the low level of ML/TF risk, which the firms have identified.

5.5 Enhanced Customer Due Diligence (EDD)

Sections 37 to 39 of the CJA 2010 prescribes a number of circumstances in which firms are required to apply EDD measures:

- Where the customer, or the customer's beneficial owner, is a PEP;
- Where a firm enters into a correspondent relationship with a respondent institution from a non-EEA state;
- Where a firm deals with natural persons or legal entities established in high-risk third countries; and
- To a business relationship or transaction that they have identified as presenting a higher degree of risk.

Firms should also apply risk proportionate levels of EDD measures in those situations where it is commensurate to the ML/TF risk they have identified. In circumstances in which a firm has determined that customers or business scenarios present a higher ML/TF risk, EDD measures should be applied. For example:

- Firms should ascertain whether they have obtained adequate information regarding the customer and the customer's business in the context of the service they are providing to the customer, to form a basis for a reliable and comprehensive assessment of the risks arising.

  If the information is not adequate, firms should seek additional documentation, which may include, for example:
  - Establishing a customer's source of wealth / source of funds; and/or
  - Additional information regarding the customer and/or service, including additional CDD information in any case where the firm has doubts about the veracity or adequacy of information previously obtained.

- Firms should apply an enhanced level of ongoing monitoring to their business with the customer, as appropriate to their assessment of the ML/TF risk arising from the business with that customer. Firms should review the level of that monitoring on a regular basis to ensure that it remains risk-appropriate.

Firms should apply EDD measures in higher risk situations to manage and mitigate those risks appropriately. EDD measures cannot be substituted for CDD measures but must be applied in addition to CDD measures.

5.6 EDD in relation to Politically Exposed Persons (PEPs)

Section 37 of the CJA 2010 requires the identification of PEPs and the application of EDD measures to PEPS.

The 2018 amendments to the CJA 2010 broadened the application of the PEP regime to include all PEPs, irrespective of residency, including PEPs from Ireland.

Individuals who have or have had, a high political profile, or hold or have held, public office, can pose a higher money laundering risk to firms as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to know close associates.

Firms should note that PEP status itself is intended to apply higher vigilance to certain individuals and put those individuals that are customers or beneficial owners into a higher risk category. It is not intended to suggest that such individuals are involved in suspicious activity.

Section 37 of the CJA 2010 provides a definition of persons who are classified as PEPs and the steps which firms must undertake to determine whether any of the following are PEPs, immediate family members of a PEP or a close associates of a PEP:

- a customer or beneficial owner connected with the customer or service concerned; or
- a beneficiary of a life assurance policy or other investment related assurance policy; or
- a beneficial owner of the beneficiary.

Firms are required to undertake the steps:

- prior to the establishment of a business relationship;
- prior to carrying out an occasional transaction, or
- prior to the pay out of a life assurance policy or the assignment of such a policy.

The steps to be taken by firms under Section 37 should reflect the level of risk that the customer or beneficial owner is involved in money laundering or terrorist financing.

In demonstrating compliance with the obligations set out under Section 37, firms should undertake the measures outlined in Sections 5.6.1 to 5.6.4 below.

5.6.1 Policies and Procedures in relation to PEPs

A. PEP Identification

Firms should put appropriate policies and procedures in place to determine:

- If a customer or beneficiary is a PEP at on boarding; or
- If a customer becomes a PEP during the course of the business relationship with the firm.

Firms should note that new and existing customers may not initially meet the definition of a PEP, but may subsequently become one during the course of a business relationship with the firm. On this basis, firms should undertake regular and on-going screening of their customer base and the customers' beneficial owners (where relevant), to ensure that they have identified all PEPs. The frequency of PEP screening should be determined by firms commensurate with their business wide risk assessment.

B. Management of PEPS

Firms' policies and procedures should address how any PEP relationships identified will be managed by the firm including:

- Application of EDD measures to PEPs, including determining Source of Wealth and Source of Funds;
- Obtaining Senior Management Approval; and
- Enhanced on-going monitoring measures.

C. Reliance on Third Parties in relation to PEPs

Firms should also have appropriate policies and procedures in place in instances where the firm is relying upon a Third Party to perform the due diligence measures on customers and beneficial owners. The policies and procedures should set out the steps to be taken by the firm when the Third Party has identified a new PEP relationship.

Firms should note that they cannot rely on the Third Party to perform the EDD measures or provide Senior Management approval. However, the Third Party may provide assistance to the firm in gathering the necessary documentation or information to establish the source of wealth and source of funds.

See also Section 5.2.6 of the Guidelines regarding reliance on Third Parties.

5.6.2 Senior Management Approval of PEPs

Section 37(4)(a) of the CJA 2010 requires firms to ensure that approval is obtained from Senior Management before a business relationship is established or continued with a PEP.

Firms should put appropriate policies and procedures in place clearly setting out;

- The reporting and escalation of PEP relationships to Senior Management;
- The timelines for obtaining Senior Management sign-off; and
- The level of seniority required in order to approve a PEP relationship.

Firms should determine the level of seniority for sign-off by the level of increased ML/TF risk associated with the business relationship. The Senior Manager approving a PEP business relationship should have sufficient seniority and oversight to take informed decisions on issues that directly impact the firm's ML/TF risk profile.

When considering whether to approve a PEP relationship, firms should take into consideration;

- The level of ML/TF risk that the firm would be exposed to if it entered into that business relationship; and
- What resources the firm would require in order to mitigate the risk effectively.

Where firms are considering whether to enter into, or to continue to carry on a business relationship with a PEP, they should ensure that:

- the matter is discussed at senior management level;
- the corresponding ML/TF risks are acknowledged; and
- the decision reached is documented.

5.6.3 Source of Wealth / Source of Funds of PEPs

Section 37(4)(b) of the CJA 2010 requires firms determine the source of wealth and funds for the following transactions in relation to PEPs

"*(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 [firm] assists the customer to carry out."

Firms should take adequate measures to establish the source of wealth and source of funds which are to be used in the business relationship in order to satisfy themselves that they do not handle the proceeds of corruption or other criminal activity.

The measures which firms should take to establish a PEP's source of wealth and source of funds will depend on the degree of risk associated with the business relationship. Firms should verify the source of wealth and the source of funds based on reliable and independent data, documents or information where the risk associated with the PEP relationship is particularly high.

When determining the source of wealth and source of funds, the firms should, at least consider:

- The activities that have generated the total net worth of the customer (that is, the activities that produced the customer's funds and property); and
- The origin and the means of transfer for funds that are involved in the transaction (for example, their occupation, business activities, proceeds of sale, corporate dividends).

5.6.4 Enhanced On-going monitoring of PEPs

Section 37(4)(c) of the CJA 2010 requires firms to apply enhanced monitoring of the business relationship with PEPs.

This is in addition to the monitoring required under Section 35(3) of the CJA 2010 in order to identify any unusual transactions by PEPs.

Firms should regularly review the information they hold on PEP customers and their beneficial owners (where relevant) to ensure that any new or emerging information that could affect the risk assessment is identified in a timely fashion. The frequency of ongoing monitoring should be determined by the firm commensurate with the higher risk associated with the PEP relationship.

5.7 EDD in Relation to Correspondent Relationships

Section 38 of the CJA 2010 sets out the EDD requirements firms are required to undertake in relation to establishing new correspondent relationships, where the respondent institution is situated outside of the EU.

The 2018 amendments to the CJA 2010 broadens the concept of correspondent banking relationships to correspondent relationships. Correspondent relationships include correspondent relationships between credit institutions and between credit and financial institutions, including relationships established for securities transactions or funds transfers.

For the purposes of this section, correspondent relationships are the provision of a current or other liability account and related services by an Irish based credit or financial institution (the "correspondent institution") to another institution situated in a place other

than a Member State (the 'respondent institution') to meet its cash, clearing, liquidity management and short-term borrowing or investment needs.

Firms may also find this useful in respect of correspondent relationships within Member States, as warranted by the correspondent institutions own risk assessment.

The correspondent institution processes and executes transactions on behalf of customers of the respondent institution. However, the correspondent institution often does not have a direct relationship with the customer of the respondent institution, as they are the customer of the respondent institution. Correspondent institutions face a heightened level of ML/TF risk due to the logistics of the correspondent relationship.

A correspondent institution's policies and procedures should adequately address all of its obligations as set out under Section 38.

5.7.1 Risk Assessment of Correspondent Relationships –

Section 38 (a) to (c) of the CJA 2010 provides that the correspondent institution shall not enter into a correspondent relationship unless, prior to commencing the relationship, the correspondent institution:

(a) "has gathered sufficient information about the respondent institution to understand fully the nature of the business of the respondent institution,
(b) is satisfied on reasonable grounds, based on publicly available information, that the reputation of the respondent institution, and the quality of supervision or monitoring of the operation of the respondent institution in the place, are sound,
(c) is satisfied on reasonable grounds, having assessed the anti-money laundering and anti-terrorist financing controls applied by the respondent institution, that those controls are sound."

Correspondent institutions should perform risk assessments of all correspondent relationships. The risk assessment of the respondent institution should take into account a number of risk factors including but not limited to:

- The jurisdiction in which the respondent institution is incorporated in and the AML / CFT regulatory regime which the respondent institution is subject to;
- The ownership and management structure of the respondent institution, including any role performed by or influenced by beneficial owners or PEPs;
- The business purpose of the relationship;
- Operations and transaction volumes;
- The correspondent institution's customer base;
- The quality of the respondent institution's AML/CFT systems and controls; and
- Any negative information known about the respondent institution or its affiliates.

The conclusion of the risk assessment should determine the appropriate risk rating attaching to a particular respondent institution and drive the level of EDD applied and the frequency of relationship review.

5.7.2 Senior Management Approval of Respondent Relationships

Section 38 (d) of the CJA 2010 requires the senior management of the correspondent institution to approve correspondent relationships

The correspondent institution should be able to evidence that appropriate consideration has been given to maintain or exit a particular correspondent relationship. Correspondent institutions should document and retain all approvals by Senior Management for all new correspondent relationships and reviews of existing correspondent relationships (see 5.6.2 in relation to senior management approval for PEPs).

5.7.3 Responsibilities of each Party regarding Respondent Relationships

Section 38 (e) of the CJA 2010 requires the correspondent institution to document …

"*the responsibilities of each institution in applying anti-money laundering and anti-terrorist financing controls to customers in the conduct of the correspondent relationship and, in*

particular—

(i) the responsibilities of the institution arising under this Part, and
(ii) any responsibilities of the respondent institution arising under requirements equivalent to those specified in the AMLD4."

Correspondent institutions should have policies and procedures in place which ensure that the respective responsibilities of the correspondent institution and respondent institution in applying AML/CFT controls is documented, prior to the establishment of the correspondent relationship.

5.7.4 Correspondent Relationships in connection with Shell Banks

Correspondent institutions should have policies and procedures in place which ensure that:

- The correspondent institution does not enter into a correspondent relationship with a respondent institution that is a shell bank; or
- The respondent institution, with whom it has entered into a correspondent relationship, does not have a relationship with a shell bank.

5.7.5 Liaison with Respondent Institutions

Correspondent institutions should appoint a member of Senior Management, the Compliance Officer, or the MLRO to:

- Liaise with and discuss any potential AML/CFT issues with the respondent institution;
- Obtain the necessary CDD information; and
- If necessary, conduct an onsite visit to the respondent institution's offices as part of the correspondent institution's CDD measures.

5.7.6 Screening of Respondent Institutions

Correspondent institutions should regularly screen respondent institutions, their controllers, beneficial owners and any other connected persons, to identify for PEP connections or persons, or affiliated or subsidiary entities subject to financial sanctions.

5.7.7 Information Requirements for Correspondent Relationships

Correspondent institutions should ensure that sufficient information is obtained on all respondent relationships and particularly for any respondent relationship where EDD is applied. Information obtained for a respondent institution may include, but is not limited to, the following:

- Jurisdiction where the respondent institution is located (EU v non-EU member state);
- Ownership/control structure (e.g. publicly listed entity);
- Structure and experience of the Board of Directors/Executive management;
- Information from respondent's web-site and respondent's latest annual return;
- Reputation of Respondent institution and regulatory status;
- Respondent's AML/CFT controls.

5.7.8 Ongoing monitoring of Correspondent Relationships

The respondent institution is in effect a customer of the correspondent institution and as such, as required under Section 35 of the CJA 2010, the correspondent institution must apply on-going monitoring measures pursuant to the level of ML/TF risk presented by the correspondent relationship.

Correspondent institutions should perform periodic reviews on a regular basis, with higher risk correspondent relationships reviewed more frequently, but at least on an annual basis. In addition, the following non-transactional trigger events should be considered:

- Material change in ownership and/or management structure;
- Re-classification of the jurisdiction where the respondent institution is located;
- Identification of a PEP relationship;
- Identification of adverse media on the respondent institution.
- Correspondent institutions should conduct transaction monitoring on the respondent institution and the associated underlying transactions.

5.7.9 Unusual Transactions in Correspondent Relationships

Correspondent institutions should put in place adequate policies and procedures to detect unusual transactions or patterns of transactions. The following examples are illustrative of possible suspicious transactional respondent activity:

- Transactions involving higher risk countries vulnerable to Money Laundering and/or Terrorist Financing;
- Transactions with those respondent institutions already identify as higher risk;
- Large (volume or value) transaction activity involving monetary instruments (e.g. money orders, bank drafts), especially involving instruments that are sequentially numbered;
- Transaction activity that appears unusual in the context of the relationship with the respondent institution;
- Transactions involving shell corporations;
- Transactions that are larger or smaller than the correspondent institution would normally expect based on its knowledge of the respondent institution, the business relationship and the risk profile of the respondent institution.

5.8 EDD in relation to Complex or Unusual Transactions

36A. (1) of the CJA 2010 requires firms to examine the background and purpose of all complex or unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose.

36A. (2) of the CJA 2010 requires firms to increase the degree and nature of monitoring of a business relationship in order to determine whether transactions referred to in subsection (1) appear suspicious.

Firms should put in place adequate policies and procedures to identify unusual transactions or patterns of transactions. Examples may include transactions or patterns of transactions that are:

- Larger than the firm would normally expect based on its knowledge of the customer, the business relationship or the category to which the customer belongs;
- Of an unusual or unexpected pattern compared with the customer's normal activity or the pattern of transactions associated with similar customers, products or services; or
- Very complex compared with other similar transactions associated with similar customer types, products, or services; and the firm is not aware of an economic rationale or lawful purpose or doubts the veracity of the information it has been given.

Where firms detect unusual transactions or patterns of transactions, they should apply EDD measures sufficient to help the firm determine whether these transactions give rise to suspicion. Such EDD measures should at least include:

- Taking reasonable and adequate measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds or finding out more about the customer's business to ascertain the likelihood of the customer making such transactions; and

- Monitoring the business relationship and subsequent transactions more frequently and with greater attention to detail. A firm may decide to monitor individual transactions where this is commensurate to the risk it has identified.

See also Section 5.3.1 of the Guidelines regarding the monitoring of large or unusual transactions.

5.9 EDD in relation to High-Risk Third Countries and other High-Risk Situations

Section 38A. (1) of the CJA 2010 requires firms to apply measures, including enhanced monitoring of the business relationship, to manage and mitigate the ML/TF risk when dealing with a customer established or residing in a high-risk third country.

Section 39.(1) of the CJA 2010 requires firms to apply measures to manage and mitigate the ML/TF risk to a business relationship or transaction that presents a higher degree of risk.

When dealing with customers established or residing in a high-risk third country and in all other high-risk situations, firms should take an informed decision about which EDD measures are appropriate for each high-risk situation.

Firms should apply appropriate EDD, including the extent of the additional information sought and of the increased monitoring carried out, based on the reason(s) why the transaction or a business relationship was classified as high risk.

Firms should decide what EDD measures they deem appropriate. For example, in certain high-risk situations a firm may deem it appropriate to focus on enhanced ongoing monitoring during the course of the business relationship as opposed to applying other or additional EDD measures. Below is a non-exhaustive list of EDD measures which a firm may decide to take in order to mitigate the ML/TF risk.

- Seeking information about the customer's or beneficial owner's identity, or the customer's ownership and control structure, in order to be satisfied that the risk associated with the relationship is well understood. This may include obtaining and assessing information about the customer's or beneficial owner's reputation and assessing any negative allegations against the customer or beneficial owner. Examples include:

- Information about family members and close business partners;
- Information about the customer's or beneficial owner's past and present business activities; and
- Adverse media searches;

- Seeking information about the intended nature of the business relationship to ascertain that the nature and purpose of the business relationship is legitimate and to help firms obtain a more complete customer risk profile. This may include obtaining information on:
  - The number, size and frequency of transactions that are likely to pass through the account, to enable the firm to spot deviations that might give rise to suspicion (in some cases, requesting evidence may be appropriate);
  - Why the customer is looking for a specific product or service, in particular where it is unclear why the customer's needs cannot be met better in another way, or in a different jurisdiction;
  - The destination of funds;
  - The nature of the customer's or beneficial owner's business, to enable the firm to better understand the likely nature of the business relationship;

- Increasing the quality of information obtained for CDD purposes to confirm the customer's or beneficial owner's identity including either:
  - Requiring the first payment to be carried out through an account verifiably in the customer's name with a bank subject to CDD standards that are not less robust than those set out in Chapter II of 4AMLD; or
  - Establishing that the customer's wealth and the funds that are used in the business relationship are not the proceeds of criminal activity and that the source of wealth and source of funds are consistent with the firm's knowledge of the customer and the nature of the business relationship. In some cases, where the risk associated with the relationship is particularly high, verifying the source of wealth and the source of funds may be the only adequate risk mitigation tool. The source of funds or source of wealth may be verified, inter alia, by reference to VAT and income tax returns, copies of audited accounts, pay slips, property registration or independent media reports;

- Increasing the frequency of reviews to be satisfied that the firm continues to be able to manage the risk associated with the individual business relationship, or conclude that the relationship no longer corresponds to the firm's risk appetite or to help identify any transactions that require further review. Examples include:

- Increasing the frequency of reviews of the business relationship to ascertain whether the customer's risk profile has changed and whether the risk remains manageable;

- Obtaining the approval of Senior Management to commence or continue the business relationship to ensure that Senior Management are aware of the risk their firm is exposed to and can take an informed decision about the extent to which the firm is equipped to manage that risk;

- Reviewing the business relationship on a more regular basis to ensure any changes to the customer's risk profile are identified, assessed and where necessary, acted upon; or

- Conducting more frequent or in-depth transaction monitoring to identify any unusual or unexpected transactions that might give rise to suspicion of ML/TF. This may include establishing the destination of funds or ascertaining the reason for certain transactions.

6. Governance

6.1 Governance

The attitude and culture embedded within a firm is of critical importance in the fight against money laundering and terrorist financing. A positive culture recognises the important public interest aspect of a firm's role in the fight against ML/TF. This includes having an approach to AML/CFT compliance that considers the legislative obligations as only the starting point. Firms should engage with the Central Bank in a positive, transparent way and should be proactive in bringing matters to the attention of the Central Bank.

Insufficient or absent AML/CFT risk management, governance, policies, controls and procedures exposes firms to significant risks, including not only financial but also reputational, operational and compliance risks.

Firms should ensure that the ML/TF risk management measures adopted by the firm are risk-based and proportionate, informed by the firm's Business Wide Risk Assessment of its ML/TF risk exposure and in compliance with the CJA 2010.

6.2 Role and Responsibilities of Senior Management

The Senior Management of firms, including the Board of Directors (the 'Board') (or its equivalent), have responsibility for managing the identified ML/TF risks by demonstrating active engagement in the firms' approach to effectively mitigating such risks.

Firms should put appropriate AML/CFT structures in place that are proportionate and reflect the nature, scale and complexities of the firm's activities.

Firms should ensure that the AML/CFT role and responsibilities of Senior Management is clearly defined and documented. Similarly the roles and responsibilities of other relevant key functions within the firm, such as the MLRO, the Risk Officer (where relevant), the Compliance Officer (where relevant) and internal audit (where relevant), should also be clearly defined and documented with regard to AML/CFT activities within the firm.

6.2.1 Governance and Oversight

Firms should ensure that there is appropriate governance and oversight with regard to its compliance with obligations under the CJA 2010. For example, firms should ensure for:

- Business Wide Risk Assessments:
  - Senior Management has reviewed and approved the methodology used for undertaking the firm's Business Wide Risk Assessment.
  - Senior Management has reviewed and approved the firm's Business Wide Risk Assessment at least on an annual basis to ensure that it is aware of the ML/TF risks facing the firm and that the corresponding AML/CFT measures which the firm has in place are appropriate for the level of ML/TF risk identified.

- Policies and Procedures
  - Senior Management has reviewed and approved all policies and procedures, and material updates to same.

- Reporting Lines:
  - Appropriate reporting lines are in place to facilitate the escalation of AML/CFT issues from the MLRO for discussion at Senior Management level.

- Senior Management Meetings:
  - AML/CFT issues appear as an agenda item at regular intervals at Senior Management meeting(s) and that the corresponding minutes reflect the level of discussion and outcomes, which took place concerning any Management Information (MI) provided by the MLRO or any particular AML/CFT/FS issues requiring discussion by the Senior Management.
  - The MLRO delivers a report to Senior Management at least on an annual basis and that a detailed discussion on its content takes place with a corresponding minute to reflect the level of discussion.

- AML/CFT Resourcing
  - The firm's AML/CFT function is adequately resourced (both in terms of staff and systems) commensurate with the level of ML/TF risk faced by the firm.
  - Reviews are undertaken on a regular and timely basis to consider whether the firm has the appropriate staff numbers, the correct skill-set and whether staff have access to adequate systems and other resources to effectively perform their role as it relates to AML/CFT issues.

Firms should ensure that appropriate evidence of discussions at Senior Management meetings and/or approvals concerning AML/CFT issues are recorded and retained in accordance with the firm's record retention policy.

Firms should also ensure that appropriate evidence is retained in accordance with its record retention policy regarding the firm's obligations in relation to:

- Politically Exposed Persons (PEPs):
  - Retention of Senior Management approvals of all new PEP relationships which a firm enters into or where the PEP status of a customer subsequently changes during the course of a relationship with a firm as required under Section 37.

- Correspondent Relationships:
  - Retention of senior management approvals of all new correspondent relationships, or the continuance of a correspondent relationship as required under Section 38. Firms should also be in a position to evidence that appropriate consideration has been given as to whether to maintain or exit a correspondent relationship.

6.3 Roles and Responsibilities of the MLRO

Firms should ensure that the person appointed as MLRO:

- Has sufficient and appropriate AML/CFT knowledge and expertise;
- Has the autonomy, authority and influence within the firm to allow them to discharge their duties effectively;
- Is capable of providing effective challenge within the firm on AML/CFT matters when necessary;
- Has the capabilities, capacity and experience to oversee the identification and assessment of suspicious transactions and to report/liaise with the relevant authorities where necessary in relation to such transactions;
- Keeps up to date with current and emerging ML/TF trends and issues in the industry and understands how such issues may impact the firm;
- Has access to adequate resources and information to allow them to discharge their duties effectively; and
- Is readily accessible to staff on AML/CFT matters.

Where an MLRO has not been appointed by the firm, the Central Bank may, under Section 54 (8), direct the firm to do so.

6.3.1 MLRO Reporting to Senior Management

Firms should ensure that there is effective reporting and escalation on AML/CFT matters by the MLRO to Senior Management. Such reporting should include at least:

- The production of regular and timely Management Information ("MI") to the Senior Management regarding the AML/CFT activities at the firm. Such MI should be sufficiently detailed to ensure that Senior Management is able to make timely, informed and appropriate decisions on AML/CFT matters;
- The production of a report ("MLRO Report") on the firm's AML/CFT activities. The MLRO Report should , inter alia;
    - Be produced by the MLRO at least on an annual basis;
    - Be presented by the MLRO to Senior Management in a timely manner;
    - Be proportionate to the nature, scale and complexities of the firm's activities;
    - Provide comment upon the effectiveness of the firm's AML/CFT systems and controls; and
    - Include recommendations, as appropriate, for improvement in the management of the firm's ML/TF risk.

6.4 Three Lines of Defence Model

Where firms have implemented a "three lines of defence" model in order to manage and oversee a firm's ML/TF risk[17], they should ensure that:

- There is adequate and effective co-ordination between the front line business unit, risk, compliance and internal audit, or equivalent within the firm, to ensure robust and well-structured oversight, as well as effective co-ordination of resources to manage overlap in areas of review;
- The second and third line work plans are prepared using a risk-based approach, with all risks/controls, including AML/CFT, reviewed on a periodic basis;
- Relevant Senior Management and governance committees are involved in the planning of the scheduled reviews and in the closing of findings;
- Testing for specific AML/CFT controls, as well as the overall framework, should be conducted on a regular basis commensurate with the risk;
- Effective systems should be used to track and monitor issues to resolution; and
- Risk, compliance and internal audit units are independent and adequately resourced with staff knowledgeable of AML/CFT.

6.5 External Audit

When selecting external auditors, firms should include consideration of the potential candidate's cognisance of and ability to assess AML/CFT requirements as part of the selection process.

6.6 Policies and Procedures

Section 54 of the CJA 2010 sets out the obligations of firms in respect of the adoption of policies and procedures, the areas to be covered and the responsibilities of Senior Management in order to prevent and detect the commission of Money Laundering and Terrorist Financing.

When developing AML/CFT policies and procedures, firms should inter alia:

- Maintain a detailed documented suite of AML/CFT policies, which are:
  - supplemented by guidance and supporting procedures;
  - accurately reflect operational practices; and
  - fully demonstrate consideration of and compliance with all legal and regulatory requirements;
- Have a clearly defined process in place for the formal review at least annually of the policies and procedures at appropriate levels, with approval where changes are material;

[17] Where this is warranted based upon the nature, scale and complexity of the firm's business

- Review and update policies and procedures in a timely manner in response to events or emerging risks[18]; and ensure that such updates are communicated to relevant staff on a timely basis;
- Ensure that policies and procedures are readily available to all staff and are fully implemented and adhered to by all staff;
- Ensure that policies and procedures are subject to review and testing; and
- Ensure that Senior Management have reviewed and approved all policies and any material updates to same

6.6.1 Group wide policies and procedures

Section 57 of the CJA 2010 sets out the obligation to implement group-wide policies and procedures where a firm is part of a group.

Section 57 also applies to those firms who operate a branch, majority-owned subsidiary or establishment outside of the State.

Where applicable, firms should ensure that they comply with their obligations and the ESA's final draft regulatory technical standards (RTS) relating to group-wide policies and procedures in third countries.

Such RTS specify how firms should manage ML/TF risks at group level[19] where they have branches or majority-owned subsidiaries based outside the EEA whose laws do not permit the application of group-wide policies and procedures on anti-money laundering and countering the financing of terrorism.

[18] Firms should use of version controls for updates to policies and procedures

[19] https://www.eba.europa.eu/documents/10180/2054088/Joint+draft+RTS+on+the+implementation+of+group+wide+AMLCFT+policies+in+third+countries+%28JC+2017+25%29.pdf

7. Reporting of Suspicious Transactions

7.1 Requirement to Report

Suspicious Transactions Reports (STRs) play a pivotal role in the fight against money laundering and terrorist financing. Information provided on STRs assist An Garda Síochána and the Revenue Commissioners (the authorities) in their investigations, resulting in the disruption of criminal and terrorist activities, and can ultimately result in prosecution and imprisonment. STRs also provide authorities with valuable market intelligence on trends and typologies.

Section 42 of the CJA 2010, provides that:

"A firm who knows, suspects or has reasonable grounds to suspect on the basis of information obtained in the course of carrying on business as a firm, that another person has been or is engaged in an offence of money laundering or terrorist financing, shall report to FIU Ireland and the Revenue Commissioners that knowledge or suspicion or those reasonable grounds."

7.2 Identifying suspicious transactions

When assessing potential suspicious transactions, firms should consider attempted transactions, as well as completed transactions.

In addition, firms should note that there is no minimum monetary threshold for reporting and no amount should be considered too low for suspicion. This is particularly important when considering potential terrorist financing transactions which often involve very small amounts of money.

Firms should consider their specific products, services and customers when making a determination of suspicion, as what might be considered suspicious for one product, service or customer may not be for another. The following is a non-exhaustive list of examples of what might raise suspicions:

- Transactions or a series of transactions that appear to be unnecessarily complex, making it difficult to identify the beneficial owner or that do not appear to make economic sense;

- Transaction activities (in terms of both amount and volume) that do not appear to be in line with the expected level of activity for the customer and/or are inconsistent with the customer's previous activity;

- Transactions in excess of a customer's stated income;
- Large unexplained cash lodgements;
- Loan repayments inconsistent with a customer's stated income, or early repayment of a loan followed by an application for another loan of similar amount;
- Requests for third party payments. For example, this might include a third party making a payment into a customer's account to pay off a loan, to fund an investment or policy, or to fund a savings account;
- Transactions involving high-risk jurisdictions*, particularly in circumstances where there is no obvious basis or rationale for doing so;
- Refusal to provide customer due diligence documentation or providing what appears to be forged documentation.

*The 2018 Act has removed the obligation on designated persons to automatically report any service or transaction connected with a high-risk jurisdiction to An Garda Síochána and the Revenue Commissioners.

7.3 Timing of Suspicious Transaction Reports ('STRs')

Section 42(2) of the CJA 2010 requires firms to make an STR …"*as soon as practicable* …"

As soon as practicable means when the firm suspects or has reasonable grounds to suspect money laundering or terrorist financing before the execution of a transaction or at the same time as the execution of a transaction. In such cases, the firm should immediately file an STR.

The firm may need to conduct further analysis and assessment in order to make its determination. Any such analysis and assessment should be conducted without delay, however as soon as the firm has established a suspicion or reasonable grounds, it should immediately file an STR.

7.4 Internal Reporting of Suspicious Transactions

Under Section 44 of the CJA 2010, firms may allow for the reporting of STRs by way of an internal reporting procedure

In relation to the identification and escalation of internal reports, firms should ensure that:

- Operational procedures for staff on filing an internal report ('internal reporting procedures') are adequately documented and that the internal reporting procedure

captures all suspicious transaction reporting requirements as prescribed under the CJA 2010. For example the internal reporting procedures should include at least:
  - All required steps for the reporting of suspicions from staff to the MLRO, or any other person(s) charged under the firm's internal reporting process with investigating suspicions, and from the MLRO to the authorities;
  - The timeframes for escalation of suspicious transactions from when a staff member first identifies a suspicious transaction to when it is raised to the MLRO;
  - Formal acknowledgement by the firm's MLRO of suspicions raised internally by staff; and
  - Information with regard to 'Tipping-off' so as to ensure that staff are aware of their obligations under the CJA 2010, the penalties for the offence of Tipping Off and that they exercise caution after the filing of an STR[20];

- AML/CFT training provided to staff includes details on the firm's internal reporting procedure as well as details on the reporting of suspicions to the authorities;

- There are no discrepancies between internal reporting procedures as documented and operational practices. For example, where the firm's internal reporting procedure states that suspicions are to be escalated using an internal reporting form then the raising of suspicions should not be conducted verbally;

- Where a firm utilises a transaction monitoring system (TMS), there is regular review of the correlation between alerts generated from the TMS and the reporting of suspicious transactions to the authorities;

- Where a suspicion has been escalated for further assessment and review, the firm's records provide sufficient detail of the assessment and adjudication giving rise to the decision to discount the suspicion or to make a report to the authorities. For example:
  - The circumstances that gave rise to the suspicion;
  - The assessment or additional analysis that took place; and
  - The rationale for discounting the suspicion or the basis for making a report to the authorities.

- Sufficient information is retained in order to record the reported suspicion, and support the firm's determination of whether to discount the suspicion, or to proceed and file the STR with the authorities.

7.5 Making Suspicious Transaction Reports

Section 42 of the CJA 2010, provides that reports in relation to money laundering and terrorist financing suspicions should be made to FIU Ireland and to the Revenue Commissioners.

[20] Please also see section 7.7 on 'Tipping-off' below.

STRs submitted to FIU Ireland[21] should be made via the goAML application[22]. Firms should ensure that they are registered with goAML as STRs cannot be submitted via goAML unless the firm has previously registered.

The Revenue Commissioners will accept a printed copy of the STR submitted on goAML which should be posted to the relevant address.

Firms should ensure that STRs submitted to the authorities are sufficiently detailed to assist the authorities in their investigations. Examples of a poor quality STR that may not assist authorities include instances where:

- customer details are not given;
- out of date information is provided;
- details on dates and amounts of transactions are not included; or
- reasons for suspicion are not outlined.

7.6 Tipping Off

Section 49 of the CJA 2010 provides for two separate but related offences being where the firm (including a representative of a firm) knows or suspects on the basis of information learned during the course of carrying on business as a firm:

- that a report has been, or is required to be, made under Chapter 4 of the CJA 2010, the firm shall not make any disclosure that would be likely to prejudice an investigation that may be conducted following the making of a report under Chapter 4; and
- that an investigation is being contemplated or is being carried out into whether an offence of money laundering or terrorist financing has been committed, the firm shall not make any disclosure that is likely to prejudice the investigation.

Sections 50 to 53 of the CJA 2010 provides for a number of defences for an offence under Section 49 in relation to a disclosure.

[21] which is part of the Garda National Economic Crime Bureau

[22] The goAML application is an electronic application which provides FIU Ireland with a central reception point for receiving, processing and analysing STRs

Where a firm or a representative of the firm[23] requests additional information from a customer in relation to a transaction, activity or service, which would not be in keeping with the firm's expectation for that customer, then as long as such requests have been conducted in a careful and considered manner they should not give rise to an offence under Section 49.

Firms should include details on the offence of 'Tipping-off', the need for staff to exercise caution and the penalties for the offence within the firm's AML/CFT policies and procedures.

Firms should include as part of their AML/CFT training to all staff, advice around the treatment of unusual transactions and the additional due diligence measures, which should be taken by staff without committing the offence of 'Tipping-off'.

[23] A representative of a firm includes or any person acting, or purporting to act on behalf of the firm including any agent, employee, partner, director or other officer of the firm ("representative of the firm")

8. Training

8.1 AML/CFT Training

Section 54(6) of the CJA 2010 requires firms to ensure that

"…persons involved in the conduct of the designated person's business are—

(a) instructed on the law relating to money laundering and terrorist financing, and

(b) provided with ongoing training on identifying a transaction or other activity that may be related to money laundering or terrorist financing, and on how to proceed once such a transaction or activity is identified."

Having well trained staff who are alert to ML/TF risks is a critically important control for firms in the detection and prevention of money laundering and terrorist financing.

Firms should ensure that all employees, directors and agents are aware of the risks of money laundering and terrorist financing relevant to the business, the applicable legislation and their obligations and responsibilities under the legislation.

Firms should provide appropriate and sufficient training which is tailored to the nature, scale and complexity of the firm and which is proportionate to the level of ML/TF risk faced by the firm.

Firms should ensure that all employees, directors and agents:

- Understand the firm's AML/CFT policy, which should be drafted in clear and unambiguous language;
- Are trained in the firm's procedures in order that they can recognise and address potential instances of money laundering or terrorist financing;
- Are made aware of the firm's internal reporting procedures in respect of STRs and the identity and responsibilities of the firm's MLRO; and
- Understand their own individual obligations under the CJA 2010 as well as those of the firm.

8.2 Role Specific and Tailored Training

Firms should provide AML/CFT training which is specific to the role carried out by the member of staff. For example, front line staff who interact with customers and perform

transactions and services should be provided with AML/CFT training relevant to the performance of that role.

Firms should also provide enhanced AML/CFT training tailored to the specific needs of staff who perform key AML/CFT and FS roles within the firm, for example the firm's MLRO or Senior Management responsible for AML/CFT oversight.

Firms should provide staff with ongoing training, especially where a staff member changes role and they may encounter different ML/TF risks to that of their previous role.

8.3 Frequency of training

Firms should ensure that AML/CFT training is provided to all new recruits upon joining the firm in a timely manner and to all staff at least on an annual basis thereafter.

Staff in customer facing roles should receive AML/CFT training prior to interacting with customers.

Firms should consider the outcomes of their own Business Wide Risk Assessments and whether the frequency and content of AML/CFT training provided is adequate for levels of ML/TF risks faced by the firm.

Firms exposed to a higher level of ML/TF risk or who have a greater exposure to constantly evolving ML/TF risks should provide training at more frequent and regular intervals if necessary.

8.4 Training Governance

Firms should ensure Senior Management's oversight and responsibility for:

- The firm's compliance with its requirements in respect of staff AML/CFT training under the CJA 2010;
- The establishment and maintenance of effective training arrangements which reflect the firm's Risk Based Approach to AML/CFT; and
- Ensuring that training content is reviewed and updated on a regular basis to ensure that it remains relevant to the firm and providing assurance to this effect.

8.5 Training of Outsource Service Providers

Where firms have outsourced an AML/CFT function, they should ensure that all staff at the outsource service provider performing AML/CFT activities on behalf of the firm have been appropriately trained on:

- The ML/TF risks relevant to the firm;
- The applicable AML/CFT legislation; and
- Their obligations and responsibilities under the applicable AML/CFT legislation.

Firms should ensure that relevant staff in the outsourced entity are aware of the firm's internal reporting procedures in respect of Suspicious Transaction Reporting (STR) and the identity and responsibilities of the firm's MLRO.

8.6 Training Channels

Firms should decide the most appropriate method or methods they wish to use in order to provide AML/CFT training to staff, senior management and agents. For example, firms may decide to use a number of different channels such as online or e-learning modules, classroom training or video presentations in order to fulfil their obligations under the CJA 2010.

8.7 Training Records

Firms should keep a comprehensive record of:

- all staff, senior management and agents who have received AML/CFT training;
- the type of AML/CFT training provided; and
- the date on which the AML/CFT training was provided.

8.8 Training Assessment

Firms should ensure that the AML/CFT training provided includes an assessment or examination at the end of the training session, which should be passed by all participants in order for the AML/CFT training to be recorded as completed.

8.7 Management Information on Training

Firms should ensure that senior management is provided with timely MI including, information on training, training completion and training pass rates.

Firms should ensure that senior management take appropriate remediation action where there are concerns in relation to training issues. Metrics in relation to the firm's training should be circulated to relevant senior management for Management Information purposes.

9. Record Keeping

9.1 Obligation to retain records

Adequate record keeping is critically important to the preservation of the audit trail which in turn can assist with any investigation into money laundering or terrorist financing. Effective record keeping allows firms to demonstrate to the Central Bank the steps which they have taken to comply with their obligations under the CJA 2010.

Firms should ensure that their AML/CFT policy and procedures contain sufficient detail of their record keeping obligations under the CJA 2010. The adequacy and detail of records kept by a firm should be reflective of the nature, scale and complexity of the firm.

Firms should also ensure that all staff including agents, outsourced service providers, and any third parties relied upon for CDD purposes adhere to the firm's procedures on record keeping.

9.2 Records a firm should retain

Firms are required to retain records in relation to the following:

- Business-wide Risk Assessments (under Section 30A. of the CJA 2010);
- Customer Information (under Section 55 of the CJA 2010); and
- Transactions (under Section 55 of the CJA 2010).

Firms should also retain records inter alia in relation to the following:

- Internal and external Suspicious Transaction Reports;
- Investigations and suspicious transaction reports;
- Reliance on Third Parties to undertake CDD;
- Minutes of Senior Management meetings;
- Training; and
- Ongoing monitoring.

9.2 1 Business-wide Risk Assessments

Firms should document and record their Business-wide Risk Assessments, as well as any changes made to Business-wide Risk Assessments as part of a firm's review and monitoring process, to ensure that they can demonstrate that their Business Wide Risk Assessments and associated risk management measures are adequate.

9.2.2 Customer Information

Firms should keep adequate records, including:

- All documentation and information obtained for the purposes of identifying and verifying a customer, person(s) authorised to act on behalf of the customer and any beneficial owners;
- All customer risk assessments;
- Copies of all additional documentation and information obtained, where EDD measures have been applied to a customer of the firm;
- Copies of any sample testing of CDD files, which the firm has undertaken as part of its assurance testing process; and
- Copies of documentation and information obtained as part of the firm's ongoing monitoring process.

9.2.3 Transactions

Firms should be cognisant of the importance of the obligations under Section 55 to retain copies of all transactions carried out for or on behalf of a customer during the business relationship with the firm for their own internal audit purposes as well as any possible investigations by law enforcement.

9.2.4 Internal and External Suspicious Transaction Reports

Firms should keep sufficient records in relation to suspicious transactions, including:

- The circumstances that gave rise to the suspicion;
- Any additional monitoring/assessment that was undertaken;
- Whether the suspicion was reported/not reported, and
- Rationale for reporting or not reporting to FIU Ireland and the Revenue Commissioners.

Firms should retain copies of all documentation and information used as part of any internal assessment into a customer following on from the filing of an internal STR by a staff member of the firm.

Firms should retain records to provide evidence and the justification behind their decision whether or not to file an STR with FIU Ireland and the Revenue Commissioners. In this regard, firms should also retain copies of the supporting documentation and information which assisted them in reaching their decision.

9.2.5 Reliance on Third Parties to Undertake CDD

Firms should ensure, when placing reliance on third parties to undertake CDD, that there is signed agreement in place between the firm and the third party provider with clear contractual terms in respect of the obligations of the third party to obtain and maintain the necessary records, and to provide the firm with CDD documentation or information as requested.

9.2.6 Minutes of Senior Management Meetings

Firms should retain all records of discussions and decisions made at senior management level in relation to:

- How the requirements of the CJA 2010 were assessed and implemented; and
- Any AML/CFT issues as they arise on an on-going basis.

9.2.7 Training

Firms should retain records of all AML/CFT training provided to staff during a given year. Information should include:

- The dates on which AML/CFT training was provided to staff;
- Attendance and sign-in sheets (where relevant) of who received the AML/CFT training;
- The nature and content of the AML/CFT training provided; and
- Results of the assessment and examination at the end of the training session.

9.2.8 Ongoing Monitoring

Firms should retain records to verify and evidence the on-going monitoring conducted by the firm, including the monitoring of transactions, the results of such monitoring and decisions taken on foot of on-going monitoring.

9.3 Assurance Testing of Record Retention

Firms should perform assurance testing at appropriate intervals to ensure the quality and legibility of documents held and that records are being retained and/or destroyed in line with the firms' policy and the relevant legislative provisions.

Section 55(7A) of the CJA 2010 provides that

"*the records may be kept outside the State provided that the firm ensures that those records are produced in the State to—*

(a) a member of the Garda Síochána,

(b) an authorised officer appointed under Section 72,

(c) a relevant authorised officer within the meaning of Section 103, or

(d) a person to whom the designated person is required to produce such records in relation to his or her business, trade or profession,

as soon as practicable after the records concerned are requested, or

where the obligation to produce the records arises under an order of a court made under Section 63 of the Criminal Justice Act 1994, within the period which applies to such production under the court order concerned"

Where identification records are held outside of the State, it is the responsibility of the firm to ensure that the records available meet the necessary requirements under the CJA 2010.

Firms should be aware that no secrecy or data protection legislation should restrict access to the records either by the firm on request, or by An Garda Síochána under court order or relevant mutual assistance procedures. If it is found that such restrictions exist, copies of the underlying records of identity should, wherever possible, be sought and retained within the State.

Firms should take account of the scope of AML/CFT legislation in other countries, and should ensure that records kept in other countries that are needed by the firm to comply with Irish legislation are retained for the required period.

10. International Financial Sanctions

10.1 Financial Sanctions Framework

Sanctions are an instrument of a diplomatic or economic nature which seeks to bring about a change in activities or policies, such as violations of international law or human rights or policies that do not respect the rule of law or democratic principles.

Financial sanctions emanate from the European Union ('EU') and the United Nations ('UN') and are contained in sanctions lists.

EU Sanctions Regulations carry the following legal obligations:

- Prohibit making funds available, directly or indirectly to or for the benefit of individuals or entities listed on an EU Sanctions List
- Prohibit specific trade / financial transactions with certain countries
- Freeze all funds and economic resources of persons and entities on sanctions lists
- Report to the relevant competent authority (the Central Bank of Ireland) in respect of financial sanctions matches and any freezing of accounts or transactions

10.1.1 UN Sanctions

The UN imposes financial sanctions and requires Member States to implement them through Resolutions passed by the UN Security Council. Up to date information on UN Financial Sanctions can be found on the UN website:

https://www.un.org/sc/suborg/en/sanctions/information

The consolidated UN Sanctions Committees list relating to terrorism can be found at the following link:

https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

10.1.2 EU Sanctions

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

https://eeas.europa.eu/headquarters/headquarters-homepage/423/sanctions-policy_en

The consolidated list of EU sanctions can be found at the following link:

https://eeas.europa.eu/headquarters/headquarters-homepage/8442/consolidated-list-sanctions_en

The Central Bank website also includes up to date information on EU financial sanctions with links to the most up to date EU financial sanctions list for searching purposes. It also includes recent updates to the EU financial sanctions list.

https://www.centralbank.ie/regulation/anti-money-laundering-and-countering-the-financing-of-terrorism/countering-the-financing-of-terrorism

10.2 Role of the Central Bank

The Central Bank is one of three competent authorities with responsibilities in relation to financial sanctions in Ireland.

The other Irish competent authorities are the Department of Jobs, Enterprise and Innovation and the Department of Foreign Affairs and Trade.

10.3 Financial Sanctions Obligations on Firms

There is a legal obligation to comply with EU Council Regulations relating to financial sanctions as soon as they are adopted.

Once a person or entity has been sanctioned under EU Financial Sanctions, there is a legal obligation not to transfer funds or make funds or economic resources available, directly or indirectly, to that person or entity.

In the event that a match or a 'hit' occurs against a sanctioned individual or entity, Firms must immediately freeze the account and/or stop the transaction and immediately report the hit to the Central Bank along with other relevant information. In certain circumstances, firms can make a transfer to a sanctioned individual or entity if a prior authorisation is received or notification is given to a competent authority.

All persons must supply any information related to suspected financial sanctions breaches to the Central Bank pursuant to the relevant EU Council Regulations.

10.3.1 Financial Sanctions Governance

Firms should ensure that Senior Management are fully aware of the firm's obligations in the area of financial sanctions. It should also be clear, who at the firm has responsibility for financial sanctions. This individual should be of sufficient seniority in order to discharge the firm's responsibilities.

10.3.2 Financial Sanctions Risk Assessment

Firms should ensure the business-wide risk assessment takes into account their obligations under financial sanctions regulations. In particular, firms should pay particular attention to the risk factors outlined in section 4 of the Guidelines.

10.3.3 Screening Customers against Sanctions Lists

Firms should have effective screening systems appropriate to the nature, size and risk of their business.

Screening new and existing customers and payments against the relevant and up to date EU and UN lists helps ensure that firms will not breach the sanctions regulations. Customer screening should take place at the time of customer take-on and at regular intervals thereafter.

10.3.4 Matches and escalation

Where a customer's name matches a person on the relevant lists, firms should take steps to identify whether a name match is real or if it is a 'false positive' (for example; a customer has the same or similar name but is not the same person).

Firms should have procedures that look at a range of identifier information such as name, date of birth, address or other customer data.

Firms should have clear escalation procedures in place to be followed in the event of a positive match.

T: +353 (0)1 224 6000
E: xxx@centralbank.ie
www.centralbank.ie

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem