CONSULTATION DOCUMENT

AMENDMENTS TO THE IMPLEMENTING PROCEDURES PART I

Issued: 30 October 2018
Closing Date: 31 December 2018

Amendments to the Implementing Procedures Part I

The Financial Intelligence Analysis Unit (FIAU) has published a revised version of the Implementing Procedures Part I for consultation. The updated set of Implementing Procedures Part I reflects the legislative amendments which took place between December 2017 and January 2018 to the Prevention of Money Laundering Act (PMLA) and the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR). The revised set of Implementing Procedures Part I provides all persons and entities subject to the PMLFTR with more in-depth qualitative guidance assisting them in better fulfilling their AML/CFT obligations. The salient amendments are listed hereunder:

1. The Risk Based Approach

The revised Implementing Procedures Part I aim to reflect the now more significant Risk Based Approach which subject persons are required to adopt and implement vis-à-vis their AML/CFT obligations. The revised Chapter 3 of the Implementing Procedures Part I should provide subject persons with a better understanding of what the Risk Based Approach entails, and provides detailed guidance on the carrying out of business risk assessments and customer risk assessments which are the basis for the application of a Risk Based Approach to AML/CFT obligations.

2. Customer Due Diligence (CDD)

The revised Chapter 4 of the Implementing Procedures Part I now deals with CDD obligations. This section was revamped so as to provide subject persons with a better understanding of their CDD obligations as required by the PMLFTR. The revised Implementing Procedures Part I, now more than even before, emphasises on the importance of conducting appropriate and effective on-going monitoring, being one of the corner stones of CDD obligations. The proposed Chapter 4 not only aims to provide subject persons with appropriate and sufficient guidance in this regard, but also on other areas which directly impinge on their CDD obligations including when subject persons are faced with high-risk scenarios such as when dealing with high-risk clients, jurisdictions, products and services and interface risk.

Through amendments to the Implementing Procedures Part I in January 2017, the FIAU recognised the usability of technological alternatives for carrying out CDD obligations, particularly for the identification and verification of customers. The revised Implementing Procedures Part I now offer more flexibility on the use of such technological alternatives to fulfil AML/CFT obligations, reflecting the traction that such alternatives have gained.

3. Outsourcing

The revised Implementing Procedures Part I now has a dedicated Chapter 6 specifically dealing with outsourcing. The aim of this Chapter is to provide subject persons with a clear understanding of what AML/CFT obligations may be outsourced, which AML/CFT obligations shall not be

outsourced as well as how should such outsourcing arrangements take place including the procedures, way and manner in which this can be carried out.

The members of the Joint Committee for the Prevention of Money Laundering and Funding of Terrorism which represent the various subject persons, and all supervisory and other competent authorities, are invited to provide their feedback through written submissions on the proposed amendments to the Implementing Procedures Part I by not later than Monday 31st December 2018.

Written submissions are to be addressed to the Legal and International Relations Section of the FIAU via electronic mail on legal@fiumalta.org.

Training Event – Save the date

The FIAU shall be organising a training session to present and explain the proposed amendments to subject persons which would also serve as a platform to provide feedback. The training sessions shall be held on the 18th and 19th December 2018. Further information will be provided closer to the date.

FINANCIAL INTELLIGENCE ANALYSIS UNIT

IMPLEMENTING PROCEDURES

ISSUED BY THE FINANCIAL INTELLIGENCE ANALYSIS UNIT IN TERMS OF THE PROVISIONS OF THE PREVENTION OF MONEY LAUNDERING AND FUNDING OF TERRORISM REGULATIONS (S.L. 373.01)

PART I

Table of Contents

ABBREVIATIONS 10

CHAPTER 1 - OVERVIEW 12

1.1 What is money laundering? 12

1.1.1 The definition of money laundering in the PMLA 13

1.1.2 Money laundering in practice 14

1.2 What is funding of terrorism? 15

1.2.1 The Funding of Terrorism in practice 16

1.3 International initiatives in the fight against money laundering and the funding of terrorism 17

1.4 Maltese Legislation on money laundering and funding of terrorism 18

1.4.1 The Prevention of Money Laundering Act 19

1.4.2 The Prevention of Money Laundering and Funding of Terrorism Regulations 20

1.5 The Financial Intelligence Analysis Unit 21

1.5.1 The FIAU's compliance monitoring function 22

CHAPTER 2 – THE IMPLEMENTING PROCEDURES 25

2.1 Who are the 'Subject Persons'? 25

2.2 Purpose of the Implementing Procedures 28

2.3 Status and application of the Implementing Procedures 29

CHAPTER 3 – THE RISK BASED APPROACH 31

3.1 Notions of Risk 31

3.2 Risk Factors 32

3.2.1 Customer Risk 33

3.2.2 Geographical Risk 35

3.2.3 Product, Service and Transaction Risk 36

3.2.4 Delivery Channels Risk 37

3.2.5 Additional Risk Factors 37

3.2.6 Sector Specific Risk Factors 38

3.2.7 Sources of Information 38

3.3 The Business Risk Assessment 39

3.3.1 The Basic Steps 39

Table 1 – Likelihood scale 41

Table 2 – Impact scale 41

Table 3 – Inherent Risk 41

Table 4 – Effectiveness 42

3.3.2 Carrying out the Business Risk Assessment 43

3.3.3 Timing of the Business Risk Assessment 44
3.3.4 Revising the Business Risk Assessment 45
3.4 Mitigating Measures, Policies, Controls and Procedures 46
3.4.1 The Customer Acceptance Policy 47
3.5 The Customer Risk Assessment 47
3.5.1 Timing of the Customer Risk Assessment 48
3.5.2 Preparing/Drafting the Customer Risk Assessment 49
3.5.3 Carrying out the Customer Risk Assessment 49
Table 5 – Risk scoring grid 51
Table 6 – Risk score 51
3.6 Application of CDD on a Risk-Sensitive Basis 53
CHAPTER 4 – CUSTOMER DUE DILIGENCE 54
4.1 Overview of CDD measures 55
4.2 Definitions 57
4.2.1 The Customer 57
4.2.2 The Beneficial Owner 60
Table 7 – Definition of a beneficial owner 61
4.3 Identification and Verification 76
4.3.1 The nature of identification and verification of a natural person 77
4.3.2 Identification and Verification of Customers other than Natural Persons 91
4.3.3 The Agent 105
4.4 The purpose and intended nature of the business relationship and the Customer's Business and Risk Profile 105
4.4.1 Purpose and Intended Nature of the Business Relationship 106
4.4.2 The Customer's Business and Risk Profile 106
4.4.3 The Source of Wealth and the Source of Funds 108
4.5 Ongoing monitoring 109
4.5.1 Overview of the duty to conduct ongoing monitoring 109
4.5.2 Transaction Monitoring 110
4.5.3 Ensuring that documents, data and information held on the customer are kept up-to-date 116
4.6 Timing of Due Diligence Procedures 119
4.6.1 Timing of CDD when establishing a business relationship 119
4.6.2 Timing of CDD when an occasional transaction is carried out 122
4.6.3 Timing of CDD in case of suspicion of ML/FT 123
4.6.4 When the subject person doubts the veracity or adequacy of CDD documentation 123

4.6.5 Timing of CDD in relation to existing customers 123
4.6.6 Acquisition of the business of one subject person by another 125
4.7 Failure to complete CDD measures laid out in Regulation 7(1)(a) to (c) 126
4.8 Simplified Due Diligence 127
4.8.1 Particular Situations in which SDD may be applied 129
4.8.2 Circumstances where SDD cannot be applied 132
4.9 Enhanced Due Diligence 133
4.9.1 Situations presenting a High Risk of ML/FT 134
4.9.2 Situations in which EDD is prescribed by law 136
4.10 Reliance on Other Subject Persons or Third Parties 152
4.10.1 Introduction 153
4.10.2 Scope 153
4.10.3 Entities that may be relied on 154
4.10.4 Carrying out reliance 156
4.10.5 The reliance agreement 157
4.10.6 When reliance is not permitted 158
CHAPTER 5 – REPORTING PROCEDURES AND OBLIGATIONS 159
5.1 The Money Laundering Reporting Officer 159
5.1.1 The Role of the MLRO 159
5.1.2 Who Can be Appointed as MLRO 159
5.1.3 Appointment and Resignation of the MLRO 161
5.2 The Designated Employee 162
5.3 The Monitoring Function 162
5.4 Internal Reporting Procedures 164
5.5 External Reporting Procedures 167
5.6 Actions After Reporting 170
5.7 The obligation to refrain from carrying out a transaction that appears to be suspicious 171
5.8 Delaying the Execution of a Suspicious Transaction 172
5.9 Monitoring Orders 178
5.10 Professional Privilege 178
5.11 Prohibited and Permissible Disclosures 179
5.12 Reports for Compliance Purposes 182
5.13 Reporting under Regulation (EU) 2015/847 183
5.14 The Protection of the Whistleblower Act 183
CHAPTER 6 – OUTSOURCING 186
6.1 What is to be considered as Outsourcing? 186

6.2 Responsibility of the Subject Person 186
6.3 Extent of Outsourcing 187
6.4 Conditions to which Outsourcing is subject 188
6.5 Outsourcing within a Group Context 190
CHAPTER 7 – AWARENESS, TRAINING AND VETTING OF EMPLOYEES 191
7.1 Awareness and training: the obligation and purpose behind it 191
7.2 Employees to be Provided with Training 192
7.3 Content of Training 193
7.4 Method of delivery of training 194
7.5 Screening of new employees 194
CHAPTER 8 – JURISDICTIONS, GROUPS AND PENALTIES 196
8.1 Non-Reputable Third Countries 196
Table 6 – Categories identified by FATF 197
8.2 Group-Wide Policies and Procedures 199
8.2.1 Parents, Majority-Owned Subsidiaries and Branches 199
8.2.2 Sharing of Information 200
8.2.3 Reporting of Suspicious Transactions 200
8.2.4 Impediments to the Application of Group-Wide Policies and Procedures 201
8.3 Penalties for Breaches of AML/CFT Obligations 201
8.3.1 Administrative Sanctions under PMLFTR 202
Table 7 – Penalties 204
8.3.2 Procedure for imposition of sanctions 204
8.3.3 Appeals from Administrative Penalties 205
8.3.4. Publication of Administrative Penalties and other Measures 205
8.3.5 CRIMINAL OFFENCES 206
CHAPTER 9 – RECORD KEEPING PROCEDURES 207
9.1 Purpose of keeping records 208
9.2 Records to be retained 208
9.3 Period of retention of records 210
9.3.1 CDD documentation 211
9.3.2 Documentation on the business relationship and on the transactions carried out in the course of a business relationship or in relation to an occasional transaction 211
9.3.3 Internal Reports made to the MLRO and STRs 212
9.3.4 Records submitted together with a STR 212
9.3.5 AML/CFT training 212
9.3.6 Employee Screening Records 212

9.3.7 Outsourcing Records 213
9.3.8 Other Records 213
9.4 Form of records 213
9.5 Retrieval of records 213
9.5.1 General Requirements 214
9.5.2 Organisation and Categorisation of Records 214
9.6 Record Keeping Obligations and Data Protection 215

ABBREVIATIONS

4th AML Directive	European Union Directive 2015/849 of 20 May, 2015
AML/CFT	Anti-money laundering/combating the funding of terrorism
CDD	Customer due diligence
EDD	Enhanced customer due diligence
EU	European Union
FATF	Financial Action Task Force
FATF Recommendations	The FATF Recommendations on Money Laundering and Terrorist Financing adopted in 2012
FSRB	FATF-Style Regional Body
FIAU	Financial Intelligence Analysis Unit
FIU	Financial Intelligence Unit
JMLSG	Joint Money Laundering Steering Group
MFSA	Malta Financial Services Authority
MGA	Malta Gaming Authority
ML/FT	Money laundering and funding of terrorism
MLRO	Money Laundering Reporting Officer
MONEYVAL	The Council of Europe Select Committee of Experts on the Evaluation of anti-Money Laundering Measures and the Financing of Terrorism
PEP	Politically exposed person
PMLA	Prevention of Money Laundering Act (Cap. 373, the Laws of Malta)
PMLFTR	Prevention of Money Laundering and Funding of Terrorism Regulations (S.L. 373.01)
RBA	Risk-Based Approach

SDD	Simplified customer due diligence
STR	Suspicious transaction report
UN	United Nations

CHAPTER 1 - OVERVIEW

1.1 What is money laundering?

Generally, money laundering is described as the process by which the illegal nature of criminal proceeds is concealed or disguised in order to give a legitimate appearance to such illegal proceeds. This process is of crucial importance for criminals as it enables the perpetrators to make seemingly legitimate economic use of the criminal proceeds. When a criminal activity generates substantial income, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or to the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.

Illegal arms sales, smuggling, activities of organised crime (such as drug trafficking and prostitution rings), bribery, corruption, fraud and insider trading are typical examples of criminal activities that could generate large profits. The source of such proceeds would need to be disguised for the criminal to be able to enjoy the ill-gotten gains made.

Traditionally, three stages were identified for the process of money laundering:

(a) the placement stage;
(b) the layering stage; and
(c) the integration stage.

Placement stage – the physical disposal of cash or other assets derived from criminal activity. During this phase, the money launderer introduces the illicit proceeds into the financial system, usually by breaking up large amounts of cash into less conspicuous smaller sums and placing these funds into circulation through formal financial institutions and other legitimate businesses, both domestic and international. This is the point at which the proceeds of crime are most apparent and most easily detected – this is the most vulnerable stage in the laundering process.

Examples of placement transactions include:

(a) Blending of funds: commingling of illegitimate funds with legitimate funds such as placing the cash from illegal narcotics sales into cash-intensive locally owned restaurants;
(b) Purchasing of foreign exchange with illegal funds;
(c) Repayment of legitimate loans using cash derived from the commission of a crime;
(d) Placing cash in small amounts and depositing it into numerous bank accounts in an attempt to evade reporting thresholds.

Once the money has been placed in the financial system, the launderer engages in a series of conversions or movements of the funds to distance them from the source – the **layering stage**. This second stage involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to obfuscate the source and the ownership of funds.

Examples of layering transactions include:

(a) Electronically moving funds from one country to another and dividing them into advanced financial options and/or markets;
(b) Moving funds from one financial institution to another or within accounts held with the same institution; and
(c) Placing money in stocks, bonds and life insurance products.

In the third stage – the **integration stage** – the launderer seeks to supply apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appears to be normal business or personal transactions. This stage entails using laundered proceeds in seemingly normal transactions to create the perception of legitimacy.

Examples of integration transactions include:

(a) Purchasing luxury assets like real estate, artwork, jewellery or high-end automobiles;
(b) Investments that can be made in business enterprises through financial arrangements or other ventures.

It should be noted that the three-stage model is rather simplistic and does not reflect every type of money laundering operation.

1.1.1 The definition of money laundering in the PMLA

The definition of money laundering in the PMLA goes beyond generically expounding the notion of money laundering on the basis of the three traditional stages identified above. In fact, passive possession of criminal property is also considered to amount to the offence of money laundering. The definition provides an exhaustive list of acts which constitute money laundering under Maltese law, which are the following:

"(i) the conversion or transfer of property knowing or suspecting that such property is derived directly or indirectly from, or the proceeds of, criminal activity or from an act or acts of participation in criminal activity, for the purpose of or purposes of concealing or disguising the origin of the property or of assisting any person or persons involved or concerned in criminal activity;

(ii) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect of, in or over, or ownership of property, knowing or suspecting that such property is derived directly or indirectly from criminal activity or from an act or acts of participation in criminal activity;

(iii) the acquisition, possession or use of property knowing or suspecting that the same was derived or originated directly or indirectly from criminal activity or from an act or acts of participation in criminal activity;

(iv) retention without reasonable excuse of property knowing or suspecting that the same was derived or originated directly or indirectly from criminal activity or from an act or acts of participation in criminal activity;

(v) attempting any of the matters or activities defined in the above foregoing sub-paragraphs (i), (ii), (iii) and (iv) within the meaning of article 41 of the Criminal Code;

(vi) acting as an accomplice within the meaning of article 42 of the Criminal Code in respect of any of the matters or activities defined in the above foregoing sub-paragraphs (i), (ii), (iii), (iv) and (v)".

The definition of money laundering in the PMLA largely emanates from Article 1(3) of the 4th AML Directive and largely reflects the definition in the *Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism* (also known as the **Warsaw Convention** or **CETS 198**), in the 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the 'Vienna Convention') and that in the 2000 United Nations *Convention against Transnational Organized Crime* (the 'Palermo Convention').

The definition of money laundering under Maltese law, however goes beyond that under EU and international conventions, for instance:

(a) Mere *suspicion* of criminal activity is sufficient (being, as it is termed, a so-called 'suspicion-based regime') and there is no need to have *knowledge*;
(b) Criminalising money laundering irrespective of the crime that generates the proceeds - 'all crime regime';
(c) Covering property that may even be *indirectly* derived from criminal activity.

1.1.2 Money laundering in practice

A money launderer will seek to operate in and around the financial system in a manner that best fits the execution of the scheme to launder funds. As soon as many governments around the world enacted AML obligations for the banking sector, a shift in laundering activity into the non-bank financial sector (such as third-party payment processors, money services businesses, insurance companies, securities broker-dealers) and to non-financial businesses and professions[1] (casinos, dealers in high value items, real estate, vehicle sellers, and various gate-keepers like notaries, accountants, auditors and lawyers, trust and company service providers) started to increase.

Money laundering is an ever-evolving activity; it must be continuously monitored in all its various forms in order for measures against it to be timely and effective. Illicit property can move through numerous different commercial channels, including products such as transferable cheques, savings and brokerage accounts, loans, wire transfers, or through intermediaries such as trustees and company service providers, securities dealers, banks and money services businesses.

FATF and FSRBs publish periodic typology reports to "**monitor changes and better understand the underlying mechanisms of money laundering and terrorist financing**."[2] Their aim is to keep efforts at combating money laundering and terrorist financing dynamic and up-to-date, precisely

[1] Referred to as DNFBPs.
[2] FATF 'Report on Money Laundering Typologies 2002-2003' of 14th February, 2003 (page 1 paragraph 2).

because of the ever-evolving nature of the crime of money laundering and the methods used by launderers to disguise the illicit origin of ill-gotten gains.

Money laundering is indeed frequently carried out in an international context, and therefore measures taken at national level or even at EU level would be futile if they did not also take into account international coordination and cooperation. Particular account should be taken of the FATF Recommendations as well as instruments of other international bodies active in the fight against ML/FT. A number of initiatives have been created to deal with the problem at an international level, such as the establishment of the Egmont Group of FIUs, which is a worldwide group that promotes closer cooperation between FIUs and facilitates information sharing through a secure internet system known as the 'Egmont Secure Web'. [3]

1.2 What is funding of terrorism?

The funding of terrorism is the process of making funds or other assets available to support, even indirectly, the carrying out of terrorist activities. The process of funding of terrorist groups or individual terrorists is addressed in Article 328B and 328F of the Criminal Code.[4] The Criminal Code also contemplates other acts which are considered to constitute funding of terrorism. These include the use or possession of money or other property for the purposes of terrorist activities (Article 328G) and the involvement in funding arrangements to support terrorist activities (Article 328H and 328I). The criminal offence of funding of terrorism under the Criminal Code reflects the definition of funding of terrorism under the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism.

The funding of terrorist activity, terrorist organisations or individual terrorists may take place through funds deriving from legitimate sources or from a combination of lawful and unlawful sources. Indeed, funding from legal sources is a key difference between terrorist organisations and traditional criminal organisations involved in money laundering operations. While the former may thrive on funds derived from legitimate sources, money laundering necessarily involves funds derived from illegal sources. Another difference is that while the money launderer moves or conceals criminal proceeds to obscure the link between the crime and the generated funds and avails himself of the profits of crime, the terrorist's ultimate aim is not to generate profit from the fund-raising mechanisms but to obtain resources to support terrorist operations.[5]

Although it would seem logical that funding from legitimate sources would not need to be laundered, there is often a need for terrorists to obscure or disguise links between the organisation or the individual terrorist and their legitimate funding sources. Therefore, terrorists must similarly find ways to process these funds in order to be able to use them without drawing the attention of authorities.[6]

[3] The FIAU became a member of the Egmont Group in 2003.
[4] Cap. 9 of the Laws of Malta.
[5] FATF, Guidance for Financial Institutions in Detecting Terrorist Financing, April 2002, pp. 4-5, paragraph 12, 13 and 16.
[6] Ibid, p.5, paragraph 15.

Financing is required not only to fund specific terrorist acts but, more generally, to meet the operational costs of terrorist organisations such as maintaining a terrorist network or cell, recruitment and training, sustaining an ideology of terrorism through propaganda, and maintaining an infrastructure of organisational support (even more so if this is to sustain an international network).

Terrorist organisations will vary from one organisation to another ranging from large, state-like organisations to small, decentralised and self-directed networks. Likewise, the nature of terrorist financing will vary depending on the size and scale of the organisation involved, if any, and the source from which funding is derived. Terrorist activities may be financed by states, companies or charities, as well as being self-financed by the terrorists themselves. Various methods of funding may be used at the same time.

1.2.1 The Funding of Terrorism in practice

Cutting off financial support to terrorists and terrorist organizations is essential to disrupting their operations and preventing attacks. Without funding, the commission of terrorist acts becomes more difficult (albeit not impossible) to perpetrate.

Terrorists continue to adapt their tactics and diversify their funding sources. Charities, for instance, appear to be highly attractive to terrorists for various reasons. Charities enjoy public trust, they often have access to considerable funds, their activities are often cash-intensive, they may be subject to significantly lighter regulatory requirements and, more specifically those with a global presence, provide the right framework for international operations as they would have branches in various parts of the world. Charities have for this reason been noted as highly vulnerable to misuse by terrorists. They can be misused in various ways such as by setting up sham organisations posing as legitimate ones, or by raising funds for a specific charitable cause through a legitimate organisation and subsequently diverting the generated funds towards terrorist purposes.

The FATF states in its 2014 *Risk of Terrorist Abuse in Non-Profit Organizations (NPO)* Report that:

"***The importance of the NPO sector to the global community cannot be overstated. It is a vibrant sector, providing innumerable services to millions of people.***"

However, this typologies project found that more than a decade after the abuse of NPOs by terrorists and terrorist organizations was formally recognized as a concern, the terrorism threat to the sector remains, and the sector continues to be misused and exploited by terrorist organisations through a variety of means. The best practices guidance was updated in 2015 with the purpose of assisting countries in implementing FATF Recommendation 8 on NPOs in line with the risk-based approach; to assist NPOs in mitigating terrorist-financing threats and assisting financial institutions in the proper implementation of the risk-based approach when providing financial services to NPOs.

The FATF's 2015 *Emerging Terrorist Financing Risks* Report details other funding methods such as:

(a) self-funding FTFs (Foreign Terrorist Fighters) the advent of social media, smartphone applications, and internet sharing sites, which now provide terrorist organizations with global reach at little to no cost;
(b) raising funds through social media;
(c) new payment products and services;
(d) exploitation of natural resources.

1.3 International initiatives in the fight against money laundering and the funding of terrorism

The Financial Action Task Force (FATF)

Formed in 1989, the FATF is an inter-governmental body whose aim is to set standards and foster international action against ML/FT. The FATF has throughout the years developed a series of Recommendations that are recognised as the international standard for combating ML/FT, and more recently the proliferation of weapons of mass destruction. These Recommendations were first issued in 1990 and have been revised on a number of occasions, most recently in February 2012.

MONEYVAL

MONVEYVAL is a body of the Council of Europe tasked with evaluating compliance with the FATF Recommendations and makes recommendations to member countries and their respective authorities in relation to improvements to their AML/CFT regimes. MONEVYAL evaluations are carried out on a regular basis through a system of peer reviews. MONEVYAL fulfils the role of a FSRB for the European region and Malta is a member of MONEYVAL.

The European Union

The EU has over the years taken a number of legislative initiatives to combat ML/FT. The EU issued the first anti-money laundering directive in 1991, and has since then issued a number of revised versions with the most recent one being the 4th AML Directive published in May 2015 and which Malta has transposed into its national law. While the EU's anti-money laundering directive is largely based on the FATF Recommendations, it often goes beyond and imposes tighter controls on a number of aspects such as with regards to the transparency of legal persons and arrangements, and the accessibility to their beneficial ownership information. Directive (EU) 2018/843, frequently referred to as the Fifth Anti-Money Laundering Directive, has introduced a number of amendments to the 4th AML Directive which are in the process of being transposed into Maltese law.

Besides enacting legislation to fight ML/FT, the EU has taken numerous initiatives to foster EU-wide cooperation in this area. An Expert Group on Money Laundering and Terrorist Financing has been set up to serve as a platform for Member States to coordinate actions, exchange views and

best practices, and provide expertise to the EU Commission in preparing legislative and implementing measures. Similarly, the EU Financial Intelligence Units Platform, an informal group set up by the EU Commission in 2006, brings together EU FIUs to enhance cooperation through a number of initiatives.

The Joint Committee of the European Supervisory Authorities (ESAs), i.e. the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA), is another important EU-wide initiative aimed at strengthening cooperation between the ESAs, and has established a sub-committee dedicated to AML/CFT which is tasked under the 4th AML Directive with the issuance of technical guidance to assist authorities and subject persons in the implementation of the 4th AML Directive. Malta actively participates in all these EU bodies and platforms through the respective authorities.

Egmont Group of Financial Intelligence Units

Recognising the benefits inherent in the development of a financial intelligence units (FIU) network, in 1995 a group of FIUs decided to establish an informal group for the stimulation of international co-operation, which has now grown into a worldwide group bringing together over 155 FIUs. Through the Egmont Group, member FIUs meet regularly to find ways to cooperate, especially in the areas of information exchange, training and the sharing of expertise. The Egmont Group facilitates the exchange of intelligence and financial information between FIUs through a secure internet system known as the Egmont Secure Web and has moreover issued a number of statements and papers to assist FIUs in engaging in international cooperation. Malta became a member of the Egmont Group in 2003.

1.4 Maltese Legislation on money laundering and funding of terrorism

The first legislative initiative to introduce an anti-money laundering regime in Malta dates back to February 1994, when Article 22 (1C) of the Dangerous Drugs Ordinance was amended to introduce the offence of money laundering in relation to the proceeds of certain drug-related offences.[7] Eventually, the PMLA was enacted in September of the same year, together with the original regulations issued thereunder, which introduced a comprehensive regime for the criminalisation of money laundering in relation to predicate offences which are not merely drug-related, as well as the prevention, investigation and prosecution of money laundering. Concurrently with the enactment of the PMLA, an amendment to Article 120A of the Medical and Kindred Professions Ordinance[8] was made to introduce the offence of money laundering in relation to proceeds of offences related to other illegal substances beyond the scope of those provided for under the Dangerous Drugs Ordinance.

After its enactment, the PMLA was amended to extend the remit of the FIAU to the area of funding of terrorism, which was criminalised through amendments to the Criminal Code. The regulations

[7] Cap. 101 of the Laws of Malta.
[8] Cap. 31 of the Laws of Malta.

were consequently repealed and replaced by the PMLFTR, which cover the emerging threat of funding of terrorism as well as other developments in the field of AML/CFT. The PMLA and the PMLFTR contain provisions which were introduced in pursuance to Malta's ongoing commitment to comply with international standards in the AML/CFT field, as well as to honour its obligations as a member of the European Union.

1.4.1 The Prevention of Money Laundering Act

The PMLA was enacted on 23rd September 1994 and was subject to a number of amendments thereafter. The more important legislative developments include the legal provisions establishing the FIAU through the amending Act XXXI of 2001, the extension of the provisions of the PMLA to include the offence of funding of terrorism by means of the amending Act VI of 2005, and the implementation of the provisions of the Council of Europe Convention No. 198 on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism through the enactment of Act XXXI of 2007. Extensive amendments to the PMLA were also introduced in 2015 and 2017, by virtue of Act III of 2015 and Act XXVIII of 2017 respectively. Act III of 2015 addressed a number of shortcomings that had been identified in MONEYVAL's fourth round Mutual Evaluation Report of Malta adopted in March 2012, while Act XXVIII of 2017 amended and introduced a number of provisions mainly intended to transpose into Maltese legislation the 4th AML Directive. These amendments also introduced a number of other provisions to strengthen the AML/CFT regime under Maltese law.

The first part of the PMLA provides a definition of money laundering (refer to Section 1.1) and criminalises the act of money laundering.[9] The maximum penalty for the offence of money laundering is a fine amounting to two million and five hundred thousand euro (€2,500,000) or to imprisonment for a period not exceeding eighteen years, or to both such fine and imprisonment. The PMLA provides that the offence of money laundering may be committed by a natural person as well as a body of persons, whether corporate or unincorporate.[10] The PMLA also provides a definition of criminal activity[11] and property[12]. Originally, the PMLA only applied to a limited list of predicate offences[13], however since 31st May 2005, with the coming into effect of Legal Notice 176 of 2005, Malta has shifted from having a restricted list of predicate offences to an 'all crimes' regime, meaning that 'any criminal offence', whenever or wherever it is carried out, may constitute the basis for the offence of money laundering.[14]

The PMLA lays down the procedures for the prosecution of money laundering[15] as well as the measures for the confiscation of property upon a conviction for money laundering[16], measures

[9] Article 3(1) of the PMLA.
[10] Article 3(2) of the PMLA.
[11] Article 2(1) of the PMLA.
[12] Article 2(1) of the PMLA.
[13] The predicate offence is the underlying criminal activity from which the illegal funds originate.
[14] Article 2(1) of the PMLA.
[15] Article 3(2A), (3), (4), (6) and (7) of the PMLA.
[16] Article 3(5) of the PMLA.

for the freezing of assets when a person is charged with money laundering[17] and measures for the issuance of an investigation and/or attachment order when a person is suspected of having committed money laundering[18]. Additionally, by virtue of article 435AA of the Criminal Code, which is applicable to the PMLA, the Criminal Court may order a bank to monitor the banking operations being carried out through one or more accounts of a person suspected of having committed money laundering for a specified period. Provisions are also provided for international mutual assistance in the implementation of measures relating to confiscation, freezing, and other court orders related to the investigation of money laundering.

The second part of the PMLA establishes the FIAU, a Government agency purposely set up to perform the functions set out in Article 16 of the PMLA. The functions and remit of the FIAU are dealt with in more detail in Section 1.5.

1.4.2 The Prevention of Money Laundering and Funding of Terrorism Regulations

The PMLFTR, which were issued by virtue of Legal Notice 372 of 2017 and came into force on the 1st January 2018, have repealed and replaced the 2008 Regulations[19] which had in turn repealed the previous 2003 Regulations. The various versions of the Regulations since 1994 reflect the corresponding international developments and legislative developments within the EU. In fact, the PMLFTR transpose the 4th AML Directive which is in turn modelled on the FATF Recommendations.

The PMLFTR set out the obligations and procedures that subject persons are required to fulfil and to implement, and without which an AML/CFT regime cannot be effective. These procedures mainly consist of the following measures:

(a) procedures on internal control, risk assessment, risk management, compliance management and communications;
(b) customer due diligence;
(c) record keeping;
(d) internal reporting; and
(e) training and awareness.

The added focus on a Risk-Based Approach (RBA) is considered to be the main development of the PMLFTR introduced in 2017.[20] This obliges a subject person to take appropriate steps (in proportion to the nature and size of its business) to identify and assess the risks of ML/FT, taking into account risk factors including those relating to their customers, countries or geographic areas, products, services, transactions or delivery channels, and to take ensuing mitigating measures commensurate to the risks identified. Whereas under the old regime the concept of a RBA was optional, under the new Regulations more emphasis is placed on the risk-based application of AML/CFT requirements.

[17] Article 5 of the PMLA.
[18] Article 4 of the PMLA.
[19] Legal Notice 180 of 2008.
[20] Legal Notice 372 of 2017.

1.5 The Financial Intelligence Analysis Unit

The FIAU is a mandatorily required national government agency, having a distinct legal personality, that handles financial intelligence. [21] The FIAU was set up in 2001 by virtue of Act XXXI of 2001, through the inclusion in the PMLA of a number of provisions which provide for the establishment of the FIAU and which define its powers and functions. The FIAU receives reports of suspicious transactions from financial institutions and other persons and entities, analyses them and disseminates the resulting intelligence to local law enforcement agencies and foreign FIUs to combat ML/FT. The model adopted by the Maltese legislator is an administrative model, meaning that the FIAU is constituted as an independent administrative authority distinct from law enforcement and judicial authorities. Thus the FIAU has no investigatory or prosecutorial powers, which powers are vested in the Police and the Attorney General. This type of arrangement serves as a 'buffer' between subject persons (composed of entities and persons carrying out financial and non-financial businesses or professional activities) and law enforcement and prosecutorial authorities.

The functions and responsibilities of the FIAU are primarily set out under Article 16 of the PMLA, with some other powers and functions conferred to the FIAU by virtue of other provisions found in the PMLA and other legislative instruments. Being the entity responsible for the collection, collation, processing, analysis and dissemination of information with a view to combating ML/FT, the core function of the FIAU is the receipt and analysis of reports made by subject persons on transactions and activities suspected to involve ML/FT or proceeds of crime (referred to as STRs), and the dissemination of financial intelligence to law enforcement authorities and other competent authorities.[22]

Another main function of the FIAU, discussed in more detail in Section 1.5.1 below, is its responsibility to supervise, monitor and ensure compliance by subject persons with their obligations under the PMLA and PMLFTR.

The FIAU is given additional and extensive powers for co-operating and exchanging information with counterpart FIUs and foreign supervisory authorities and has wide ranging powers to demand information both for the carrying out of its functions and also to assist foreign FIUs and supervisory authorities. In fact, in carrying out its functions according to the PMLA, the FIAU may demand information deemed to be relevant and useful for the purposes of pursuing its functions from subject persons, the Police, any government ministry, department, agency or other public authority, any supervisory authority, and any other natural or legal person who, in the opinion of the FIAU, may hold such information.

The FIAU also has the power to impose administrative sanctions consisting in administrative penalties and reprimands in writing for any failure by subject persons to comply with lawful

[21] The setting up of a FIU is a mandatory requirement emanating from various international commitments such as the FATF Recommendations and the 4th AML Directive.
[22] Regulation 16(1) of the PMLA.

requirements, orders or directives issued by the FIAU or for contraventions of provisions of the PMLFTR or procedures or guidance issued thereunder. The FIAU may also issue written directives requiring subject persons to carry out or refrain from carrying out any act and may, in certain particular circumstances, require the termination of business relationships or the closure of branches, and is also empowered to delay the execution of transactions that are deemed to be suspicious.

The FIAU is composed of two main organs: the Board of Governors and the Director, together with the permanent staff of the FIAU. The members of the Board are appointed by the Minister responsible for finance from four panels each consisting of at least three persons, nominated respectively by the Attorney General, the Governor of the Central Bank of Malta, the Chairman of the Malta Financial Services Authority and the Commissioner of Police. All Board members discharge their duties in their personal capacity and are not subject to the direction of any person or authority. The main responsibility of the Board is to lay down the policy to be followed by the FIAU, which is then to be executed and pursued by the Director. The Board of Governors remains responsible to ensure that the Director carries out that policy accordingly. Additionally, the Board is responsible for advising the Minister responsible for finance on all matters and issues relevant to the prevention, detection, investigation, prosecution and punishment of ML/FT offences.

In 2016, the EU initiated a number of measures to strengthen the role of FIUs and their ability to share information across Europe as part of its comprehensive action plan towards the fight against terrorism. The European Commission had presented an Action Plan to strengthen the fight against FT, which included revisions to the 4th AML Directive aimed at enhancing the powers of FIUs to exchange information and to cooperate. The EU Commission will also be tasked with assessing whether additional legislative or other initiatives are required to promote further cooperation between FIUs, and with enhancing their roles and powers. This follows a detailed mapping exercise which was carried out by EU FIUs to analyse the obstacles that FIUs faced in carrying out their functions and cooperating and exchanging information with each other.

1.5.1 The FIAU's compliance monitoring function

The FIAU is responsible for monitoring compliance by subject persons with the obligations set out under the PMLA and PMLFTR. The FIAU adopts a risk-based approach when carrying out its supervisory function. For this purpose the FIAU conducts risk assessments to understand the risk posed by the various sectors, businesses and professions, and the various entities and individuals operating within such sectors. A risk-based approach ensures that the FIAU is able to focus its resources where it matters the most to enhance the effectiveness of its role.[23] In the fulfilment of such responsibility the FIAU conducts both off-site and on-site monitoring as will be explained in further detail below. To assist the FIAU in carrying out proper risk assessments, subject persons may be required to submit compliance reports containing information and data on their activities or business (for further details on the compliance report refer to Section 5.12). In accordance with the authority granted to it under Regulation 19 of the PMLFTR, the FIAU may also from time to time request the submission of other periodical reports apart from the compliance report.

[23] Regulation 4(1) of the PMLFTR.

Compliance monitoring is carried out by the FIAU through either on-site or off-site reviews, or through a combination of both. On-site reviews entail visits to the premises of the subject person to determine the extent to which the provisions of their AML/CFT obligations are being implemented in practice. Such examinations typically involve meetings and interviews with key officials of the subject person, such as the MLRO and other officials or employees, as well as reviews of a number of customer files and records, the subject person's policies and procedures and any automated systems that the subject person may be using. It is normal practice for subject persons to be informed beforehand of an impending on-site examination and to be requested to provide information and documentation to enable the carrying out of the assessment, such as client lists and policy and procedures documents. However, the FIAU may also opt to carry out surprise visits without prior notice.

Off-site reviews on the other hand do not involve visits to the subject person's premises but are carried out through a so called 'desk-review' of information received or requested by the FIAU from the subject person. Such information and documentation may for example include AML/CFT procedures or policy documents, risk assessment documentation and ongoing monitoring methodologies, and will depend on the scope and purpose of that particular review.

The extent of both on-site and off-site reviews may vary depending on a number of factors. Reviews may be carried out to assess the general implementation of AML/CFT obligations, to focus on particular and specific obligations (such as the implementation of ongoing transaction monitoring), or to analyse particular services or products, be it across a sector/s or in relation to one particular subject person. The extent may also vary depending on the risk of ML/FT posed by the subject person being reviewed, with the riskier ones to expect more comprehensive and thorough examinations as opposed to brief supervisory meetings that might be carried out on subject persons that are deemed to be exposed to a low risk of ML/FT.

It is important to note that the PMLA enables the FIAU to request a supervisory authority, having supervisory powers over certain categories of subject persons (such as the MFSA and the MGA), to carry out on-site or off-site AML/CFT examinations on behalf of or jointly with the FIAU.[24] In all cases where on-site and off-site examinations are conducted by the MFSA or the MGA, the findings of the examination are reported to the FIAU and the FIAU determines whether any subsequent administrative action is necessary. Moreover the FIAU may deem it expedient to engage experts to assist it in the carrying out of its functions, including compliance monitoring.[25]

Cooperation with other supervisory authorities, both domestic and foreign, is an important aspect of the FIAU's supervisory function. The FIAU is empowered to cooperate with supervisory and regulatory authorities generally to ensure that the financial sector or any other sector is not misused for criminal purposes and thus to safeguard its integrity. This would for example involve the sharing of information with authorities empowered to issue licenses or authorisations to assist such authorities in their due diligence and fit and properness tests carried out prior to granting licenses or authorisations or the carrying out of joint supervisory actions with foreign

[24] Article 27(3) of the PMLA.
[25] Article 26A of the PMLA.

counterparts in respect of obliged entities that have branches, majority owned subsidiaries or other physical establishments in Malta or subject persons that have branches, majority owned subsidiaries or other physical establishments in foreign jurisdictions. The FIAU in its supervisory role is also expected to cooperate and exchange information with the respective ESA acting in terms of EU directives and regulations.[26]

[26] Regulation 2(5) of the PMLFTR.

CHAPTER 2 – THE IMPLEMENTING PROCEDURES

The misuse of the financial system to channel illicit gains, or even lawful gains destined for unlawful purposes (namely terrorism) poses a clear risk to the integrity, proper functioning, reputation and stability of the financial system. These criminal acts know no boundaries and jurisdictions having weak, ineffective or inadequate AML/CFT legislative and regulatory frameworks are most vulnerable. Thus, the upholding of legal and professional standards is critical to the integrity of financial markets.

The techniques used by money launderers constantly evolve to match the source and amount of funds to be laundered, and the legislative/regulatory/law enforcement environment of the market in which the money launderer operates. Therefore, persons undertaking certain activities, defined as subject persons, need to adopt measures in order to ensure that money gained through unlawful means is not channelled and laundered through the system and/or that such money, or even money from totally legitimate sources, is not used to finance terrorism. Subject persons should ensure that their AML/CFT policies, controls processes and procedures are appropriately designed and implemented, and are effectively operated to reduce the risk of them being used in connection with money laundering or terrorist financing activities.

Being used for ML/FT purposes involves firms, businesses and professionals in reputational, legal and regulatory risks. On any level, an operator should have an inherent interest – if not also an altruistic one in the interests of society and the jurisdiction's reputation as a whole – to ensure that it is not used as a vehicle to launder funds or to fund terrorist organisations. Many service providers invest lots of money and time to develop their business, and their reputation invariably takes years to develop. However, all this can be lost in an unbelievably short time if the organisation gets embroiled in a ML/FT scandal. The same can be said about a country's reputation, which would be harmed by the negative publicity of ML/FT cases attract, and which would in turn have serious repercussions on the country's economic well-being and the ability to attract the right type of business and investment.

By appropriately implementing effective AML/CFT policies and measures and being able to detect and flag suspicious transactions subject persons would be assisting the authorities in defending the financial system, and the entity, business or profession concerned, from criminal activity. They are essentially enabling the relevant authorities to perform their functions at law in an effective manner, as ultimately it is subject persons who are the first points of contact for criminals. For this reason, subject persons and their relevant employees and officials that deal with customers should be aware and appropriately trained in how to recognise and deal with transactions and other activities which may be related to ML/FT.

2.1 Who are the 'Subject Persons'?

The PMLFTR define subject persons as those persons, legal or natural, carrying out "relevant activity" or "relevant financial business".

'Relevant activity' is defined in the PMLFTR as:

"*… the activity of the following legal or natural persons when acting in the exercise of their professional activities:*

(a) auditors, external accountants and tax advisors, including when acting as provided for in paragraph (c);
(b) real estate agents;
(c) notaries and other independent legal professionals when they participate, whether by acting on behalf of and for their client in any financial or real estate transaction or by assisting in the planning or carrying out of transactions for their clients concerning the –
  (i) buying and selling of real property or business entities;
  (ii) managing of client money, securities or other assets, unless the activity is undertaken under a licence issued under the provisions of the Investment Services Act;
  (iii) opening or management of bank, savings or securities accounts;
  (iv) organisation of contributions necessary for the creation, operation or management of companies;
  (v) creation, operation or management of companies, trusts, foundations or similar structures, or when acting as a trust or company service provider;
(d) trust and company service providers;
(e) nominee companies holding a warrant under the Malta Financial Services Authority Act and acting in relation to dissolved companies registered under the said Act;
(f) casino licensees;
(g) gaming licensees; and
(h) any natural or legal person trading in goods, but only where a transaction involves payment in cash in an amount equal to ten thousand euro (€10,000) or more whether the transaction is carried out in a single operation or in several operations which appear to be linked." [27]

'Relevant financial business' is defined in the PMLFTR as:

"(a) any business of banking carried on by a person or institution who is for the time being licensed, or required to be licensed, under the provisions of the Banking Act;
(b) any activity of a financial institution carried on by a person or institution who is for the time being licensed, or required to be licensed, under the provisions of the Financial Institutions Act;
(c) any long term insurance business other than business of reinsurance carried on by a person or institution who is for the time being authorised, or required to be authorised, under the provisions of the Insurance Business Act;
(d) any insurance intermediary activities carried out by an insurance intermediary or by a tied insurance intermediary related to long-term insurance business which person or institution is enrolled or required to be enrolled under the provisions of the Insurance Intermediaries Act, other than a natural person who is registered or enrolled and acts on behalf of a tied insurance intermediary or a person or institution enrolled as a tied insurance intermediary

[27] Regulation 2 of the PMLFTR.

that does not collect premiums, or other amounts intended for the policyholder or the beneficiary;

(e) any long term insurance business other than business of reinsurance carried on by a person in accordance with the Insurance Business (Captive Insurance Undertakings and Captive Reinsurance Undertakings) Regulations, by a cell company in accordance with the provisions of the Companies Act (Cell Companies Carrying on Business of Insurance) Regulations or by an incorporated cell company and an incorporated cell in accordance with the provisions of the Companies Act (Incorporated Cell Companies Carrying on Business of Insurance) Regulations;

(f) investment services carried on by a person or institution licensed or required to be licensed under the provisions of the Investment Services Act;

(g) administration services to collective investment schemes carried on by a person or institution recognised or required to be recognised under the provisions of the Investment Services Act other than administration services provided by recognised incorporated cell companies in accordance with the Companies Act (Recognised Incorporated Cell Companies) Regulations;

(h) a collective investment scheme marketing its units or shares, licensed, recognised or notified, or required to be licensed, recognised or notified, under the provisions of the Investment Services Act; [28]

(i) any activity other than that of a retirement scheme or a retirement fund, carried on in relation to a retirement scheme, by a person or institution licensed or required to be licensed under the provisions of the Retirement Pensions Act and for the purpose of this paragraph, ''retirement scheme'' and ''retirement fund'' shall have the same meaning as is assigned to them in the Retirement Pension Act;

(j) any activity of a regulated market and that of a central securities depository authorised or required to be authorised under the provisions of the Financial Markets Act;

(k) safe custody services provided by any person or institution not covered under paragraph (a) or (f);

(l) any activity under paragraphs (a) to (k) carried out by branches established in Malta and whose head offices are situated outside Malta." [29]

Over the years, the categories of subject persons has continued to broaden as the sophistication of the money launderer or terrorist financier has continued to increase and as their patterns or trends have shifted from the more mainstream financial services providers to the less mainstream or non-financial. The last revision to the PMLFTR is no exception. Gaming licensees have, in fact, been added as a new category of subject persons (deemed to be carrying on a relevant activity) and even the threshold for natural or legal persons trading in goods where a transaction involves a payment in cash, has been decreased from €15,000 to €10,000 to, in effect, catch a broader number of operators. New additions have also been made to persons carrying out 'relevant financial business' which now also covers safe custody services even when provided by any person

[28] "Marketing its units or shares" means the direct or indirect offering or placement at the initiative of the collective investment scheme ("the scheme") or on behalf of the scheme, of units or shares in it, to or with investors. Thus, all schemes the units or shares in which are offered to or placed with investors, whether directly or indirectly, by the scheme itself or by other third parties on behalf of the scheme, are considered to be subject persons.

or institution other than those licensed or authorised under the Banking Act or the Investment Services Act.

2.2 Purpose of the Implementing Procedures

The purpose of the Implementing Procedures is to assist subject persons in understanding and fulfilling their obligations under the PMLFTR, thus ensuring an effective implementation of the provisions of the PMLFTR. When applying certain AML/CFT measures, a degree of proportionality and flexibility is envisaged. Therefore, subject persons have a degree of discretion in how they comply with AML/CFT measures, and on the procedures that they put in place for this purpose, which should be proportionate to the size, type and complexity of their business activities. The manner and extent to which this flexibility is to be exercised is explained in detail in different parts of these Implementing Procedures.

In essence, the Implementing Procedures are being issued in order to achieve the following purposes:

(a) To outline the requirements set out in the PMLFTR and other obligations emanating from the PMLA;
(b) To interpret the requirements of the above-mentioned laws and regulations and provide measures as to how these should be effectively implemented in practice, promoting the use of a proportionate risk-based approach;
(c) To provide industry-specific good practice guidance and direction on AML/CFT procedures; and
(d) To assist subject persons in designing and implementing systems and controls for the prevention and detection of ML/FT.

When considering the purpose of AML/CFT measures it is helpful to go back to basics and understand the *utility* and *purpose* of such measures. Broken down to their very basic elements, AML/CFT measures are intended to ensure the following:

(a) identification and verification of a customer and ultimate beneficial owner: ensures that the subject person knows who his customer and, where appropriate, the ultimate beneficial owner is and is sure that the person being dealt with is, in fact, who he purports to be; this in turn enables the subject person to let the FIAU know (where obliged to do so by law) who the person involved in any suspicious activity is;
(b) record keeping: ensures that the details of a customer relationship or transaction are preserved for eventual assessment by the FIAU and other law enforcement and relevant authorities, which in turn ensures that any suspicious transaction can be properly examined by the competent authorities, investigated and acted upon;
(c) suspicious transaction reporting: ensures that any suspicious transaction is brought to the FIAU's attention as required by law, to enable it to take the appropriate action. This is considered to be the most important AML/CFT obligation of all and it could be safely stated that other AML/CFT obligations are the means to detect and flag suspicious transactions; and

(d) training: ensures that a subject person's staff remain up to date on current legal obligations, money laundering and terrorist financing methods and trends, as well as on their own organisation's policies and procedures, amongst other things.

Of course other obligations also exist in terms of applicable law and these Implementing Procedures, all of which have a useful function to fulfil, but the above main obligations help one appreciate the important role that subject persons have in the fight against ML/FT. They also emphasise the fact that ultimately both the FIAU and subject persons are on the same side of the fence when it comes to the fight against ML/FT.

The primary consideration in applying AML/CFT measures should be the extent of the ML/FT risks to which the subject person in question may be prone or exposed. As a general rule, subject persons are required to assess, understand and manage their ML/FT risks in the most appropriate and proportionate manner. Subject Persons must address their management of risk in a thoughtful and considered way, and establish and maintain systems and procedures that are appropriate, and proportionate to the risks identified in order to achieve the intended purpose of the PMLFTR and these Implementing Procedures. The Implementing Procedures also seek to assist subject persons in achieving this objective within the parameters of the law.

2.3 Status and application of the Implementing Procedures

These Implementing Procedures are being issued in terms of Regulation 17 of the PMLFTR, which empowers the FIAU to issue such procedures and guidance for the carrying into effect of the provisions of the PMLFTR. In accordance with this regulation, these Implementing Procedures are legally binding on all subject persons and are not merely consultative.

The Implementing Procedures set out what is expected of subject persons and their staff in relation to the prevention of ML/FT by providing an interpretation as to how the PMLFTR are to be effectively implemented in practice and by indicating what the FIAU expects from subject persons when implementing their obligations at law. In view of this, subject persons should be aware that failure to comply with such procedures may render subject persons liable to the imposition of administrative sanctions.

The Implementing Procedures are divided into two parts. Part I is applicable to all sectors falling within the definition of 'relevant activity' and 'relevant financial business'. Part II, on the other hand, constitutes the more specific sectoral guidance that applies to each sector specifically, and must necessarily be read in conjunction with Part I of the Implementing Procedures. By adopting this method, it is possible for particular sectors to have implementing procedures that are tailor-made to the realities of their industry and to take into account any specific matters that it may not be possible to address comfortably or properly by rules that are of a more general application.

From time to time the Implementing Procedures may be amended to ensure that they remain harmonised with amendments to legislation and other material developments originating from changes in international standards, especially those emanating from the FATF and EU AML

Directives and Regulations. Subject persons should therefore ensure that they adhere and refer to the most recent version of the Implementing Procedures.

A reading of the Implementing Procedures should, of course, not be a substitute for a reading of the PMLFTR and the PMLA themselves, besides the relevant provisions of the Criminal Code dealing with terrorist financing and related offences. Moreover, this document should not be used as an internal procedures manual or as an exhaustive checklist of steps to be taken when complying with AML/CFT obligations.[30]

The Implementing Procedures are binding on subject persons as from the date on which they are issued.

[30] Cap. 9 of the Laws of Malta.

CHAPTER 3 – THE RISK BASED APPROACH

The PMLFTR oblige subject persons to adopt and implement a series of measures, policies, controls and procedures to prevent the financial system or other systems from being abused for ML/FT. However, the PMLFTR also recognise that the risk of ML/FT may vary from one sector to another, from one subject person to another as well as from one business relationship, or occasional transaction, to the other.

Therefore, to ensure that the AML/CFT measures, policies, controls and procedures adopted are truly effective, the PMLFTR require subject persons to implement the same on a **risk-sensitive basis** through the adoption of a **risk-based approach**. This means that subject persons must identify and assess the ML/FT risks they are exposed to, and vary and adapt the said measures, policies, controls and procedures in a way that ensures that resources are applied where most needed, i.e. where the subject person determines that it is exposed to a higher than normal risk of ML/FT.

3.1 Notions of Risk

The effectiveness of the risk-based approach depends on the proper understanding of the ML/FT risk to which a subject person is exposed. **Risk** is here understood as being **inherent risk**, i.e. the risk one is exposed to prior to adopting and applying any measures, policies, controls and procedures to mitigate the same.

To assess risk, it is therefore necessary to understand how risk can manifest itself having regard to one's:

(a) **vulnerabilities**, i.e.: the weaknesses which may be exploited for ML/FT purposes; and
(b) **threats**, i.e.: the external elements that seek to exploit a subject person's vulnerabilities.

Regard must therefore be had to **risk factors**, i.e. those variables that either on their own or in combination with each other may increase or decrease the ML/FT risk posed to a subject person.

Identification of ML/FT risk has to be followed by an assessment of the same by considering the **likelihood** of risk manifesting itself and the **impact** any such manifestation would have on the subject person. Impact consists in the nature and seriousness of the damage occasioned if a threat manages to exploit one or more vulnerabilities, and it can take a number of forms including reputational risk, business risk, regulatory risk, legal risk, financial loss and others. **Likelihood** and **impact** will lead to the determination of the level of **inherent risk** a subject person is exposed to.

Determining the likelihood and impact of risk will highlight the areas where a subject person's mitigating measures, i.e. its AML/CFT measures, policies, controls and procedures, need to be the strongest so as to mitigate the level of inherent risk identified. To evaluate the effectiveness of one's AML/CFT measures, policies, controls and procedures, one has to look at what level of risk

is left after applying the said measures, policies, controls and procedures to the level of inherent risk it has identified. Any risk left is termed the **residual risk**.

Thus:

Level of Inherent Risk – Mitigating Measures = Level of Residual Risk

It is acknowledged that independently of the measures, policies, controls and procedures adopted, there will remain a degree of ML/FT risk that cannot be addressed, avoided or controlled.

At this stage, a subject person has to consider whether the residual risk falls within its **risk appetite**, i.e.: whether the subject person is prepared to accept that level of residual risk in the pursuit of its business objectives. Risk appetite is set through a simple consideration on the part of the subject person: Does the subject person deem it worthwhile to carry out activities in an environment where the likelihood of risk materialising itself and the resulting impact are high, or is it preferable to minimise as much as possible the possibility of risk actually materialising itself and effecting the subject person's activities?

Where the residual risk falls outside one's risk appetite, and to the extent that it may be possible, the mitigating measures applied have to be revisited so as to further strengthen their efficacy in preventing the materialisation of risk and reduce the residual risk within acceptable parameters. Alternatively, the subject person would only be able to control risk through desisting from pursuing that particular activity.

While risk appetite is an expression of one's risk tolerance, it is important to remember that this leaves unaffected one's obligations at law. Independently of a subject person's willingness to expose itself to risk, the subject person has to bear in mind that this may lead to supervisory and/or law enforcement action.

3.2 Risk Factors

The risk-based approach hinges on two aspects, namely an understanding of the risks one is facing and, based on this understanding of risk, the variation of one's controls, policies, measures and procedures so as to achieve the strongest mitigating effect possible. This calls not only for an assessment of risk that takes into consideration one's business as a whole but also for an assessment of risk that is more focused on individual business relationships or occasional transactions. While the former risk assessment is referred to as the '**business risk assessment**', the latter is known as the '**customer risk assessment**'.

In both instances, the assessment of the inherent risks will depend on identifying the threats and vulnerabilities that one is exposed to. This can be done by considering those areas from which risk may manifest itself, i.e. the risk factors. In determining what these risk factors are, subject persons are to refer to Regulation 5(1) of the PMLFTR which makes reference to "***risk factors***

including those relating to customers, countries or geographical areas, products, services, transactions and delivery channels".

The hereunder is intended to provide subject persons with guidance on some of the main risk factors falling within each of these categories, but should in no way be considered as being exhaustive. The risk factors a subject person may be exposed to will vary depending on the nature and size of its business, understood as being both its structures and systems, as well as its actual activities. While some of these risk factors will be applicable both in the context of the business risk assessment and in that of the customer risk assessment, other factors may have more relevance when carrying out the business risk assessment rather than the customer risk assessment, and *vice versa*.

3.2.1 Customer Risk

Customer Risk is the risk of ML/FT that arises from entertaining relations with a given person or entity due to (a) the business or professional activity; (b) the reputation; (c) the nature of the entity and the behaviour of the said person or, where applicable, of its beneficial owner. Possible risk factors include:

(a) Business or Professional Activity – Some business or professional activities from which the customer or the beneficial owner, if applicable, are deriving their wealth or the funds to be used in the course of a business relationship or an occasional transaction are to be considered as presenting a high risk of ML/FT.

These include:

(a) The activity pursued is cash (or cash equivalent) intensive;
(b) The activity is commonly associated with a higher risk of corruption (e.g.: the arms trade and defence industry, the mining industry etc.);
(c) The activity is associated with a higher risk of ML/FT (virtual currencies, money remittance etc.);
(d) The activity is conducted through opaque and complex structures for which there does not seem to be a legitimate justification;
(e) The customer is an asset holding vehicle;
(f) The customer has benefitted from citizenship or residency by investment schemes or is a prospective applicant for such as scheme;
(g) The individuals involved in the activity pursued include PEPs or individuals having otherwise prominent public positions which may be equally exploited for one's own personal advantage.

On the other hand, there are activities that can be considered as presenting a lower than usual risk of ML/FT.

These include:

(a) Entities listed on a regulated market and subject to enforceable disclosure requirements which ensure adequate transparency of beneficial ownership;
(b) Entities carrying out relevant financial business or equivalent activities subject to equivalent AML/CFT obligations as those applicable in Malta and which are subject to effective supervision;
(c) Entities forming part of the public administration or public enterprises.

While subject persons can consider the above as posing a low risk of ML/FT, it is important to stress that this should not be a foregone conclusion. Subject persons have to consider whether these entities have been the subject of supervisory action or, in the case of public administration entities, what is the level of corruption in the particular jurisdiction. In the presence of these additional circumstances, it would no longer be possible to consider any of the above as presenting a low risk of ML/FT.

Subject persons should also consider the extent of the difficulty encountered to establish the actual business or professional activity of the customer or its beneficial owner, and how consistent the information obtained or provided is when compared with their former, current or planned business activity, their business' turnover, and so on.

(b) Reputation

Subject persons should consider whether a customer or its beneficial owner has been subject of adverse reports linking him to crime (especially financial crimes) and/or terrorism. The absence of an arraignment or of a conviction should not be automatically taken to mean that any adverse reports can be ignored. Subject persons are expected to consider how reliable these reports are on the basis of the quality and independence of their source/s, and how persistent these reports are.

Subject persons need also to consider what is known about a (prospective) customer and its beneficial owner through official means (e.g.: criminal convictions, assets seizures, sanctions etc.) as well as internally through previous dealings with the same. For example anyone who has been the subject of a STR should be considered as representing a high risk of ML/FT.

(c) Nature and Behaviour

The behaviour of a customer or of a beneficial owner, as well as the way an entity which seeks the services of a subject person is structured, may in itself be indicative of a high risk of ML/FT. The following are among the risk factors that should be considered as indicative of high risk:

(a) The customer or the beneficial owner is reluctant to provide any documentation and/or information requested by the subject person without a legitimate reason for doing so;
(b) The documentation presented to meet a subject person's request for information/documentation gives rise to doubts as to its veracity or authenticity;

(c) The customer is avoiding the establishment of a business relationship, preferring instead to carry out several one-off transactions without there being any economic justification for doing so;
(d) The customer or its ownership and control structure involve bearer shares or nominee/fiduciary shareholders;
(e) There are material changes to the customer's ownership and control structure for which there does not seem to be a legitimate rationale;
(f) The customer requests transactions that are complex, unusually or unexpectedly large or have an unusual or unexpected pattern without an apparent economic or lawful purpose or a sound commercial rationale;
(g) The customer requests unnecessary or unreasonable levels of secrecy;
(h) The customer is non-resident and there is no sound economic and lawful reason for seeking services or products from the subject person; and
(i) The customer is a voluntary organisation which primarily engages in raising or disbursing funds for charitable, religious, cultural, educational or social purposes (especially when they remit funds to third countries), and hence its activities are particularly susceptible to be abused for funding of terrorism.

3.2.2 Geographical Risk

Geographical risk is the risk that arises from links with one or more geographical areas, usually related to those jurisdictions (a) where the customer or its beneficial owner are based or have their main place of business or where the activity generating the customer's or beneficial owner's wealth is carried out; and/or (b) with which the customer or its beneficial owner have relevant personal links (for example an individual's residence or a jurisdiction with which a particular entity has strong trading or financial connections).

The factors that a subject person has to consider when determining whether a geographical area poses a higher risk of ML/FT include:

(a) Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
(b) Countries identified by other credible sources as having serious deficiencies within their AML/CFT framework (e.g.: FATF, FSRBs like MONEYVAL, IMF etc.);
(c) Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations Security Council or the European Union. In addition, in some circumstances, countries subject to sanctions or measures which may not be universally recognised (e.g.: OFAC sanctions) should be given credence by the subject person because of the standing of the issuer and the nature of the measures;
(d) Countries identified by credible sources as providing funding or support for terrorist activities or that have terrorist organisations operating within them;

(e) Countries identified as having significant levels of corruption or other criminal activity through credible sources like the Corruption Perception Index compiled by Transparency International;[31]
(f) Countries which have shown a lack of willingness to comply with international tax transparency and information sharing standards (e.g.: failure to adhere to or apply the Common Reporting Standard);
(g) Countries which fail to implement effective beneficial ownership transparency and availability measures and hence allow the legal entities or arrangements set up in such a jurisdiction to be used as secretive vehicles and abused for ML/FT purposes.

Membership of regional or international bodies such as the FATF and MONEYVAL is not to be taken to mean that the country necessarily presents a low risk of ML/FT. The same applies to countries which are missing from international black or grey lists, as it may well mean that a country has still to be evaluated or that the failures identified, which may be in key areas and of relevance to the subject person, were not sufficient to result in its listing.

The relative importance of the geographical risk will at times be dependent on the nature and purpose of the business relationship or occasional transaction. Thus, in situations where the funds to be used have been generated abroad, the subject person should pay attention to the levels and types of criminal activities occurring in the jurisdiction of origin. On the other hand, if the service or product allows for the remittance or transfer of funds to third countries, funding of terrorism would be a more important aspect to consider and hence one should scrutinise the jurisdiction of destination for any known concerns with terrorism or terrorist groups.

3.2.3 Product, Service and Transaction Risk

The product, service or transaction risk is the risk one is exposed to as a result of providing a given product or service, or carrying out a particular transaction. Much will depend on (a) the level of transparency or opaqueness that the product, service or transaction affords; (b) the complexity of the product, service or transaction; and (c) the value or size of the product, service or transaction.

(a) Transparency

Products or services that allow the customer or the beneficial owner to remain anonymous or facilitate hiding their identity are to be considered as presenting a higher risk of ML/FT than other products or services. These include products like nominee or omnibus accounts and services like investments in non-financial assets, and fiduciary and trustee services. The ability of a third party to give instructions even though not a party to the business relationship should also be factored in.

(b) Complexity

[31] The Corruption Perception Index is available through the website of Transparency International - https://www.transparency.org/

The risk of a product or service is commensurate to the complexity of the transactions that can be carried out by making use of the same. A product or service allowing the carrying out of international transactions involving multiple parties and multiple jurisdictions as can be the case in trade finance is to be considered as presenting a higher risk than a product or service used to carry out regular transactions involving amounts that are constant and the source of which is known such as an account to receive social security benefits or salaries only.

(c) Value and Size

A product or service which is cash intensive is to be considered as presenting a higher risk than other products which cannot be so funded. Regard should also be had to whether the product or service allows high-value transactions to take place. A payment instrument or an account without any limits or capping presents a higher risk than a similar instrument or account which applies the same, though regard has to be had to how high any such limits or capping are.

Subject persons should here also consider how funding is to be made available by the subject person as some payment methods allow a higher degree of anonymity than others (e.g. cash, pre-paid cards, virtual currencies etc.).

3.2.4 Delivery Channels Risk

The delivery channel, or interface risk, is the risk arising from how the subject person interacts with the customer and the channels it uses to provide a given product or service. Interacting with customers on a non-face to face basis presents a high risk of ML/FT unless the subject person has adopted technological means within its systems to address the risk of impersonation or identity fraud.

The same applies where these relations with the customer are entertained through multiple layers of intermediaries. Subject persons have to consider the reliability of these intermediaries and the standards of AML/CFT they are subject to. The same applies where a customer is recommended by an introducer or another entity forming part of the same entity. This is especially true in those instances where the subject person exercises reliance thereon as provided for in terms of Regulation 12 of the PMLFTR.

3.2.5 Additional Risk Factors

Through the wording adopted in Regulation 5(1) it is clear that the above risk factors are not exhaustive, thus a subject person has to consider whether there are additional risk factors that would need to be considered. One example would be outsourcing; that is, delegating the implementation of parts of one's AML/CFT measures, policies, controls and procedures to a third party service provider. Doing so introduces an additional variable as the subject person will be

dependent on the reliability and quality of work of the service provider to obtain the necessary information on which to base its decisions, including information that may influence the subject person's risk assessment and changes thereto.

It is also important to note that risk factors are not static and it is possible that a subject person will have to consider additional or new risk factors as time goes by. The environment within which they carry out their respective activities as well as their relations with their customers will inevitably evolve, leading to the emergence of risk factors which were not previously considered.

3.2.6 Sector Specific Risk Factors

Subject persons carrying out one or more specific relevant activities and/or relevant financial business will be exposed to particular risk factors. It is therefore imperative that subject persons consider any risk factors that may be peculiar to their particular area of activity. In particular, subject persons have to consider:

(a) Any risk factors that may be highlighted by the FIAU in any sector specific Implementing Procedures that the FIAU may issue from time to time; and
(b) The Risk Factors Guidelines issued by the European Supervisory Authorities ("ESAs") on 4 January 2018 in so far as these may be applicable to them. These Guidelines contain sections setting out risk factors particular to activities which in terms of the PMLFTR constitute "relevant financial business". Thus, anyone carrying out any relevant financial business referred to in the said document and is assessing its ML/FT risk, is to also consider any sector specific risk factors referred to in the said document.

The Risk Factor Guidelines are available on the ESAs' website - https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_EN_04-01-2018.pdf .

3.2.7 Sources of Information

In determining the risk factors that subject persons are to consider as well as any change thereto, subject persons can avail themselves of a large body of information. The PMLFTR themselves oblige subject persons to consider any supranational risk assessment (i.e. the Supranational Risk Assessment carried out by the European Commission)[32] as well as any national risk assessment.

Apart from these assessments, a subject person would also be expected to consult and make use of:

(a) Any relevant reports issued by the FATF, MONEYVAL and other FSRBs;
(b) Reports, typologies and other information made available by FIUs or law enforcement agencies;

[32] The Supranational Risk Assessment is available on the website of the European Commission - http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272

(c) Information, reports and guidance made available by the ESAs and competent authorities;
(d) Information from industry or professional bodies;
(e) Information from civil society, such as corruption indices and country reports;
(f) Information from international standard-setting bodies such as mutual evaluation reports or legally non-binding blacklists;
(g) Information from credible and reliable open sources, such as reports in reputable newspapers;
(h) Information from credible and reliable commercial organisations, such as risk and intelligence reports; and
(i) Information from statistical organisations and academia.

Subject persons can also make use of what experience they may already have in providing their services and/or products.

3.3 The Business Risk Assessment

A Business Risk Assessment is a process whereby the subject person identifies the threats and vulnerabilities that it is exposed to and assesses the likelihood and impact of ML/FT risks. On the basis of this assessment, it will be able to determine which areas to prioritise in terms of AML/CFT and ensure that its AML/CFT measures, policies, controls and procedures are commensurate to the ML/FT risks it faces so as to mitigate the same.

The Business Risk Assessment is therefore the foundation of the risk-based approach and the PMLFTR impose an obligation on the subject person to "***take appropriate steps, proportionate to the nature and size of its business, to identify and assess the risks of money laundering and funding of terrorism that arise out of its activities or business***." Subject persons forming part of a group are also expected to carry out their individual Business Risk Assessment. While a group can carry out a group-wide risk assessment, this cannot be relied upon blindly by the subject persons forming part of the same, without considering whether such a risk assessment is comprehensive enough to cover all its activities and operations.

3.3.1 The Basic Steps

The identification of the threats and vulnerabilities one is exposed to requires a consideration of the risk areas and risk factors referred to in Section 3.2 above both from a qualitative and quantitative point of view. Thus, for the purposes of the Business Risk Assessment, it is not sufficient for the subject person to merely draw up an inventory of the threats or vulnerabilities but it also has to consider how numerous these threats or vulnerabilities are along the following lines:

(a) Customer Risk:

- Number of customers within each risk factor;
- Maturity of the client base, i.e. the duration of existing business relationships;

- Volume of business.

(b) Geographical Risk:

- Number of subsidiaries or branches within a given jurisdiction;
- Number of customers and/or beneficial owners from a given jurisdiction;
- Number of transactions to/from a given jurisdiction;
- Number of trade finance relationships;
- Number of correspondent banking relationships.

(c) Products, Services and Transaction Risk:

- Number of products, services and transactions;
- Customers per each product and service;
- Volume per product and service.

(d) Delivery Channel:

- Number of relationships started on a non-face to face basis;
- Number of introducers and intermediaries;
- Number of customers introduced through introducers and intermediaries.

Existing subject persons will have to examine their current business structures, client-base and portfolio of services and products as well as any diversification or expansion plans they may have. On the other hand, prospective subject persons will have to look at how they intend to structure their business, which markets they intend to target, what services or products they are to offer and any estimates made.

Doing so should allow a subject person to identify the various risk factors that it is to take into consideration for its Business Risk Assessment. The combination of these risk factors will allow the subject person to identify the threats it is exposed to and the vulnerabilities that may be exploited for ML/FT purposes. Having done so, the subject person has to determine the likelihood of any one scenario materialising itself, and the possible impact thereof. Taken together, likelihood and impact will lead to one's inherent risk. While it is left to the individual subject person to determine how to do so, the following set of tables is one of the possible options that a subject person may adopt based on scales.

A **Likelihood Scale** refers to the potential of an ML/FT risk occurring in the subject person's business for the particular risk being assessed. Four levels of risk are shown in Table 1, but a subject person can have as many as it believes are necessary.

Table 1 – Likelihood scale

Likelihood Scale Frequency	Likelihood of ML/FT Risk
4- Extreme	Can occur several times a year – very high chance
3- High	Can occur a few times a year – reasonable chance
2- Medium	Can occur once a year – small chance
1- Low	Can occur less than once a year – very unlikely

An **Impact Scale** refers to the seriousness of the damage (or otherwise) which could occur should the event happen (and the risk, therefore, materialises). Four levels of risk are shown in Table 2, but a subject person can have as many as it believes are necessary.

Table 2 – Impact scale

Consequence	Impact – of ML/FT Risk
4- Extreme	Severe loss or damage, heavy supervisory action – long-term effect
3 – High	Large loss or damage, supervisory action – medium-term effect
2 – Medium	Limited loss or damage, minor supervisory action – short-term effect
1 – Low	Negligible loss or damage, no supervisory action – no effect

Taken together, the subject person will be able to determine the level or degree of **inherent risk** it is exposed to:

Table 3 – Inherent Risk

IMPACT / LIKELIHOOD	1	2	3	4
1	**Low Risk**	**Low Risk**	**Moderate Risk**	**High Risk**
2	**Low Risk**	**Low Risk**	**Moderate Risk**	**Extreme Risk**
3	**Moderate Risk**	**Moderate Risk**	**High Risk**	**Extreme Risk**
4	**High Risk**	**High Risk**	**Extreme Risk**	**Extreme Risk**

Having determined the inherent risk, the subject person has to then consider what measures, policies, controls and procedures it already has in place or it plans to adopt, and establish how effective these are in mitigating the inherent risk. In so doing, a subject person has to consider regulatory guidance as well as its own experience (e.g.: internal audit reports, compliance reports, incidents that may have already led to supervisory action). In particular, subject persons are to ensure that to the extent applicable to them, they consider adopting the mitigating measures referred to in the ESAs' Risk Factor Guidelines referred to in Section 3.2.6 above.

Effectiveness can be rated using a scale akin to the ones used to rate likelihood and impact.

Table 4 – Effectiveness

Level of Mitigation	Description of Effectiveness
4- Strong	There are several measures in place to control risk which are fully operational and fully effective
3 – Effective	Risk is managed adequately but could be improved in certain parts – mitigating measures work adequately and are effective
2 – Ineffective	Risk is not managed adequately, substantial improvement necessary but has some effect
1 – Non-Existent	No controls or controls are ineffective

Considering the inherent risk level in light of the effectiveness score will enable the subject person to determine the residual risk.

Example: Low inherent risk & ineffective level of mitigation = low or medium residual risk
High inherent risk & ineffective level of mitigation = high residual risk

It is important to note that the effectiveness of one's measures will leave the inherent risk unchanged; independently of how effective a mitigating measure may be, a high risk situation will remain high risk.

The residual risk will allow a subject person to determine whether it is able to tolerate the same as it falls within its risk appetite, or whether it needs to take further remedial action; that is, either taking additional measures to further mitigate the risk and bring it within acceptable levels, or to decline pursuing that particular business in its entirety.

3.3.2 Carrying out the Business Risk Assessment

The Business Risk Assessment, changes thereto, and any connected decision have to be duly documented to evidence that an appropriate review has taken place, and are to be made available to the FIAU and supervisory authorities upon demand.

All the aspects of the Business Risk Assessment should be covered, including:

(a) the methodology adopted by the subject person;
(b) the reasons for considering a risk factor as presenting a low, medium or high risk;
(c) the outcome of the Business Risk Assessment, including the measures, policies, procedures and controls adopted to mitigate the identified risks; as well as
(d) any information sources used.

The same applies to any change made to the Business Risk Assessment from time to time

The Business Risk Assessment has to be proportionate to the nature and size of a subject person's business, i.e.: both the nature and size of a subject person's systems and structures, as well as the nature and size of its activities.

A subject person with a large business conducted through multiple branches, agencies and subsidiaries is less likely to know its clients personally and it could offer a greater degree of anonymity than a small business. The same applies with a business that conducts complex transactions across various jurisdictions, which could offer greater opportunities to money launderers than a purely domestic business. Thus, the more complex the activities of a subject person, the more sophisticated its risk assessment is expected to be. Conversely, a subject person that does not offer complex products, services or transactions, and with limited or no international exposure, will not require a complex or sophisticated assessment.

To the extent applicable, the Business Risk Assessment, revisions thereof, as well as any decision taken in relation thereto, have to be approved by the Board of Directors or equivalent management body of the subject person. Even such approval has to be properly documented (e.g.: through Board minutes or resolutions). Naturally such an obligation applies in the case of subject persons that are entities, firms or similar arrangements, but would not apply in the case of sole-practitioners which would themselves be responsible for the implementation and carrying out of appropriate business risk assessments.

In terms of the PMLFTR, each subject person is responsible for having its own Business Risk Assessment. However, this does not necessarily mean that the subject person has to draw it up itself, since subject persons are free to engage external consultants to assist them or to carry out the Business Risk Assessment on their behalf. To ease the regulatory burden on subject persons, it is also possible for subject persons carrying out a specific relevant activity or a specific relevant financial business to adopt as their own a sectoral Business Risk Assessment prepared by an industry representative body.

In the circumstances described above, subject persons are to remember that they remain responsible to ensure that the Business Risk Assessment is at all times current and reflects their actual circumstances. Hence, when relying on a standard sectoral Business Risk Assessment or engaging a consultant, subject persons are to ensure that they review the Business Risk Assessment and the methodology being used to ensure that it always reflects their actual activities and specificities. Similarly, to the extent that may be applicable, the Board of Directors or equivalent body will retain responsibility to endorse and approve the Business Risk Assessment, and to also update it as may be necessary from time to time.

Moreover, the possibility does exist that subject persons carrying out a particular relevant activity or a relevant financial business may be exempt from carrying out a Business Risk Assessment. This is, however, a sectoral exemption, and not an individual exemption, and depends on the FIAU granting said exemption as provided by Regulation 5(2) of the PMLFTR on the basis of a nationwide risk assessment, whether it is all-encompassing or sectoral, which clearly sets out what the ML/FT risks to which the given sector is exposed are.

An exemption is intended to be granted where the risks are shown to be known and uniform throughout a sector, meaning that all business relationships or transactions will present the same risk or that risk will materialise itself where specific factors materialise themselves. In such circumstances, the FIAU may provide for the said exemption and the conditions governing the same through an Interpretative Note or sector-specific Implementing Procedures.

3.3.3 Timing of the Business Risk Assessment

The general principle is that in respect of subject persons who are still to undertake a relevant activity or a relevant financial business, the Business Risk Assessment is to be carried out prior to the commencement of activity on the basis of the kind of services, products or transactions it intends to offer, the markets it intends to target, the technologies it will use to deliver the same, and its intended business model and activities. Eventually the Business Risk Assessment would have to be revised as set out in Section 3.3.4 hereunder.

Existing subject persons may be said to be better placed to carry out a Business Risk Assessment than new subject persons. Through their experience and on the basis of internal reports and/or other compliance findings, existing subject persons may already be aware of the areas where they are most vulnerable and the main threats they face when it comes to ML/FT. Moreover, existing clients may easily provide a benchmark as to what the expected level of activity is, making it easier for them to set thresholds to identify activity that is unusual and that may be indicative of a higher risk of ML/FT. Thus, existing subject persons should have more concrete data on the basis of which to carry out a Business Risk Assessment or to revise any such assessment they may have already conducted prior to the coming into force of the PMLFTR to ensure it complies with the new requirements at law.

3.3.4 Revising the Business Risk Assessment

Regulation 5(4) of the PMLFTR lays down that a Business Risk Assessment *is regularly reviewed and kept up-to-date*. This requirement stems from the very nature of risk, which is not static but evolves continuously in view of external changes as well as changes in the activities or services of the subject person.

A subject person is therefore required to revise its Business Risk Assessment:

(a) **Whenever new threats and vulnerabilities are identified:** it is possible that in the carrying out of its activities, the subject person will become aware of risks that it did not factor in during its original Business Risk Assessment. Information may also become available that new threats have arisen that are exploiting certain vulnerabilities.

(b) **Whenever there are changes to its business model/structures/activities**: the changes that may require a revision of the Business Risk Assessment are many. The mere increase in the number of clients serviced may be sufficient in itself to expose a subject person to a higher risk of ML/FT than originally considered. The same applies if new markets are ventured into, be it through an increase in the portfolio of services, products or transactions offered or the targeting of new customer segments and/or jurisdictions. The use of new technologies in delivering services, products or affecting transactions may also increase the possibility of ML/FT. Moreover, the adoption of new technologies may also impact the ability of the subject person to fulfil its AML/CFT obligations, increasing the operational and legal risks to which the subject person is usually exposed.

Where a revision of the Business Risk Assessment is occasioned through planned changes to be implemented by the subject person, the revision should take place prior to any such change being implemented. This will enable the subject person to understand whether this change will heighten the ML/FT risk it is exposed to and ensure that any necessary action is taken to adequately address the change in risk.

(c) **Whenever there are changes to the external environment within which the subject person is operating**: these may be brought about by, for instance, regulatory changes and developments in technologies creating new threats.

(d) **On an annual basis**: the absence of any event provided for above does not mean that the Business Risk Assessment does not require periodical review. Subject persons should consider on an annual basis whether there have been any other changes which may affect the reliability and relevance of its Business Risk Assessment. If it is found that there is no need to change or alter the Business Risk Assessment, a note should be kept stating that following a review of the Business Risk Assessment it was determined that it was still current and valid, without requiring any updates. Subject persons are not expected to repeat the assessment annually but to consider at least

on an annual basis whether there exists a basis for revision in order to always keep it up to date.

3.4 Mitigating Measures, Policies, Controls and Procedures

Once a subject person has identified the ML/FT risks it is exposed to through the Business Risk Assessment, it has to take measures to prevent these risks from materialising or at least mitigate their occurrence as much as possible. This is reflected in the obligation arising from Regulation 5(5) of the PMLFTR which lays down that a subject person must have in place and implement measures, policies, controls and procedures to address the said risks identified as a result of the Business Risk Assessment.

These measures, policies, controls and procedures are to include:

(a) CDD, record-keeping procedures and reporting procedures as further explained in these Implementing Procedures; and

(b) Risk management measures, including customer acceptance policies, internal control, compliance management, communications, and employee screening policies and procedures.

It is important that any measures, policies, controls and procedures be clearly documented and, where applicable, approved by senior management. This applies not only to the initial measures, policies, controls and procedures adopted by the subject person but to any subsequent revision of the same. Where changes to any such measures, policies, controls and procedures are intended to address a variation in ML/FT risks caused through a planned change in the subject person's activities, it is important that the revised measures, policies, controls and procedures be in place prior to the planned change/s taking place.

The complexity of these measures, policies, controls and procedures will depend on the nature and size of the subject person's business and activities. Again, the subject person must factor in the complexity of its internal structure including the use of branches or agencies if any; the range and complexity of the services/products it offers or transactions it effects; the number and nature of its clients and its employees; the distribution channels it makes use of; and the technological resources it has at its disposal.

The effectiveness of any such measures, policies, controls and procedures will inevitably depend on their proper application throughout the subject person's business structures. It is therefore imperative that a subject person takes the necessary steps to inform its officers and employees about the same and how they are to be applied internally.

Their effectiveness will become apparent through their application in the day-to-day operations of the subject person. It is therefore imperative that a subject person monitors, on an ongoing basis, how the same are applied. This will allow a subject person to determine their effectiveness, and identify and address, in a timely manner, any shortcomings thereof. Moreover, additional

risks may be identified which may contribute to further strengthen one's Business Risk Assessment.

The PMLFTR themselves lay considerable emphasis on the need to conduct ongoing monitoring of one's measures, policies, controls and procedures. They not only require that the subject person identifies, where applicable, a member of its management body who is to be responsible for the overall adoption of the same but they also require the subject person to consider whether, given the size and nature of its business, this ongoing monitoring function needs to be strengthened through:

(a) The appointment of an officer at management level whose duties are to include monitoring of the day-to-day implementation of the measures, policies, controls and procedures adopted by the subject person; and

(b) The implementation of an independent audit function to test the said internal measures, policies, controls and procedures from time to time.

The latter need not necessarily result in the creation of an internal audit function, as it is possible for the subject person to engage an external consultant independent of the subject person to evaluate the adequacy of its internal controls, policies and procedures. Alternatively the subject person may assign this task internally to a person other than the MLRO or anyone else involved in the implementation or operation of the subject person's AML/CFT compliance programme.

3.4.1 The Customer Acceptance Policy

As part of the measures, policies, controls and procedures that the subject person is to implement, it is especially important that it adopts and applies a Customer Acceptance Policy. This policy is to provide a description, with non-exhaustive examples, of the type of customers that are likely to pose a higher than average risk of ML/FT; the risk indicators which will lead to a business relationship or an occasional transaction being considered as presenting a low, medium or high risk of ML/FT; the level and nature of CDD measures, including ongoing monitoring, to be applied in relation thereto; and under what circumstances the subject person will decline to service someone.

When drawing up their Customer Acceptance Policy, subject persons are to remember their obligation in terms of Regulation 11(5) of the PMLFTR whereby their risk management procedures must be conducive to determining whether a customer or its beneficial owner is a PEP and the measures to be undertaken whenever a PEP is identified. This can also be included within the Customer Acceptance Policy.

3.5 The Customer Risk Assessment

A subject person will only be able to apply its Customer Acceptance Policy once it has understood the risk inherent in entering a particular business relationship or carrying out an occasional

transaction. To this end, the subject person has to carry out a Customer Risk Assessment, i.e.: an assessment of the particular risks it will be exposed to in providing its services or products, either in the course of a business relationship or as a one-off event (i.e.: occasional transaction), to specific customers linked to particular jurisdictions through one or more channels. The information collected to draw up the Customer Risk Assessment is the customer's **risk profile**.

On the basis of the Customer Risk Assessment, CDD can then be applied as stipulated in the Customer Acceptance Policy and in a manner that addresses the identified risks effectively. This is why the Customer Risk Assessment has to be carried out prior to the subject person entering into a business relationship or carrying out an occasional transaction.

Care has to be exercised, as identifying a customer as presenting a higher risk of ML/FT does not automatically mean that the customer is involved in ML/FT. Similarly, identifying a customer as carrying a lower risk of ML/FT does not mean that the customer presents no risk at all. A subject person, its officers and employees need to remain vigilant at all times.

The process followed to carry out the Customer Risk Assessment is to form part of the measures, policies, controls and procedures adopted by the subject person and already referred to in Section 3.4.1 above. The level of detail of a Customer Risk Assessment is to reflect the complexity of the business relationship or occasional transaction to be entered into. The more complex the relationship or transaction, the more structured and rigorous the Customer Risk Assessment should be to show that the risk assessment took account of all the circumstances involved rather than being based on a generic or categorised basis. On the other hand, where the relationship or transaction is fairly simple and straightforward, a subject person may use standardised profiles where these are proven to effectively assess the risks of ML/FT.

When assessing the risks posed by a customer, the subject person should consider all risk factors that are known, including those referred to under Section 3.2 above, and ensure that all of these factors are included in the customer's risk profile, taking care to ensure that any mitigating factors applied are fully documented. A subject person must be able to objectively and reasonably justify a Customer Risk Assessment classification and document those justifications.

Where a customer has been identified as posing a higher risk of ML/FT and the relevant person is not satisfied that it is able to effectively mitigate those risks, the relevant person shall consider desisting from entering into a business relationship with or carrying out an occasional transaction for that customer. Where such risks give rise to a suspicion of ML/FT, then an internal disclosure must be made to the MLRO or the designated employee.

3.5.1 Timing of the Customer Risk Assessment

The Customer Risk Assessment is to be carried out whenever a new business relationship is to be entered into or an occasional transaction is to be carried out. However, given that risk is dynamic, it is important that in the case of a business relationship the Customer Risk Assessment be reviewed from time to time depending on the risk presented by the particular business relationship, and especially where there is an event marking a material departure from the business and risk profile of the customer which may be noted through the ongoing monitoring of

transactions (e.g.: a client acquires a new service or product). A revision of a customer's risk assessment may also be required whenever the Business Risk Assessment is itself revised.

3.5.2 Preparing/Drafting the Customer Risk Assessment

As is the case with the Business Risk Assessment, any decisions relative to the Customer Risk Assessment and changes thereto have to be duly documented so as to evidence that an appropriate review has taken place, and made available to the FIAU and other relevant supervisory authorities upon demand. The same applies to any revisions made to the Customer Risk Assessment.

The Customer Risk Assessment needs to cater for a situation where a 'provisional' risk rating based on the information and documentation collected initially may be revised once any questions are answered or doubts cleared through the collection of additional information/documentation. For some customers a comprehensive profile might become evident when operations initiate, hence there may be various tiers of risk assessments at different points throughout the relationship.

However, whilst it is possible for subject persons carrying out a specific relevant activity or a specific relevant financial business to adopt as their own a sectoral Business Risk Assessment prepared by an industry representative body, as seen in Section 3.3.2, the same does not apply to the Customer Risk Assessment. In fact, it would still be up to the individual subject person to carry out a Customer Risk Assessment each time that a new occasional transaction is carried out or a new business relationship is entered into.

In situations where the FIAU exercises its power under Regulation 5(2) of the PMLFTR and exempts a category of subject persons from carrying out a Business Risk Assessment (as explained in Section 3.3.2), the same category of subject persons will be equally exempted from carrying out a Customer Risk Assessment. Hence, it would be possible for subject persons within the exempted sector to take a standard approach to CDD and dispense with the Customer Risk Assessment.

3.5.3 Carrying out the Customer Risk Assessment

The effectiveness of the Customer Risk Assessment will depend to a large extent from the methodology applied to carry out the same. There is no one methodology that is recommended though there are common factors that would need to be present throughout. Thus, the methodology adopted has to consider the risk factors included in the Business Risk Assessment and apply the conclusions reached by the same.

Regardless of the methodology used, the subject person has to ensure that it understands it and deems it to be adequate and appropriate in view of the nature and size of its business. It is not necessary that the said methodology be developed by the subject person itself as it may engage consultants to assist it or acquire specific IT software or tools. However, the adoption of the

methodology and any major change thereto has to be approved by senior management. As for the Customer Risk Assessment itself, every aspect and decision relating to the methodology applied has to be clearly documented.

(a) Categorisation of Risk Factors

The subject person should be able to categorise the various risk factors it may face when entering into a business relationship or an occasional transaction on the basis of its Business Risk Assessment. The most simple categorisation system involves dividing risk factors in low, medium and high risk categories but a subject person may wish to adopt a system with more levels of risk categorisation.

(b) Weighting and Rating of Risk Factors

The relevance or weight of a risk factor within a business relationship or an occasional transaction will, more often than not, depend on the context of the particular relationship or transaction as already referred to in the case of geographical risk. Thus, the purpose for establishing the relationship, the level of assets involved or the size of the actual transactions to be undertaken, as well as the regularity or expected duration of the business relationship, will all influence the relative importance of one or more risk factors.

The individual risk factors are often weighted on the basis of a scoring systems, with scores assigned to the individual risk factors depending on the perceived severity thereof. Thus, an effective Customer Risk Assessment is only possible if the methodology applied allows for sufficient flexibility to take into account the particular circumstances of each case. For example, the product risk associated with the opening of a savings account, which can be equally used by a regularly employed individual with a steady salary to be received by means of direct credit and by a non-resident individual where the funds to be deposited are generated through an activity carried out in one or more high risk jurisdictions, will be higher in the latter scenario.

The following is an example of a methodology based on a scoring system that may be used in practice. The different risk variables within each of the four risk categories in Section 3.2 are each awarded a score on a scale from 1 to 10, where a score of 1 is awarded to the variable which poses the **lowest** risk and a score of 10 is awarded to the variable which poses the **highest** risk. This methodology is merely being provided as a guide or model. It is not exhaustive and consequently should not be considered to be mandatory. Subject persons are free to design a system that is most appropriate to its circumstances.

Table 5 below illustrates how this system works in practice.

Table 5 – Risk scoring grid

	Scoring	Type of Customer	Product/ Service	Interface	Geographical
EXTREME	**9 – 10**	• PEPs • Sanctioned individuals or entities	• Services intended to render the customer anonymous	• Non face-to-face through intermediaries and using means with no embedded safeguards	• Country subject to sanctions, embargoes
HIGH	**6 – 8**	• Non-Profit Organisations sending funds to non-reputable/high risk jurisdictions • Correspondent banks • Fiduciary arrangements	• Internet-based products • Services or products identified as posing a high risk of ML/FT	• Non face-to-face (using other means) •	• Non-reputable/high risk jurisdiction
MEDIUM	**3 – 5**	• Highly paid employees • Public figures • General public	• Normal products	• Non face-to-face (using system with embedded safeguards)	• Reputable jurisdiction •
LOW	**1 – 2**	• Other individuals (e.g. pensioners, average-salaried mployees)	• None	• Face-to-face	• EU Member State • Domestic

The following table explains what the four categories of risk scores mean:

Table 6 – Risk score

Rating	Impact of ML/FT risk
Extreme	Risk almost sure to happen and/or to have very dire consequences. Response: Do not establish business relationship or allow transaction to occur or reduce the risk to acceptable level.
High	Risk likely to happen and/or to have serious consequences. Response: Do not allow transaction until risk reduced.
Medium	Possible this could happen and/or have moderate consequences. Response: May go ahead but preferably reduce risk.
Low	Unlikely to happen and/or have minor or negligible consequences. Response: Fine to go ahead.

Taken together, the scores assigned to the individual risk factors should then allow the subject person to generate an overall risk score and lead it to understand whether the business relationship or occasional transaction falls within its risk appetite. Where this is the case, the subject person is then to categorise the business relationship or occasional transaction accordingly.

The categorisation system adopted by a subject person is expected to at least allow for business relationships or occasional transactions to be classified as low, medium or high risk, according to the perceived level of ML/FT risk. These three classifications are the basic rating system, but other categorisations are possible. It is therefore left to the discretion of subject persons to adopt a rating system that can provide a proper categorisation of business relationships and occasional transactions.

While the method used to weight risk factors is left to the individual subject person, and subject persons enjoy the discretion of designing and implementing a system that is most appropriate to its circumstances, it should be noted that any such methodology has to, as a minimum, adhere to certain basic principles:

(a) Weighting is not to be unduly influenced by just one factor;
(b) Monetary considerations are not to influence the risk rating;
(c) The provisions of the PMLFTR regarding situations that always present a high ML/FT risk (referred to in Regulation 11(3) to (9) cannot be over-ruled by the subject person's weighting; and
(d) Weighting does not lead to a situation where it is impossible for any business relationship or occasional transaction to be classified as high risk.

In deciding on the risk weighing methodology to be adopted, it is important that subject persons also take into consideration the results of the National Risk Assessment, the Supranational Risk Assessment and other risk assessment or authoritative guidance on risk that may be available and be relevant to the subject person concerned.

The above does not exclude the possibility of considering groups of customers or business relationships that share similar characteristics as presenting the same level of risk as long as the subject person can demonstrate that the groupings are logical and specific enough to reflect the reality of the subject person's business**.**

Where a subject person uses automated IT systems to allocate overall risk scores to business relationships or occasional transactions, and does not develop these in-house but purchases them from an external provider, it should thoroughly understand how the system works and how it allocates weightings and ratings, i.e. how it combines risk factors to achieve an overall risk score.

In this manner, the subject person should be able to determine whether the system-generated score actually reflects the subject person's understanding of risk. The subject person must also ensure that the IT systems are properly calibrated to cater for its own specific situation in view of its risk assessment. A subject person must always be able to

satisfy itself that the scores allocated reflect its understanding of ML/FT risk and it should be able to demonstrate this to the FIAU or any supervisory authority.

Where risk weighting is carried out using an automated process, the subject person must retain the ability to over-ride the automatically generated score where necessary. The rationale for the decision to over-ride such scores should be documented appropriately. In so doing, attention should be made to ensure that the risk scoring is not meddled with, that not all officials and employees may affect changes, and that there is a clear audit trail of who took the decision and actually over-rode the system-generated score.

3.6 Application of CDD on a Risk-Sensitive Basis

Having identified and assessed both the individual and the overall risk of a business relationship or an occasional transaction, the subject person is to then apply a commensurate level of CDD and the necessary CDD measures to mitigate the said risks. Use can be made of the flexibility inherent to the risk-based approach in order to better address risk, as subject persons are allowed to vary the timing and extent of CDD.

Thus, for business relationships or occasional transactions identified as presenting a low risk of money laundering, subject persons may apply SDD. It is important to note that SDD is not an exemption from CDD obligations but rather the ability to vary the timing and extent when determinate CDD measures are to be carried out. However, all CDD measures will have to be carried out at some point or other. In this respect, setting thresholds which are reasonably low can be particularly useful as long as the subject person has systems in place to monitor customer activity and determine the moment in time when the threshold is met and the application of one or more CDD measure is triggered.

On the other hand, business relationships or occasional transactions considered as high risk oblige the subject person to apply EDD measures thereto. In determinate instances, the PMLFTR themselves lay down what these measures have to be. In high risk situations which are not expressly dealt with in the PMLFTR, the subject person has to make an informed decision as to the measure/s it is to apply. The appropriate type of EDD measure applied, including any additional information/documentation or ongoing monitoring, will depend on the reason/s why the business relationship or occasional transaction was deemed to present a high risk of ML/FT and is to mitigate this risk.

As already remarked, risk is not static and therefore one's risk assessment has to be reviewed from time to time to ensure that it is still relevant. In particular, subject persons have to pay attention to any material change in the business relationship which can lead to a change in risk associated thereto. Should any such revision lead to a change in the individual or overall risk rating, the subject person has to consider whether this needs to translate itself in a different level of CDD or the application of different CDD measures.

The subject person should refer to Chapter 4 of the Implementing Procedures which explains in greater detail the basic CDD measures that have to be adopted. Moreover, subject persons are also to refer to the Risk Factor Guidelines issued by the ESAs, which contain general examples of possible EDD measures to apply in high risk situations as well as more specific examples applicable to the areas falling within relevant financial business.

CHAPTER 4 – CUSTOMER DUE DILIGENCE

The implementation of a sound customer due diligence programme is key for all subject persons to safeguard their services and products from being misused and end up serving as conduits for proceeds of crime, and to protect the reputation and integrity of the Maltese financial sector and other relevant sectors. Additionally, the implementation of CDD measures enables subject persons to assist the FIAU and law enforcement authorities in carrying out their responsibilities of analysing and investigating cases of ML/FT in an effective manner.

Inadequate implementation of CDD requirements on the other hand could result in enforcement action being taken against the subject person, which could have serious reputational, operational and financial repercussions.

The requirement to apply CDD measures ensures that subject persons have adequate mechanisms in place in order to:

(a) Determine who the customer, or any beneficial owner is,
(b) Verify whether such person is the person he purports to be,
(c) Determine whether such person is acting on behalf of another person,
(d) Establish the purpose and intended nature of the business relationship and the business and risk profile of the customer; and
(e) In the case of a business relationship, monitor the same on an ongoing basis.

CDD measures assist subject persons in determining whether a customer falls within their risk appetite and to understand the business profile of the customer with sufficient clarity so as to be able to identify those transactions that fall outside this profile and thus consider whether there is a suspicion of ML/FT or of proceeds of crime.

This Chapter focuses on providing guidance on the implementation of the CDD requirements which are envisaged under Regulations 7 – 12 of the PMLFTR.

Regulation 7 of the PMLFTR sets out the CDD measures which are to be undertaken by subject persons in relation to their customers and the business relationships and occasional transactions that they seek to set up or carry out. Regulation 7 also stipulates the instances when such CDD measures are to be applied.

Regulation 8 of the PMLFTR sets out the timing when verification of identity measures are to be implemented providing for a number of exceptions. Actions required when CDD measures cannot be completed are also set out in Regulation 8.

Regulation 9 deals with the application of CDD measures by casino and gaming licensees, and lays down a number of additional obligations that are to be undertaken by such licensees.

Regulations 10 and 11 respectively set out the instances when SDD and EDD are to be undertaken and the measures which are expected in each case.
Regulation 12 provides for the possibility of relying on certain CDD measures carried out by other subject persons or third parties (referred to as the “reliance procedure”).

Whilst this Chapter sets out certain standard procedures as to how certain CDD obligations are to be implemented within the subject person's policies and procedures, and how such procedures are to be applied, a certain degree of flexibility is allowed in order to cater for the application of a risk-based approach to CDD in accordance with Regulation 7(8) of the PMLFTR.

Subject persons are, therefore, allowed to determine, on a risk sensitive basis, the extent and timing of CDD measures to be applied in relation to the customer, depending on the type of customer, product, service, transaction, delivery channels and geographical connections. The risk assessment undertaken by the subject person on the customer should determine the extent and timing of CDD measures which are to be applied by the subject person, including the CDD information and documentation to be obtained, the extent to which the business relationship will be scrutinised and the nature and frequency of ongoing monitoring. Subject persons should be able to demonstrate to the FIAU that the extent and timing of CDD measures applied by the subject person on the customer is appropriate in view of the risks of ML/FT posed by the business relationship or occasional transaction in question. For further information on the application of the risk-based approach, subject persons should refer to Chapter 3.

4.1 Overview of CDD measures

Regulation 7 of the PMLFTR sets out the CDD measures which are to be applied by subject persons. The CDD measures to be applied are the following:

(a) The identification of the customer and the verification of the identity of the customer on the basis of documents, data or information obtained from a reliable and independent source (refer to Section 4.3)

    Where the customer is a body corporate, a body of persons or any other form of legal entity or arrangement, the subject person also has to verify the legal status of the customer and also identify all directors or, where the customer does not have directors, all such other persons vested with its administration and representation (refer to Section 4.3.2);

(b) The identification, where applicable, of the beneficial owner(s), and the taking of reasonable measures to verify the identity of the beneficial owner(s), so that the subject person is satisfied of knowing who the beneficial owner(s) is/are, including, in the case of a body corporate, foundation, trust and similar legal arrangements, the taking of reasonable measures to understand the ownership and control structure of the customer (refer to Section 4.2.2);

    In case of customer(s) that are trusts or similar legal arrangements, whose beneficiaries are designated by particular characteristics or class, the subject person has to obtain sufficient information concerning the beneficiaries to be able to identify and verify their identity at the time of payout or at the time the beneficiaries seek to exercise their vested rights;

(c) Assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship, and establishing the business and risk profile of the customer (refer to Section 4.4; and

(d) Conducting ongoing monitoring of the business relationship (refer to Section 4.5);

Regulation 7(3) stipulates that where any person purports to act on behalf of a customer, in addition to identifying and verifying the identity of the customer and, where applicable, the beneficial owner (as highlighted under points (a) and (b) above), the subject person shall ensure that such person is duly authorised in writing to act on behalf of the customer and shall identify and verify the identity of that person (refer to Section 4.3.3).

It is to be noted that the PMLFTR prohibit subject persons from keeping anonymous accounts or accounts in fictitious names.[33]

CDD measures are to be applied by a subject person in the following instances:[34]

(a) When establishing a business relationship;
(b) When carrying out an occasional transaction;
(c) When the subject person has knowledge or suspicion of proceeds of criminal activity, ML/FT, regardless of any derogation, exemption or threshold that would otherwise be applicable;
(d) To existing customers, at appropriate times and on a risk-sensitive basis, including at times when the subject person becomes aware that the relevant circumstances surrounding a business relationship have changed;
(e) When doubts arise about the veracity or adequacy of previously obtained customer identification information.

Casino and gaming licensees

By way of derogation from the provisions of Regulation 7(5)(a) and (b), which require the application of CDD when establishing a business relationship or carrying out an occasional transactions, Regulation 9(1) of the PMLFTR expects that casino and gaming licensee apply CDD measures when they carry out transactions that amount to or exceed two thousand euro (€2,000), and this applies both to business relationships (i.e. when casino or gaming licensees open gaming accounts) and occasional transactions. This derogation however does not apply if the casino or gaming licensee has knowledge or suspicion of proceeds of criminal activity, ML/FT. Casino and gaming licences are also expected to carry out CDD on existent customers (as explained under point (d) above) and when they have doubts about previously obtained customer identification information.

It should also be pointed out that Regulation 9(2) of the PMLFTR requires casino licensees to carry out additional customer due diligence requirements. These include:

(a) Identifying any person prior to entering a casino; and

[33] Regulation 7(4) of the PMLFTR.
[34] Regulation 7(5), (6) and (7) of the PMLFTR.

(b) Ensuring that the particulars relating to the identity of a person exchanging chips or tokens to the value of two thousand euro (€2,000) or more is matched with, and cross referred to, the particulars relating to the identity of the person exchanging cash, cheques or bank drafts, or making a credit or debit card payment in exchange for chips or tokens, as well as ensure that chips or tokens are derived from winnings made whilst playing a game or games at the casino. Casino licensees should ensure that they carry out this requirement not only in the case of individual transactions amounting to €2,000 or more, but also where in any one gaming session a person carries out transactions which in aggregate equal or exceed such amount.

4.2 Definitions

The concepts of "**customer**" and "**beneficial owner**" are referred to throughout this Chapter and therefore it is important for subject persons to understand who is considered to be a "customer" and a "beneficial owner" in terms of the PMLFTR. The aim of this Section 4.2 is to expand on the definitions of "customer" and "beneficial owner" in order for subject persons to understand who should be classified as such.

4.2.1 The Customer

The PMLFTR defines a customer as *"**a legal or natural person who seeks to form, or who has formed, a business relationship, or seeks to carry out an occasional transaction with a person who is acting in the course of either relevant financial business or relevant activity**"*.[35]

The customer is therefore:

- a person (whether legal or natural);
- who seeks to form a business relationship (i.e. a potential customer); or
- with whom a business relationship is formed (i.e. an existing customer);
- or for whom an occasional transaction is carried out.

A legal or natural person

The customer may either be a natural (physical) or a legal person. This notion is important as the application of CDD measures varies depending on whether the customer is a natural person, a legal entity or other legal arrangement. In fact, where the customer is a body corporate, a body of persons, or any other form of legal entity or arrangement, subject persons must also verify the legal status of the customer and identify all directors or, where the customer does not have directors, all such other persons vested with its administration and representation, as well as the customer's beneficial owner(s).

[35] Regulation 2(1) of the PMLFTR.

A potential and an existent customer

The definition of customer in the PMLFTR makes reference to the phrase ***"seeks to form or who has formed"*** in order to seek to capture both potential and existent customers. This is important given that subject persons are required to carry out CDD both with respect to potential customers (such as the identification and verification of a potential customer prior to establishing a business relationship or undertaking an occasional transaction) as well as on existent customers with whom a business relationship is established (such as the ongoing requirement to keep documents, data or information on such customers up-to-date). Thus, the term "customer" needs to be read in this context as well as in the respective context of the different provisions of the PMLFTR.

A business relationship or an occasional transaction

The definition of "customer" under Regulation 2 refers to a person seeking to form or who has formed a **business relationship**, or a person who seeks to carry out an **occasional transaction**. Thus two types of customer emerge.

The first is the customer who seeks to form or who has formed a **business relationship**. A business relationship, in accordance with the definition contained in the PMLFTR, must comprise three important cumulative elements, which are the following:

(a) The relationship must be of a business, professional or commercial nature between two or more persons;
(b) At least one of the persons involved in the relationship must be a subject person (whether undertaking a relevant financial business or a relevant activity); and
(c) The relationship has, or is expected to have at the time when the contact is established, an element of duration.

Point (c) seeks to capture those instances where it is clear from the outset that a continuous relationship is being set up (such as for example where a credit institution or a gaming operator open an account for a customer) and also scenarios where the relationship is inferred from the ongoing provision of the service which is not clear at the outset (such as when a property contractor is using the service of a notary on a regular basis).

The "element of duration" will need to be assessed on a case by case basis. Entering into an agreement, such as a retainer agreement, with a subject person for the ongoing provision of services/products/transactions in itself suggests that the customer is entering into a business relationship with the subject person. On the other hand, if the subject person is being engaged to undertake a transaction or provide a service and the interaction with the customer will terminate following the completion of the task by the subject person, then a business relationship is not considered to be established. Instead the transaction or service will be regarded as an occasional transaction, unless the services or transactions are being carried out on a regular basis on behalf of the same customer even though there is no intention to setup a relationship at the outset.

The second type of customer is the customer who seeks to carry out an **occasional transaction** with a subject person. The PMLFTR defines an occasional transaction as any transaction or service carried out or provided by a subject person for his customer, other than a transaction or service carried out or provided within a business relationship and includes, but is not limited to, the following:

(a) a transaction amounting to fifteen thousand euro (€15,000) or more, carried out in a single operation or in several operations which appear to be linked;
(b) a transfer of funds as defined under Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 (i.e. the Funds Transfers Regulation), which exceeds one thousand euro (€1,000) in a single operation or in several operations which appear to be linked;
(c) a transaction in cash amounting to ten thousand euro (€10,000) or more, carried out by a natural person or legal person trading in goods in a single operation or in several operations which appear to be linked;
(d) a transaction amounting to two thousand euro (€2,000) or more, carried out by gaming or casino licensees in a single operation or in several operations which appear to be linked;
(e) the provision of tax advice; and
(f) the formation of a company, trust, foundation or a similar structure.[36]

The above list is not an exhaustive list.

For the purposes of determining whether the thresholds mentioned under paragraphs (a) to (d) above are met or exceeded one should take into consideration the monetary value of the transaction or a series of linked transactions that the subject person carries out for the customer, and not the actual fee charged by the subject person for carrying out such a transaction or transactions.

For the avoidance of doubt, the formation of companies, trusts, foundations or similar structures, and/or the provision of tax advice (without the provision of additional services that lead to the establishment of an enduring relationship) by a subject person shall be considered to constitute an occasional transaction. No thresholds are applicable and therefore CDD measures should be carried out at all times. By way of example, CDD measures should be undertaken by the subject person even when incorporating a company with a share capital amounting to €1,200. Given that the formation of a new company (without the provision of additional services, following incorporation, that would lead to the establishment of a business relationship, such as the provision of directorship services) is by definition an occasional transaction, CDD measures should be applied irrespective of whether the initial share capital is of a minimal amount or not and irrespective of the professional fees charged.

Similarly the provision of tax advice will always give rise to CDD measures, irrespective of the values involved.

Customer vs Agent

[36] Regulation 2(1) of the PMLFTR.

It is also important to distinguish between situations where a customer is acting directly on his own behalf and where a customer is being represented by another person acting as his agent. Where the customer is represented by another person acting as agent the subject person is required to carry out additional measures (refer to Section 4.3.3). In fact, Regulation 7(3) stipulates that where a person purports to act on behalf of a customer, in addition to identifying and verifying the identity of the customer and, where applicable, the beneficial owner, subject persons are to ensure that such person is duly authorised in writing to act on behalf of the customer and are to identify and verify the identity of that person.

Subject persons must therefore determine whether whoever is requesting the establishment of a business relationship or the carrying out of an occasional transaction is doing so on his own behalf or on behalf of someone else. In the latter case, the person making the request is not to be considered as being the customer but as the customer's agent; the customer would be the person on whose behalf the agent is requesting the establishment of the business relationship or the carrying out of the occasional transaction.

Notwithstanding the fact that a person might have indicated that he is acting on his own behalf and is therefore to be considered as the customer, there may be circumstances which indicate that he is actually an agent. The subject person should therefore consider whether the declaration provided is reliable, including by having regard to the following:

(a) from where the subject person is receiving instructions;
(b) the source of funds;
(c) the destination of the funds;
(d) payment references or rationale that do not appear to relate to the purported customer;
(e) unusual delay in answering questions (due to the fact that the customer is referring the questions to the third party for a reply).

4.2.2 The Beneficial Owner

Subject persons are required to identify the beneficial owner, where applicable, and to take reasonable measures to verify the identity such that the subject person is satisfied of knowing who the beneficial owner is. In the case of a customer being a body corporate, foundation, trust or similar legal arrangement, subject persons are also required to take reasonable measures to understand the ownership and control structure of the customer.

The phrase "where applicable" is used in view of the fact that a business relationship or an occasional transaction does not always involve a beneficial owner, given that the customer may be an individual directly representing himself. Hence the obligation to identify and verify the identity of the beneficial owner outlined in Regulation 7(1)(b) of the PMLFTR is not always applicable.

Regulation 2 of the PMLFTR defines a beneficial owner as:

(a) Any **natural** person or persons who ultimately own or control the customer; and/or

(b) The **natural** person or persons on whose behalf a transaction or activity is being conducted.

The key element in this definition is the notion of a 'natural person'. A body corporate, body of persons, trust or other legal arrangement can never qualify as a beneficial owner. The beneficial owner, when there is one, must **always** be a natural person.

In cases where the customer is a natural person, the customer is deemed to be the beneficial owner himself, unless features of the transaction or surrounding circumstances suggest otherwise. The following is a non-exhaustive list of indicators that a natural person requesting a service or transaction from the subject person is doing so on behalf of another person:

(a) Instructions on the operation of the business relationship are received from another person who is not the person who established the business relationship;
(b) There are unusual delays in replying to questions posed by the subject person on the operation or activity – this may be owed to the fact that the said person has to refer to someone else for instructions; and
(c) The source of funds or the destination of the funds do not correspond with the purpose and intended nature of the established relationship – this might be indicative that a particular account or service is being used to process funds belonging to a third party.

Where it appears that a person is not acting on his own behalf, appropriate enquires should be made to determine on whose behalf that person (agent) is acting and additional customer due diligence measures must be carried out (refer to Section 4.3.3).

The definition of beneficial owner under Regulation 2(1) of the PMLFTR further clarifies who shall be considered a beneficial owner in certain determinate situations. This is illustrated in Table 7 below.

Table 7 – Definition of a beneficial owner

(a) Body corporate or body of persons	**(i)** The beneficial owner is the natural person/s who ultimately owns or controls that body corporate or body of persons through the **direct** or **indirect** ownership of **a sufficient percentage** of the shares, voting rights or ownership interest. Direct ownership or control of the body corporate or body of persons means: • Direct ownership of 25% plus one (1) of the shares (including bearer shares); • Direct ownership of more than 25% of the voting rights; or • A direct holding of an ownership interest of more than 25%. Indirect ownership or control of the body corporate or body of persons means:

	• Indirect ownership of 25% plus one (1) of the shares (including bearer shares); or • Indirect ownership of more than 25% of the voting rights; or • An indirect holding of an ownership interest of more than 25%. **(ii)** A natural person(s) who exercise(s) control via other means. **(iii)** The natural person(s) holding the positon of senior managing official(s) - If, after having exhausted all possible means, no beneficial owner as defined under paragraphs (i) and (ii) above is identified.
(b) Trusts	The following are considered to be beneficial owners: **(i)** Settlor; **(ii)** Trustee or trustees; **(iii)** Protector (where applicable); **(iv)** Beneficiaries, or where the individuals benefiting from the trust have yet to be determined, the class of persons in whose main interest the trust is set up or operates; and **(v)** Any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means.
(c) Other types of legal entities (such as a foundation) or legal arrangements similar to a trust, which administers and distributes funds	Natural person(s) holding equivalent or similar positions to those referred to in (b) above.

The contents of the above table are explained in further detail below.

4.2.2.1 Body corporate or body of persons

This sub-section shall be interpreting paragraph (a) of the definition of "beneficial owner" under Regulation 2(1) of the PMLFTR and analysing the three different manners in which a natural person(s) can ultimately own or control a customer that is a body corporate or a body of persons and thus be considered a "beneficial owner".

(i) ***The beneficial owner of a body corporate or a body of persons includes all natural persons who ultimately own or control, whether through direct or indirect ownership, 25% plus one (1) or more of the shares or more than 25% of the voting rights or ownership interests, including, where applicable, through bearer shareholdings, or through control via other means, other than a company that is listed on a regulated market which is subject to disclosure requirements***

consistent with European Union law or equivalent international standards which ensure adequate transparency of ownership information.[37]

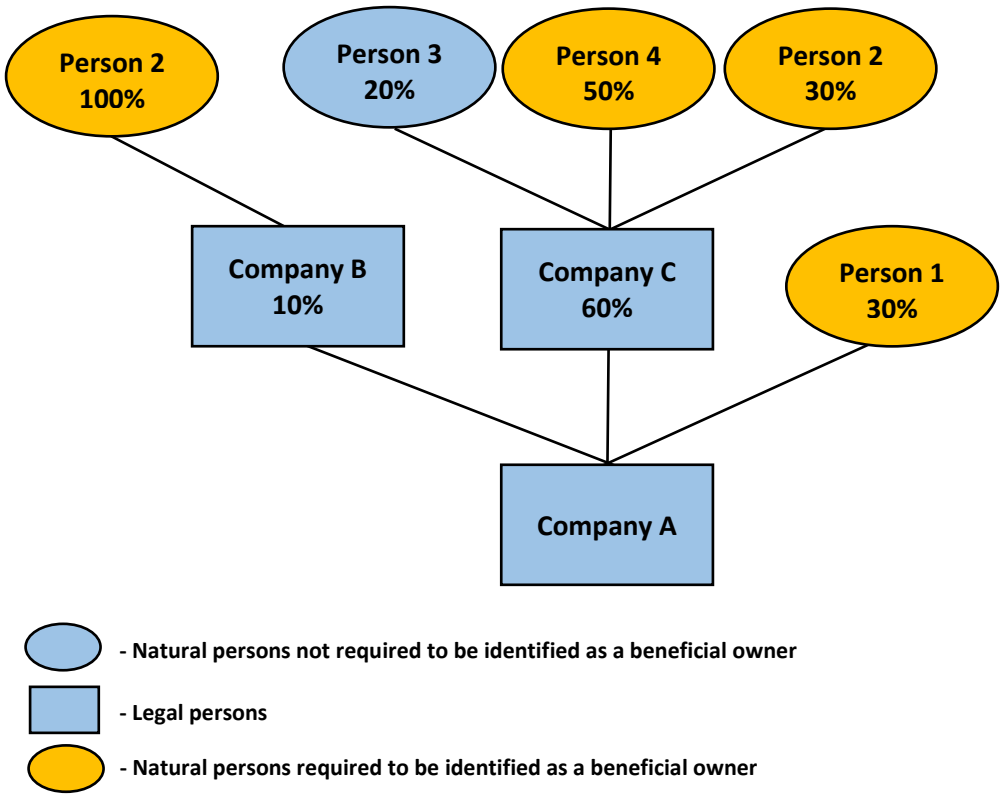
The beneficial owner is the natural person who ultimately owns or controls that body corporate or body of persons through the **direct** or **indirect** ownership of **a sufficient percentage** of the shares, voting rights or ownership interest.

> ***NOTE:*** Natural person(s) who ultimately own or control a **company that is listed on a regulated market** which is subject to disclosure requirements consistent with European Union legislation, or equivalent international standards which ensure adequate transparency of ownership information **need not to be identified and verified as beneficial owner(s)** for the purposes of the PMLFTR. Therefore the customer due diligence obligations envisaged under Regulation 7(1)(b) do not apply to such customers (refer to Section 4.3.2.2). This exemption is also applicable to companies that are majority-owned and consolidated subsidiaries of such listed companies.

In order to determine who ultimately owns or controls 25% plus one (1) of the shares or 25% or more of the voting rights in the body corporate or body of persons, reference may be made to the examples in Figures 1 to 5 below.

[37] Regulation 2(1) of the PMLFTR.

Figure 1 – Beneficial owner through direct and indirect ownership of a sufficient percentage of shares.



In Figure 1 subject persons are required to identify the beneficial owners of Company A (the Customer). Persons 1, 2 and 4 ultimately own 25% or more of the shares in Company A and thus should be identified as the beneficial owners of Company A. In the case of Person 1 the shares in Company A are owned directly, while in the case of Persons 2 and 4 the shares are owned indirectly through Companies B and C.

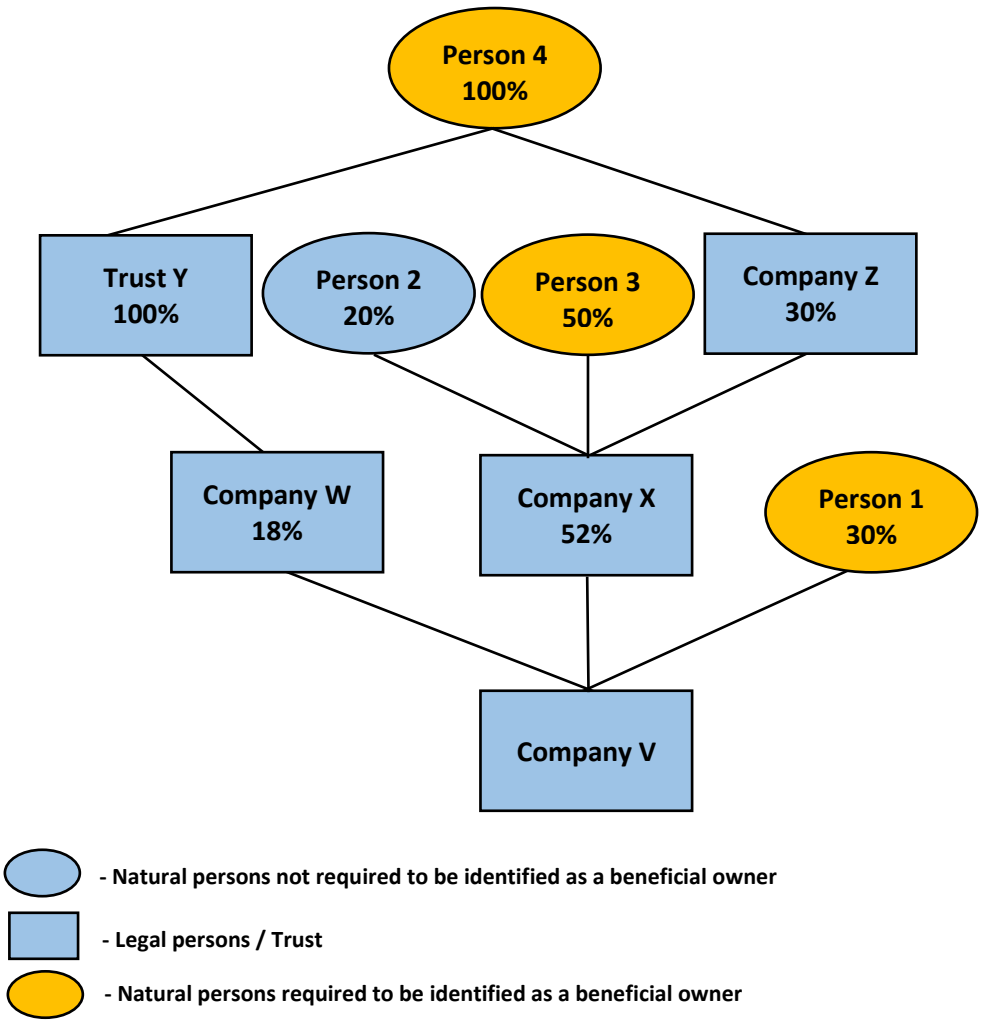
At the first layer, Natural Person 1 holds 30% of the shares in Company A and therefore qualifies as a beneficial owner for the purposes of the PMLFTR.

At the second layer, Natural Persons 2 and 4 qualify as beneficial owners for the purposes of the PMLFTR. Natural Person 2 holds 10% of the shares in Company A by virtue of being the sole (100%) shareholder in Company B which holds 10% in Company A, and holds another 18% of the shares in Company A by being holder of 30% of the shares in Company C which in turn holds 60% of the shares in Company A. Natural Person 2 thus owns 28% of the shares in Company A, indirectly through two Companies being Company B and Company C. Natural Person 4 ultimately holds 30% of the shares in Company A through a 50% shareholding in Company C, which in turn holds 60% of the shares in Company A.

NOTE: It is important for the subject person to establish and figure out the entire corporate structure of the customer to be in a position to understand whether an individual features within an ownership structure through more than one entity. In such cases the subject person is expected to assess all the holdings of that same individual to determine whether he holds a sufficient percentage of shareholding in the customer that would make him a beneficial owner.

Natural Person 3 ultimately holds 12% of the shares in Company A through Company C and therefore does not hold a sufficient percentage of shares to qualify as a beneficial owner.

Figure 2 – Beneficial owner through direct and indirect ownership of a sufficient percentage of shares. Including indirect ownership through a trust.



In Figure 2 subject persons are required to identify the beneficial owners of Company V (the Customer). The natural persons who ultimately own 25% or more of the shares in Company V, directly or indirectly, are Persons 1, 3 and 4. Directly in the case of Person 1 and indirectly in the case of Persons 3 and 4.

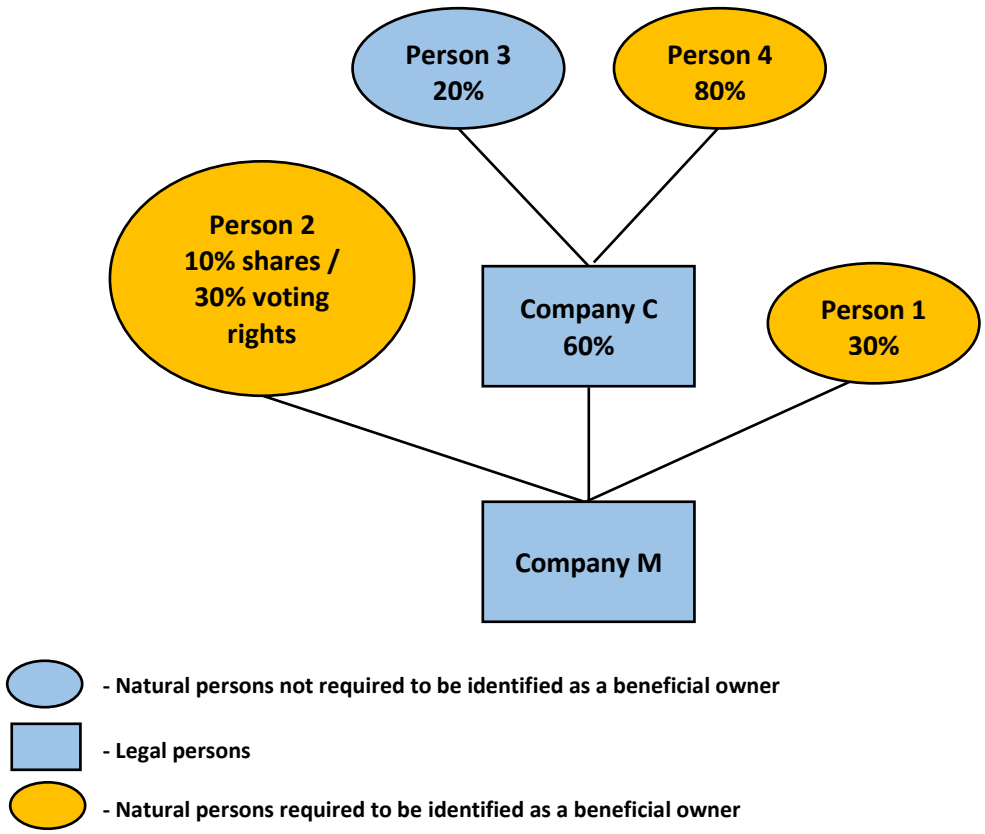
At the first layer, Natural Person 1 holds 30% of the shares in Company V and therefore qualifies as a beneficial owner for the purposes of the PMLFTR.

At the second layer only Natural Person 3 holds a sufficient percentage of shares (i.e. 26% of the shares in Company V indirectly through Company X) to be considered a beneficial owner. Natural Person 2 ultimately holds 10.4% of the shares in Company V and therefore does not hold a sufficient percentage of shares to be considered a beneficial owner.

At the third layer Natural Person 4 qualifies as a beneficial owner for the purposes of the PMLFTR as he ultimately owns 33.6% of the shares in Company V, due to the fact that he owns 18% of the shares in Company V through Trust Y and Company W and 15.6% of the shares in Company V through Company Z and Company X.

NOTE: Whenever the shares of a body corporate (being the customer) are held in Trust, and that trust is administered by a corporate trustee, subject persons are not expected to identify and verify the beneficial owner(s) of that corporate trustee. The requirement is to identify and verify the identity of the beneficial owner of the customer, i.e. the body corporate, and not the trustee administering the trust which holds the shares in that body corporate.

Figure 3 – Beneficial owner through direct and indirect ownership of a sufficient percentage of shares and voting rights.

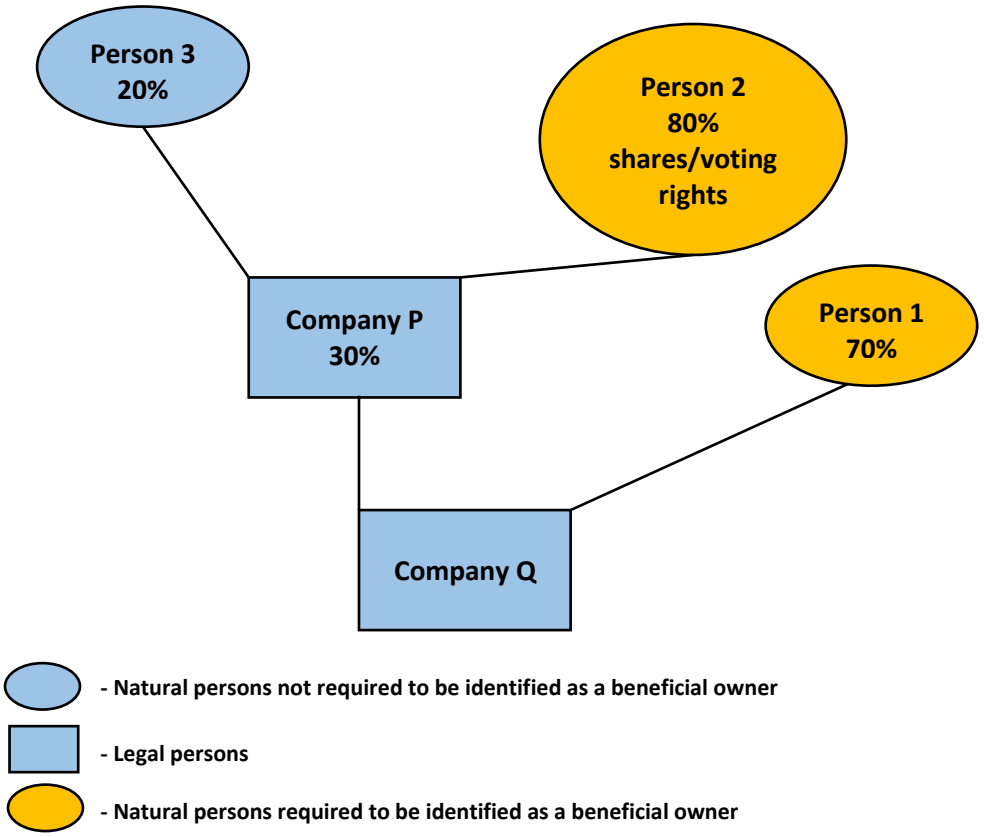


In Figure 3 subject persons are required to identify the beneficial owners of Company M (the Customer). Persons 1 and 4 ultimately own 25% or more of the shares in Company M and thus should be identified as beneficial owners of Company M. Person 2 shall also be identified as a beneficial owner given that he is holding 30% of the voting rights in Company M, even though he only holds 10% of the shares in Company M.

At the first layer, Natural Person 1 holds 30% of the shares in Company M directly and therefore qualifies as a beneficial owner for the purposes of the PMLFTR. Natural Person 2 does not hold 25% or more of the shares in Company M since he holds only 10%. However, each share held directly by Natural Person 2 in Company M carries 3 voting rights and thus Person 2 holds 30% of the voting rights in Company M. Natural Person 2 therefore qualifies as a beneficial owner for the purposes of the PMLFTR.

At the second layer, only Natural Person 4 qualifies as a beneficial owner for the purposes of the PMLFTR as he ultimately holds 48% of the shares in Company M through a 80% shareholding in Company C, which in turn holds 60% of the shares in Company M. Natural Person 3 ultimately hold 12% of the shares in Company M and therefore does not hold a sufficient percentage of shares to qualify as a beneficial owner.

Figure 4 – Beneficial owner through direct and indirect ownership of a sufficient percentage of shares and voting rights.



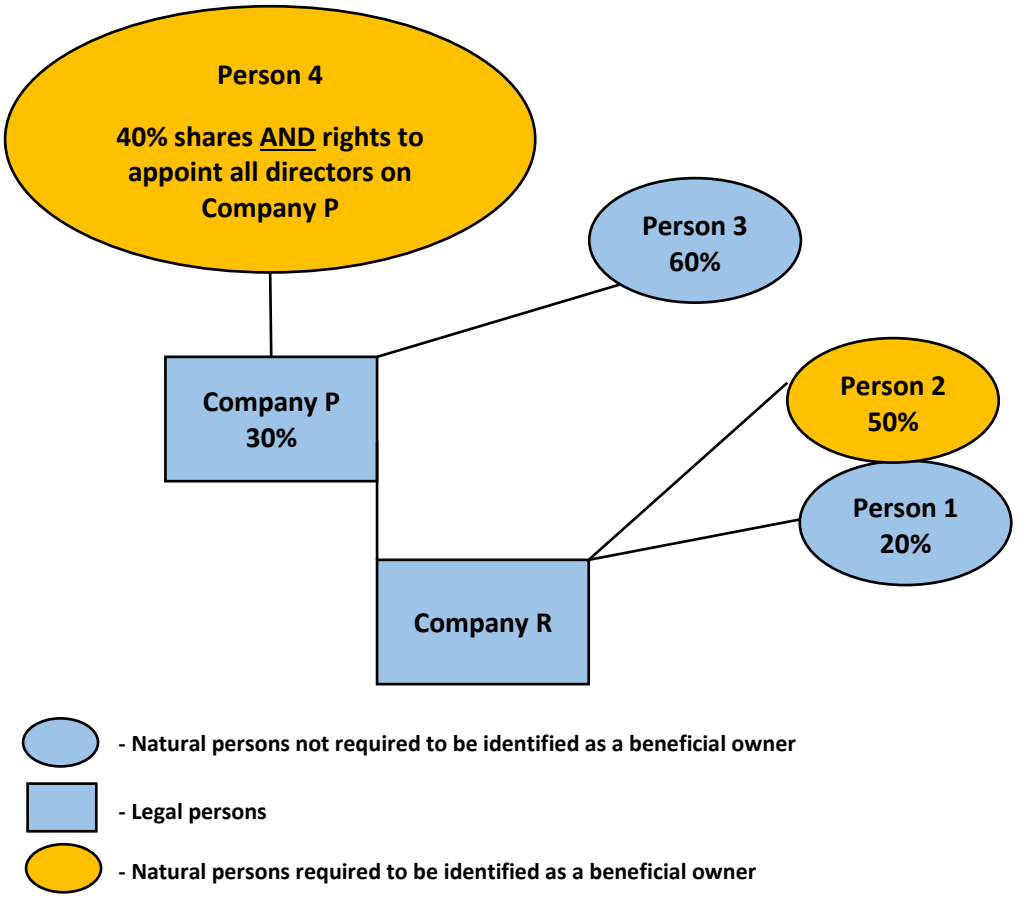
In Figure 4 subject persons are required to identify the beneficial owners of Company Q (the customer). Person 1 ultimately owns 25% or more of the shares in Company Q and thus should be identified as a beneficial owner of Company Q. Person 2 is also to be identified as a beneficial owner of Company Q given that he is controlling 30% of the voting rights in Company Q, even though he is considered as controlling only 24% of the shares in Company Q.

At the first layer, Natural Person 1 holds 70% of the shares in Company Q directly and therefore qualifies as a beneficial owner for the purposes of the PMLFTR.

At the second layer, Natural Person 2 also qualifies as a beneficial owner for the purposes of the PMLFTR. Being a majority shareholder in Company P, he ultimately controls 30% of the voting rights in Company Q through an 80% shareholding in Company P. The 80% shareholding in Company P allows Natural Person 2 to determine who is to sit on the Board of Directors of Company P and therefore how the 30% voting rights in Company Q are to be exercised.

Unlike in the case of shares, controlling a parent company will also mean that one is able to determine how the voting rights associated with the parent company's shareholding in the subsidiary are to be exercised in their entirety.

Figure 5 – Beneficial owner through direct and indirect ownership of a sufficient percentage of shares and voting rights.



In Figure 5 subject persons are required to identify the beneficial owners of Company R (the Customer). Person 2 ultimately owns 25% or more of the shares in Company R and thus should be identified as a beneficial owner of Company R. Person 4 is also to be identified as a beneficial owner given that he controls 30% of the voting rights in Company R, even though he only owns indirectly 12% of the shares in Company R.

At the first layer, Natural Person 2 holds 50% of the shares in Company R directly and therefore qualifies as beneficial owner for the purposes of the PMLFTR.

At the second layer, Natural Person 4 also qualifies as a beneficial owner for the purposes of the PMLFTR as he ultimately controls 30% of the voting rights in Company R through the special voting rights associated with its 40% shareholding in Company P. Those voting rights allow Natural Person 4 to determine who is to be appointed on the Board of Directors of Company P and in turn how the 30% voting rights held by Company P in Company R are to be exercised.

Companies whose share capital is issued in the form of bearer shares or that issue warrants to bearer

Companies whose share capital is issued in the form of bearer shares or that issue warrants to bearer are likely to pose increased difficulties for subject persons in determining beneficial ownership. Subject persons should exercise additional care and diligence when carrying out CDD measures on companies having bearer shares due to the fact that such companies pose higher risks of ML/FT. Companies that issue bearer shares are frequently incorporated in high risk jurisdictions. In this regard, additional measures are required to be undertaken by subject persons in order to mitigate the risk of ML/FT. In the event that the customer, or any company within the ownership and control structure of the customer, is a company with bearer shares subject persons have to determine the beneficial owners of such companies by applying one of the following measures:

(a) Where documents granting rights of ownership of bearer shares (such as a bearer share certificate) are issued in a jurisdiction that requires shareholders to **notify the company of their shareholding and the company to record their identity in a register**, subject persons must:

- require a copy of such register signed and certified as a true copy by the company secretary, the director or the registered agent, as the case may be; **and**
- obtain a written undertaking from the company secretary, director or registered agent and the beneficial owner that the subject person would be notified immediately if the bearer share certificate is transferred to any other person.

(b) Where bearer share certificates are **deposited with a regulated financial institution or a regulated custodian**, the subject person must:

- obtain a copy of the bearer share certificate;
- obtain a written declaration signed by a representative of the financial institution or the custodian certifying on whose behalf the document is held; **and**
- obtain from the financial institution or the custodian, as the case may be, a written undertaking that he would notify immediately the subject person if the bearer share certificate is transferred to any other person.

In the eventuality that the bearer share certificates are deposited with a regulated financial institution or a regulated custodian and are also recorded in the company's register subject persons may choose to apply either of the above measures.

In the light of the higher ML/FT risk that these companies may present, subject persons must desist from establishing a business relationship with, or carrying out an occasional transaction for, any such company when it is not possible to determine the beneficial owners of the bearer shares in accordance with the procedure outlined above.

(ii) *A natural person or persons who ultimately controls that body corporate or body of persons via other means.*[38]

[38] Regulation 2(1)(a) of the PMLFTR.

Subject persons are required to assess and determine whether any individual falls under this second category of the beneficial ownership definition in two situations. The first is when no individual could be identified under category (i). The second is when a beneficial owner was identified under category (i) but the subject person is aware or has reason to believe that another person(s) is exercising ultimate control over the running of that body corporate or over its management through other means (i.e. even if he owns an insufficient percentage of shares/voting rights or owns none). Such persons would also qualify as beneficial owners for the purposes of the PMLFTR.

Directors are not considered to fall under this part of the definition of beneficial owner, as in their capacity of directors they do not have an ownership interest in the body corporate, they do not control the voting rights in that body corporate or body of persons, and they do not exercise control over the management of that body corporate (i.e. they are not able to control the composition or voting rights of the board of directors).

Since it is impossible to provide an exhaustive list of persons who fall within this category (ii), subject persons must make a determination on a case-by-case basis. However, certain circumstances by their very nature would indicate that a person is exercising control over the management of a body corporate or body of persons. By way of example such cases could include:

(c) Persons who are granted rights through formal arrangements (such as shareholders' agreements or through rights attached to shares) by means of which that person(s) can exert dominant influence or veto the decision making of that legal person (e.g. having absolute discretion or veto rights over the entity's business plan, borrowing options or business model);
(d) Individuals who though not being owners of a sufficient percentage of shares or voting rights (i.e. less than 25%) collectively exceed the 25% threshold and are subject to an arrangement to exercise their rights collectively in the same way;
(e) Individuals who hold the right to directly or indirectly appoint or remove the majority of the board of directors (or administration) of an entity, or to appoint or remove the CEO of that entity; and
(f) Individuals who through family connections exert influence over the decision making body of that entity (e.g. a family business whereby a family member, even though not being formally involved in that entity, is routinely referred to for direction about company decisions).

One must appreciate that these rights may also be granted on a temporary basis. The more restricted the use of such right is, the less likely it is for that individual to exercise ultimate control over that body corporate. Hence, one should not regard these circumstances as ultimate indicators of absolute control but should make a case by case assessment.

For additional guidance, reference may be made to the FATF's "*Guidance on Transparency and Beneficial Ownership*" Report[39] or Article 22(1) to (5) of Directive 2013/34/EU.

[39] http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf

(iii) ***If no beneficial owner is identified in accordance with the above, the natural person(s) who hold the position of senior managing official or officials.***[40]

The definition of beneficial owner in Regulation 2(1) of the PMLFTR provides that if:

(a) after having exhausted all possible means; and
(b) provided there are no grounds of suspicion,

no beneficial owner has been identified in accordance with category (i) and (ii) explained above, subject persons are to consider the natural person or persons who hold the position of senior managing official or officials of the customer to be the beneficial owners, and are to keep a record of the actions taken to try and identify the beneficial owner in terms of categories (i) and (ii) above.

Subject persons should note that in such cases it is the senior management of the customer itself (i.e. the company that has requested the service) that should be identified and regarded as the beneficial owners and not the senior managing official(s) of the other entity(s) or arrangement(s) within the corporate structure of that entity.

It should be noted that the obligation to identify the "senior managing official(s)" as the beneficial owner(s) is not intended to be a default obligation for all customers that are body corporates or a body of persons, but an obligation that is triggered whenever the subject person:

(a) Cannot identify a person(s) who directly or indirectly own(s) 25% or more of the shares, or more than 25% of the voting rights or ownership interest within that legal entity (i.e. a beneficial owner under category (i)); and
(b) Cannot identity any natural person(s) who is controlling the body corporate or body of persons via other means.

Such a measure is intended to ensure that in those situations where a structure is of a particular complexity or where the ownership and control interest are so diversified that no person(s) can be regarded as ultimately controlling that body corporate, the senior managing official(s) who is/are responsible for taking strategic decisions and operating that body corporate are identified and known, and avoid circumstances whereby corporate entities will be providing services without knowing who is ultimately responsible for controlling that entity.

The definition of "senior managing official(s)" will depend on the type of body corporate or body of persons, however it is meant to capture those individual(s):

(a) Who are responsible for taking strategic decisions that fundamentally effect the business operations or general direction of that entity; and
(b) Who exercise executive control over the daily or regular affairs of the entity through a senior management position.

Paragraph (b) would typically include individuals who have executive functions or are otherwise responsible for the management of the entity such as executive directors, chief executive officers

[40] Regulation 2(1)(a) of the PMLFTR.

(CEO) and chief financial officers (CFO). Directors who do not have any executive functions would fall under paragraph (a).

Where there is more than one official that fulfils either criterion outlined above, and none is more senior that the other, the subject person should treat all as senior managing officials. Identifying directors who are "nominee directors" (where this concept is allowed) or corporate directors, that are acting on behalf of other individuals/entities who are instructing them and ultimately directing the affairs of the body corporate is however of no-value and the subject person should understand whether in such scenarios there are persons who would be considered as beneficial owners in view of the fact that they are ultimately controlling the company through other means as explained above (see category (ii)).

4.2.2.2 Trusts

Regulation 2(1) of the PMLFTR provides that in case of trusts, the beneficial owners are the following persons:

(a) The settlor,
(b) The trustee or trustees,
(c) The protector, where applicable (since not all trusts may necessarily have a protector or equivalent appointed),
(d) The beneficiaries, or the class of persons in whose main interest the trust is set up or operates, and
(e) Any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means.

Therefore, for the purpose of the PMLFTR, within the context of a trust, all the above persons will qualify as beneficial owners and therefore CDD measures, on a risk-sensitive basis, should be undertaken on such persons in accordance with Section 4.3.2.5.

The definition of beneficial owner for trusts under Regulation 2(1) of the PMLFTR should not be confused with the concept of beneficiaries (i.e. the beneficiaries who benefit or who may benefit from the trust) in terms of applicable trust law. The definition of a beneficial owner with respect to trusts has, as stated above, been made to also include the settlor, as well as the protector/s (if one or more are appointed) and the trustee, who typically enjoy no benefit, as such, under a trust. The trustees of a trust are deemed to be its beneficial owners because of the control they invariably exercise over the trust assets, as they will naturally exercise control over the trust property. The PMLFTR (reflecting the 4th AML Directive and the FATF 2012 Recommendations) also include the settlor within the definition of beneficial owner (given that he may still exercise a degree of control, even though to a lesser extent than that which a trustee has). In the case where a protector is appointed, the protector may typically also exercise some measure of control over the trust and the trust property (as laid out in the trust instrument), often by retaining a power of veto to approve or otherwise block certain decisions, as well as the power to remove or appoint trustees, replacement trustees or successor trustees, besides generally by keeping the trustee in check.

The definition of beneficial owner in the case of trusts includes also all the beneficiaries of the trust (i.e. the persons indicated in the trust deed as being the beneficiaries of the trust or the

persons who may potentially benefit under the trust), irrespective of the extent of their beneficial interest. This would include beneficiaries who are determined, as well as those who are not determined from the outset due to the nature of the trust and also beneficiaries designated by class (such as for examples trusts set up for the future grand-children of the settlor or some types of purpose trusts or charitable trusts). Reference should be made to Section 4.3.2.5 for an explanation of the CDD requirements in the case of such trusts and trusts in general.

In addition, the definition of 'beneficial owner' in Regulation 2(1) of the PMLFTR, with respect to trusts and similar arrangements, also provides that other natural persons who, in some way or another, exercise ultimate control over the trust, possibly by holding significant powers, are also considered as beneficial owners. In this regard, "control" means a power (whether exercisable alone, jointly with another person or with the consent of another person) under the trust instrument or by law to:

(a) dispose of, advance, lend, invest, pay or apply trust property;
(b) vary or terminate the trust;
(c) add or remove a person as a beneficiary or to or from a class of beneficiaries;
(d) appoint or remove trustees or give another individual control over the trust;
(e) direct, withhold consent to or veto the exercise of a power mentioned in points (a)-(d),

and which typically are held by the trustee or possibly a protector, albeit sometimes (to some degree or other) retained by the settlor or other named person in the trust instrument.

4.2.2.3 Legal entities such as foundations, and legal arrangements similar to trusts.

Paragraph (c) of the definition of beneficial owner under Regulation 2(1) of the PMLFTR covers legal entities such as foundations and legal arrangements that have a function or structure similar to trusts. Legal entities or arrangements having functions or structure similar to trusts would for example include *Treuhands* and *Fiducie* which are considered as the 'civil law' equivalents of the trust. Certain other succession-law institutes (e.g.: executorship of a will), various forms of shared ownership and community of property (in particular, silent partnerships and contractual investment funds), mandate and commission contracts, intermediated holding of securities and fiduciary ownership for security purposes can also be used in a manner so as to 'mimic' trusts, and each structure should be assessed on a case-by-case basis.

With respect to such legal entities and legal arrangements, the subject person will need to identify the equivalent persons undertaking a similar role as the ones identified under Section 4.2.2.2. Therefore, in the case of foundations, for instance, the subject person would have to identify and verify the identity of:

(a) The founder (equivalent to the settlor in the case of a trust);
(b) The administrator (equivalent to the trustee in the case of a trust);
(c) Member/s of the supervisory council (equivalent to the protector in the case of a trust);
(d) The beneficiaries or the class of persons in whose main interest the foundation is set up or operates, and any other person exercising control as further detailed in Section 4.2.2.2.

Similar to trusts, legal entities or legal arrangements might not be established for the benefit of beneficiaries or a private interest but rather would be set up for a cause or purpose. In such cases there would be no beneficiaries to identify, however subject persons should clearly determine the cause or purpose for which such entity or arrangement is set up. Reference should be made to Section 4.3.2.4 for an explanation of the CDD measures that are to be carried out with respect to such entities and arrangements.

4.3 Identification and Verification

Subject persons are required to have in place and implement CDD policies and measures which include customer identification and verification procedures that allow the subject person to ascertain the true identity of its customers and, where applicable, the beneficial owners.

Regulation 7(1) of the PMLFTR sets out the CDD measures to be undertaken by subject persons when establishing a business relationship or when undertaking an occasional transaction. The CDD measures relating to identification and verification of identity of the customer and beneficial owner(s) are the following:

(a) Identification of the customer, and the verification of the customer's identity on the basis of documents, data or information that is obtained from a reliable and independent source;[41] and
(b) The identification, where applicable[42], of the beneficial owner(s), and the taking of reasonable measures to verify their identity so that the subject person is satisfied of knowing who the beneficial owner(s) are.[43]

The **identification process** includes obtaining a set of personal or identifying details on the customer whilst the **verification process** entails verifying these personal and identifying details against documentation, data or information obtained from reliable and independent sources. The term "independence" should be interpreted as meaning a source which is independent of the customer (therefore not a declaration by the customer, but an identification document or a constitutive instrument issued by a third party but which may however be provided by the customer himself).

Through the identification and verification of identity procedures carried out the subject person has to be satisfied that he knows and has verified that the customer **exists** and that the customer **is who he purports to be**. This process also ensures that the customer is not acting anonymously or under a fictitious or stolen identity.

The CDD policies and measures should be tailored to address the ML/FT risks that are posed by business relationships or occasional transactions and as stipulated under Regulation 7(8) of the PMLFTR may vary from case to case so long as the subject person is able to demonstrate that the CDD measures, including the identification and verification measures adopted, are

[41] Regulation 7(1)(a).
[42] A business relationship or an occasional transaction does not always involve a beneficial owner.
[43] Regulation 7(1)(a).

commensurate to the risk of ML/FT identified through the customer risk assessment. This section will indicate what information on identity subject persons are expected to collect in various scenarios and which verification of identity measures are reliable and suitable to ascertain that a customer is who he says he is. Subject persons should determine, on a risk sensitive basis, the timing and the extent of verification measures on a case by case basis in accordance with the risk assessment carried out by the subject person.

The identification and verification measures to be applied to the customer depend also upon whether the customer is a natural person or a body corporate, a body of persons, or any other form of legal entity or arrangement. The identification and verification measures to be applied with respect to a natural person are dealt with in the section hereunder, whereas measures to be applied with respect to a body corporate, body of persons or any other form of legal entity or arrangement are dealt with in Sections 4.3.2 hereunder.[44]

4.3.1 The nature of identification and verification of a natural person

The subject person must first identify the customer and then verify such identity. Section 4.3.1(i) sets out the standard and minimum set of details which should be obtained by a subject person when identifying a natural person. Section 4.3.1(ii) provides guidance on the verification measures to be adopted.

As explained above, the aim and objective of carrying out identification and verification is for the subject person to ensure and be able to demonstrate that it knows and has verified that the customer exists and that the customer is who he/she purports to be. Identification and verification procedures also ensure that the customer is not acting anonymously or under a fictitious or stolen identity.

While this chapter will be laying down a standard set of identification details, information and documentation that has to be collected on customers that are natural persons, companies, trusts, foundations, etc., and will provide guidance to subject persons on how verification should be carried out, the approach to CDD should be risk-based. Subject persons should therefore determine on a risk sensitive basis (therefore considering the risk posed) the timing, means and extent of verification.

(i) <u>Identification</u>

Identification of a natural person takes place by obtaining a set of personal details. The standard set of personal details that is to be obtained for the generality of customers that are natural persons are the following:

(a) official full name;
(b) place and date of birth;

[44] The list provided in Sections 4.3.2.1 to 4.3.2.5 is not exhaustive since there may be other legal persons or arrangements acting as principals, but are intended to provide an indication of the measures to be applied in similar circumstances.

(c) permanent residential address;
(d) identity reference number, where available; and
(e) nationality.

However, in low risk situations, subject persons will be considered to have satisfied the identification requirements by obtaining the following details:

(a) official full name;
(b) date of birth; and
(c) permanent residential address.

These are considered to be the minimum personal details required to identify a natural person.

(ii) <u>Verification</u>

Verification of the customer's identity takes place by making reference to documents, data or information obtained from a reliable and independent source. The source has to be independent i.e. the source used to verify the customer's identity details should not be the customer himself. A source is reliable if it is reputable and is trusted by the subject person to provide extensive and sufficiently accurate data or information to verify the identity of the customer. For the purposes of this obligation, a reliable and independent source includes, but is not limited to:

(a) a government authority, department or agency;
(b) a regulated utility company; or
(c) a subject person carrying out relevant financial business in Malta, in a Member State of the EU[45] or in a reputable jurisdiction.

The above documents are deemed to be reliable and independent as the issuing entities would have already checked the existence and characteristics of the customer concerned.

The customer's identity may be verified by referring to documents or by making use of electronic sources. By far the most obvious and common sources used to verify the identity of a customer are identity cards, passports, driving licences and residence cards. Notwithstanding, subject persons may also refer to, and rely on, other documents to verify aspects of the customer's identity, such as documents issued by regulated financial business entities or utility companies which have dealt with or serviced the customer in order to verify the identity of the customer. Verification of the identity of the customer may also take place through electronic sources, such as E-IDs or Bank-IDs (widely used in Scandinavian countries) and electronic commercial databases.

4.3.1.1 Where the customer is present for verification purposes (face-to-face on-boarding)

(i) Standard Verification Requirements

Verification of identity

[45] For the purpose of this document, references to an EU Member State include reference to an EEA State.

Where customers are on-boarded on a face-to-face basis, the verification of the identity details is to be carried out by either making reference to a government-issued document containing photographic evidence of identity or by making reference to other documents bearing a photo of the individual which are recognised as a legal means of identity verification even if not issued by a government authority.

Documents issued by government departments or agencies, documents issued by a court or local authority and other documents that are recognised as a legal means of identity verification provide a high level of confidence because there is a greater likelihood that the authorities will have checked the existence and the characteristics of the persons concerned.

Government-issued documents containing photographic evidence of identity include:

(a) a valid unexpired passport;
(b) a valid unexpired national or other government-issued identity card;
(c) a valid unexpired residence card; or
(d) a valid unexpired driving licence.

Verification of residential address

The verification of the residential address may be carried out through any of the identification documents listed above (e.g. national identity card or driving license). Where such identification document does not contain information on the residential address of the customer, the subject person has to verify the residential address by making reference to any one of the following documents, provided that the residential address and the full name of the customer are referred to in a clear and unequivocal manner in the document itself:

(a) correspondence from a central or local government authority, department or agency;
(b) an official conduct certificate;
(c) any other government-issued document not mentioned above;
(d) a recent statement or reference letter issued by a recognised credit institution or entity carrying out relevant financial business in Malta, or equivalent activities in a Member State of the EU or in a reputable jurisdiction;
(e) a recent utility bill;
(f) a lease contract or agreement;
(g) any other document as may be specified in sectoral implementing procedures issued by the FIAU.

The documents listed above must not be more than six (6) months old when made available to the subject person. In the case of a lease contract or agreement, the six (6) month rule does not apply but the subject person has to ascertain that the same is still valid.

Where the residential address is verified through reference to a utility bill, the subject person should ensure that such utility bill was issued in relation to services linked to that residential property. Therefore, a bill issued in relation to a fixed line telephone service installed at that

property would be acceptable, but mobile telephony bills, where the services are not linked to a fixed premises, would not be acceptable.

The residential address of the customer may also be verified by adopting an alternative procedure that would involve the mailing of correspondence via registered mail or other mail courier service, or the mailing of codes generated by automated systems to the residential address provided by the customer. Where subject persons avail themselves of this measure to verify the residential address they should keep the following records:

(a) documentary evidence (such as an advice of delivery or a printout of the online tracking report) which indicates that the correspondence was delivered at the specified address and a copy of the correspondence signed by the customer indicating the residential address where it was sent;
(b) the advice of delivery signed by the customer himself; or
(c) evidence that the automatically generated code was received by the customer.

(ii) Verification requirements in Exceptional Scenarios

Some customers may not be able to produce the standard verification documentation referred to above for various reasons. In such cases the subject persons should consider whether this inability is due to a deliberate avoidance or reluctance by the customer to provide the necessary documents, data or information, or whether it is because the required identification information or documentation does not exist.

If the subject person is unable to complete the necessary procedures due to the reluctance by the customer to provide the necessary documents, data or information, the subject person is not to enter into the business relationship or carry out the occasional transaction and, if there is a suspicion of ML/FT, the subject person is to file a report with the FIAU as set out in Section 5.5.

The customer may be unable to meet the standard verification requirements due to the fact that certain identification details do not exist or the customer is unable to procure the envisaged verification documentation, as in the following cases:

(a) customers with a legal, mental or physical inability to manage their affairs;
(b) individuals dependent on the care of others;
(c) dependant spouses/partners or minors;
(d) students;
(e) refugees and asylum seekers;
(f) customers using temporary addresses;
(g) customer residing on yachts; and
(h) individuals residing in residential care.

The subject person will therefore need to adopt an approach that compensates for the difficulties that such customers may face in providing the standard evidence of identity, subject and commensurate to the customer risk assessment. Such an approach is necessary to ensure that, where people cannot reasonably be expected to produce standard evidence of identity, they are not unreasonably denied access to financial services (i.e. financial exclusion). Subject persons may

therefore have recourse to alternative measures that give reasonable confidence as to the identity of a customer, which may be applied to verify the customer's identity or some aspects of his identity.

Below are a few examples of alternative measures which may be applied:

(a) Where a customer only has a temporary address and has no permanent residential address elsewhere, such as seasonal workers, a letter from a director or manager of the employer confirming the residence at a stated address and indicating the expected duration of employment would be sufficient;
(b) Where a customer resides on a yacht, the residential address of the customer may be verified by obtaining documentation relating to the chartering of the yacht and berthing agreements;
(c) Where the customer is residing in a nursing home or similar residential care, the subject person may verify the residential address of the customer by obtaining a letter from the director or manager of the home confirming the address where the customer resides;
(d) Where customer is homeless or a member of the travelling community, subject persons shall gather sufficient information, and where available, documentation on the customer's situation and frequent whereabouts;
(e) Where the customer is a student or part of the academic staff, and is residing in a university, college or any other institutional residence, the subject person may verify the residential address of the customer by obtaining a letter from the director or senior official of the university, college or institution confirming the address where the customer resides.
(f) Where the customer is a minor (and therefore might not have identification documents or cannot present documents issued by recognised credit institutions or other financial service providers) subject persons may rely on a birth certificate to verify the minor's identity. The subject persons shall additionally proceed to identify and verify the parent(s) or legal guardian(s) and obtain reasonable evidence of parenthood or legal guardianship. With respect to the residential address, verifying the residential address of the parents or guardians with whom the minor resides would suffice.
(g) where the customer is an asylum seeker, a refugee or otherwise enjoys international protection status, verification of identity may be carried out on the basis of the identity documents referred to in the FIAU's Guidance Note on AML/CFT Obligations in relation to Payment Accounts with Basic Features.

When obtaining confirmation or declarations by third parties, the subject person is to gather information to satisfy itself as to the suitability of the person making the declaration. The subject person is therefore required to carry out checks on open sources or conduct confirmatory phone calls in order to ensure that the person providing the declaration is who he really purports to be. The checks which the subject person has undertaken to confirm the identity of the third party providing the confirmations have to be documented and retained by the subject person.

The above list is not an exhaustive list and subject persons may adopt different alternative measures, depending on the risk posed and on how reasonably reassuring such measures are to verify the identity of that customer.

(iii) Records to be kept

Where verification is carried out by making reference to and viewing in person any of the above mentioned identification and other documents, subject persons are required to:

(a) keep the original itself, where this is possible, or else
(b) keep a true copy of the original document on file or in electronic form.

The copy of the original document viewed for identity verification purposes has to be dated and certified as a true copy by an officer or employee of the subject person. Subject persons may instead retain scanned copies of the original documents using electronic systems which are able to meet all the following criteria:

(a) The electronic system used to record the document has to automatically record data so as to allow the subject person to determine the officer who would have scanned the document;
(b) The electronic system also has to automatically record the date and time of the scanning of the document; and
(c) The electronic system has to have safeguards so as not to allow any of the data referred to in the previous two points from being altered, amended or tampered with.

Utility bills, bank statements or other documents may be received or retrieved by customers through electronic means and hence customers may provide print-outs of such documents or relay them electronically to the subject persons. Subject persons should take risk-based measures to determine the reliability of such documents (such as verifying the existence of the utility company through open sources). Subject person's officials receiving such documents should date them or else retain a copy of the email through which they were received.

Where subject persons have recourse to exceptional means of verification (refer to paragraph (ii) above) subject persons shall, besides keeping a record of the documents obtained for verification of identity purposes, appropriately document the reasons for recurring to such exceptional means of verification and the reasons for considering such means as reasonably re-assuring to verify the customer's identity.

(iv) Authenticity Checks

Particular care should be taken to ensure that the documents obtained are authentic and have not been forged or tampered with. The following are some checks that may be carried out to verify the authenticity of identification documents. These include:

(a) examining the optical security features that are present on the document and confirming that these can be seen;
(b) examining the lamination of the identification document to check for any signs, such as borders around the photographic image of the document or raised surfaces that might be indicative of the fact that the document has been tampered with;
(c) checking for any uneven document colours and non-uniformity of text, font or typeface that would be indicative of a potentially counterfeit document; and

(d) verifying or decoding the Machine Readable Zone (MRZ) code contained on the identification document.

There are a number of open sources of information that subject persons may use to assist them in carrying out authenticity checks. Subject persons may refer to the following websites to view identification document samples of a number of jurisdictions around the world. These include:

www.edisontd.net

https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/borders-and-visas/schengen/docs/handbook-annex_23_part_1_and_2.pdf

https://www.consilium.europa.eu/prado/EN/prado-start-page.html

Additionally, subject persons may also refer to commercial software solutions which check the algorithms used to generate passport numbers. This can be used to check the validity of passports of any country which issues machine-readable passports. Subject persons should exercise due care when relying on documents that are issued by high-risk or remote jurisdictions and are, on a risk-sensitive basis, to determine whether additional checks or documentation should be carried out or obtained.

Subject persons should be wary of receiving downloaded utility bills, banks statements or other documentation in a format that may be more easily tampered with (e.g. word documents), in the sense that the data within may be amended or fabricated. In such cases subject persons should take practical and proportionate steps to establish whether the relevant source should be considered to be reliable and be used.

Subject person must moreover ensure that any documentation obtained for verification purposes is in a language that is understood by the subject person and the officers or employees carrying out the verification process. Where this is not the case appropriate steps should be taken to ensure that the document does provide the necessary evidence to verify the identity details of the customer. Translations of any such documents should be reduced in writing and retained on file.

4.3.1.2 Where the customer is not present for verification purposes (non face-to-face on boarding):

The type of businesses that are conducted online or provided remotely are on the increase, leading to more customers not being met physically by subject persons (i.e. non-face to face on-boarding). The provision of services and the carrying out of occasional transactions on a non-face-to-face basis increases the risk of ML/FT and of customer impersonation. This is due to a number of factors, such as the ease of accessing services at any time and from any location, the possibility of setting up multiple fictitious accounts and avoiding detection, the absence of physical documents that can be viewed and the speed with which services are provided and transactions carried out. Subject persons should thus factor this in their business and customer risk

assessments and be more diligent when undertaking CDD measures on customers on-boarded on a non-face-to-face basis.

Whilst, as explained, there is an increased risk when undertaking non-face-to-face business relationships and occasional transactions, such relationships and transactions should not automatically be considered to be high risk and the extent of CDD should be determined on the basis of a holistic customer risk assessment which also takes into consideration other elements of risk such as the nature and characteristics of the product, service or transactions being offered or carried out and the type of customer.

This notwithstanding, subject persons have to bear in mind what verification of identity entails and should therefore assess whether the identification and verification measure(s) to be applied, whether documentary or electronic, provide sufficient comfort that the customer exists and that he is truly who he says he is. Should the subject person still have doubts as to the identity of the customer, or of the authenticity of the documents, the subject person should assess whether, in view of the other risk elements of the relationship or transaction, additional or different identification and verification measures or checks should be carried out.

(i) Verification on the basis of documents

Where the customer is not present for verification purposes, subject persons would only be in a position to obtain copies of the identification documents listed under Section 4.3.1.1(i) above. With respect to other documents that may be used to verify the residential address listed under the same section (such as utility bills or banks statements) subject persons may obtain either originals or copies thereof. It would also be acceptable to verify the residential address through the mailing of correspondence or codes as explained in Section 4.3.1.1(i).

When receiving documentation in copy or scanned format subject persons should be mindful of a number of factors when determining the reliability and suitability of that document for verification purposes. Subject persons should avoid accepting documents provided in formats that are more susceptible to be tampered with (e.g. MS Word documents) and should instead request copies in other more tamper resistant formats (such as pdf format). Subject persons should be wary of identification documents and other documents issued by authorities or entities in high risk or remote jurisdictions. Copy documents sent via email address that do not seem to tally with the name or other details of the customer sending the documentation should also raise concerns.

Subject persons have also to ensure, when receiving copies or scanned documentation that the information and contents of such documentation is clearly visible and legible and that the document is in a language that is understood by the subject person and the officers or employees carrying out verification. Translations of any such documents should be reduced in writing and retained on file. Similarly to face-to-face on-boarding, subject persons should carry out checks to ascertain the authenticity of the document supplied (reference may be made to Section 4.3.1.1 (iv) for guidance on authenticity checks that may be carried out).

The subject person should then determine whether, on the basis of the documentation obtained, it is confident of having adequately verified the customer or whether additional checks or measures should be carried out. This determination should be made on the basis of the customer risk assessment for that particular business relationship or occasional transaction and also on the basis of a number of other factors, such as the type of document provided and whether doubts arise on the authenticity of the document itself. By way of example in low risk business relationships or occasional transactions, the provision of an identification document in copy would be sufficient so long as no issues arise as to its authenticity or reliability. In other situations, where the risk of ML/FT is not low subject persons should consider applying additional measures to verify the identity of the customer.

The following is a list of additional measures that may be applied by subject persons to verify the identity of the customer and hence be satisfied of having verified that the customer exists and he is who he says he is:

(a) ***Requesting additional identification documentation*** – through this measure the identity details (at least the identity details required in low risk scenarios) would be verified at least twice on the basis of multiple documents as set out in Section 4.3.1.1. For such a measure to be effective the documents relied on for verification purpose should not be issued by the same source. By way of example, if the subject person obtains a bank statement to confirm the residential address, it would not be an effective measures to obtain as a second and additional document a reference letter issued by the same bank (given that the source of information would be the same bank);

(b) ***Requiring certified documentation*** **-** this measure consists in the certification of identification or other documents used for verification purposes by legal or accountancy professionals, entities/persons undertaking a relevant financial business or equivalent activities in reputable jurisdictions, or by embassy officials. The reasoning here is that the certifier would be providing added comfort as to the authenticity of the document and confirming that the personal details appearing on the certified document correspond to the customer.

Where certified documents are obtained these should include a written statement confirming that:

- the document certified is a true copy of the original document,
- the original document has been seen and verified by the certifier, and
- the photo visible on the document (where applicable) is a true likeness of the customer.

The certified copy must be signed and dated by the certifier and is to include the certifier's:

- name and surname;
- address;
- contact details; and
- profession, designation or capacity.

Subject persons should make independent checks to verify the existence of such certifier and document such checks (e.g. checks on open media sources or professional registers). Subject persons must exercise caution when accepting certified copy documents, especially where such documents originate from a country or territory perceived to represent a higher risk than usual.

(c) **Ensure that the first payment or transaction into the account is carried out through another account held by the same customer in his name with a credit institution authorised under the Banking Act[46] or otherwise authorised in another EU Member State or a reputable jurisdiction** – when receiving funds from a bank account held by the same customer with another bank, the subject person would be ascertaining that the customer's identity would have already been verified by another entity. It is to be noted that the first payment or transaction into the account held by the customer may also be an electronic card payment, so long as the electronic card used to effect the payment is linked to an account held by the payer with a credit institution. E-money payments are not admissible in terms of this paragraph.

(d) **Requesting the customer to confirm automatically generated codes or PINs before accessing the service / account** – such codes or PINs automatically generated may be supplied to the customer via mail to his residential address or via verified means of communications (e.g.: mobile phone) requiring the customer to input such security codes or PINs before acceding to the service or being able to operate an account.

(e) **Holding a 'welcome call' with the customer via a verified home or mobile phone number and confirming certain personal information or a transaction to be undertaken** – through this method of verification, the subject person may verify the personal details provided by the customer at an earlier stage or details of requested transactions via a telephone call held through a fixed line or mobile phone number that can be linked to the customer.

(f) **Using information that can be retrieved from a customer's device to corroborate certain personal details provided by the customer** (e.g. customer's I.P. address or the geo-location of a mobile phone to confirm residence).

(g) **Sending a small transfer of funds to a bank account held by the customer asking him to return the funds or to indicate the value of that transaction**.

(h) **Requiring the customer to send a photograph clearly showing the customer's face and the image on the identity document being held in the same picture to demonstrate this actually belongs to the customer** – the subject person would be able to compare the face, and the features of the face, of the customer with that included on the identification document and therefore verify that the identification document truly belongs to such individual.

This list should not be construed as an exhaustive list of additional measures or checks that subject persons may carry. Subject persons may recur to other measures or checks, so long as such

[46] Cap. 371 of the Laws of Malta.

measures assist in determining that the customer really exists and that he is who he is indicating to be.

Use of video conferencing tools

Subject persons may also remotely verify the identity details of a customer through video conference facilities. A video call may be carried out subsequent to the customer submitting copies of the identification or other verification documents listed in Section 4.3.1.1(i) to the subject person (e.g. by email) or by making such documentation visible in the course of the video conference call. When making use of such means subject persons must observe a number of conditions which are set out in the following paragraphs.

The video call has to allow the subject person and the customer to make both visual and verbal contact simultaneously. It should be of a sufficiently good quality to enable clear verbal communication and to allow the subject person to clearly visualise the face of the customer, as well as view the contents and security features of identification documents produced by the customer (where identification documents are being presented through the video call).

Checks to verify the authenticity of verification documents presented through the video call, may either be carried out manually by the officer of the subject person or automatically if the software being used for the video conferencing itself has the capability to carry out such authentication checks. Subject persons may make reference to Section 4.3.1.1 (iv) for guidance on authenticity checks that may be carried out manually. To carry out some of the listed checks (e.g. to visualise the security features of the presented identification document) the customer should be asked to tilt the document during the video call.

The official carrying out this procedure shall also examine the image on the identification document (presented during the video call or submitted to the subject person prior to the video call) to ensure that it matches the visual appearance of the customer as well as the details of the person produced on the identification document (such as age).

Where a subject person carries out verification of identity through video conferencing, the following records must be retained to demonstrate compliance with the above requirements:

(a) at least an audio recording of the video call or the entire video call itself, which includes the entire conversation between the official of the subject person and the customer;

(b) screenshots taken during the video call, which must include an image of the customer as well as the date and time displayed by the video conference tool; and

(c) where the identification document is produced by the customer throughout the video call screenshots of the identification document (all relevant pages or sides) will need to be recorded. The photographic evidence of identity as well as all the information on the identification document shall be clearly visible and legible from the screenshots.

Use of identity verification software

Subject persons may make use of identity verification software which allows customers to upload facial images, video clips and scans of the identification documents listed in Section 4.3.1.1(i) and are able to carry out authentication checks on such documents as well as visual checks to compare the uploaded customer's facial image with the image appearing on the uploaded document.

Prior to acquiring any software, the subject person should assess the system and evaluate the capabilities of the software (such as what types of documents the system is able to screen for authentication, whether the system allows for the retention of documents uploaded, etc.) in order to ensure that the requirements set out in this Section are satisfied.

The identity verification software should be able to carry out the following automated checks upon the receipt / uploading of the identification document:

(a) ***Visual Checks*** – the system should be able to compare automatically the facial features of the customer shown on the photographic image visible on the identification document with the facial features shown on a separate photograph or a video clip taken and sent by the customer contemporaneously with the transmission of the identification document.[47] Moreover, the system should have the capability of comparing the images and determining that the person represented in both photographic images is one and the same.

(b) ***Authentication Checks*** – the system should have the capability of automatically verifying the authenticity and validity of the identification document submitted by performing, a number of checks such as:

- verifying that the security features (such as holograms) of that particular identification document are in place;
- examining the lamination and ensure that there are no indicative signs of the fact that the document may have been tampered with;
- examining the document's layout and features (such as font, typeface and colour) and ensure that these match the document's standard; and
- reading and validating the Machine Readable Zone (MRZ) code on the identification document.

The subject person should be satisfied that the systems' authentication checks are suitable and reliable and that they are effective in detecting fake or forged documents.

Subject persons should ensure that an electronic copy of the identification document and the photograph taken and sent by the customer or stills of the video clip showing the customer's face are retained on file. These documents should be saved automatically by the same system used to receive these documents, and the time and date when such documents were received should be recorded. Moreover the system shall have measures in place to ensure that such records cannot be altered or tampered with.

[47] For the avoidance of doubt it should be noted that the photograph / video clip with which the comparison is made should be taken at the same time that the person has accessed the system to upload the identification document and the system should have inbuilt features that verify and confirm this.

(ii) Electronic verification of Identity

The methods of verification of identity mentioned in this section do not entail the presentation of identification documents or other verification documents but rather allow for the identity of the customer to be verified remotely through electronic means.

Verification through the use of commercial electronic data providers

It is possible to carry out the verification of the identity of a person electronically through recognised commercial electronic data providers. Such commercial data providers may have access to multiple data sources such as electoral registers, driving licence databases and passport identity registers among others.

Subject persons would only be in a position to make use of such services if the provider satisfies all of the following criteria:

- it is recognised, through registration with the data protection authority of the country where it is set up, to store personal data;
- unless it is registered with the data protection authority of the country where it is set up, it is accredited, or certified, to offer the identity verification service through a governmental, industry or trade association process that involves meeting minimum published standards;
- it uses a range of multiple, positive information sources that can be called upon to link an applicant to both current and previous circumstances;
- it accesses negative information sources, such as databases relating to identity fraud and deceased persons;
- it accesses a wide range of alert data sources;
- arrangements exist whereby the commercial electronic data provider's continuing compliance with the minimum published standards is assessed;
- its published standards, or those of the scheme under which it is accredited or certified, require its verified data or information to be kept up to date, or maintained within defined periods of re-verification; and
- it has transparent processes that enable the subject person to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject.

It is important to note that the process of verification carried out by commercial electronic data providers should meet a standard level of confirmation that should at least comprise the following:

- from one source, one match on an individual's full name and current permanent residential address; and
- from a second source, one match on an individual's full name and either his current permanent residential address or his date of birth.

The commercial electronic data provider should allow the subject person availing himself of its services to capture and store the information it used to verify the identity.

Where commercial electronic data providers only cross check the provided customer personal details to ensure that they belong to an existing individual without determining whether the customer is, in fact, who he says he is, the subject person cannot rely solely on the checks undertaken by the commercial electronic data provider, as the subject persons would not be considered to have successfully verified the identity of the customer. In such instances, the subject person should also apply one or more additional measures as specified in Section 4.3.1.2(i) to verify the identity of the customer.

Use of E-Ids

A number of jurisdictions have developed identification documents and means of identifications that allow holders to provide evidence of their identities remotely. Such systems usually consist in encrypted data stored either on electronic chips embedded on an identification document or on devices such as mobile phones, which can be transmitted to and read by whoever requests verification of one's identity.

Where the subject person intends to make use of this method of identity verification, the identity details provided by the customer are to be verified on the basis of the data read either from an electronic chip embedded on an identification document which in terms of Section 4.3.1.1(i) can be used to verify one's identity or from other electronic devices (such as mobile applications or computer software) which meet all of the following conditions:

- this measure is recognised to be a legally valid means of identity verification in the jurisdiction of nationality or residence of the customer, provided that the jurisdiction is an EU member state or a reputable jurisdiction;
- the use of the electronic device (such as mobile applications or computer software) as a means of identity verification is administered or approved by the government of an EU member state or a reputable jurisdiction; and
- the software and/or hardware used by the customer to transmit data and by the subject person to read that data has to be administered or approved by the government of an EU member state or a reputable jurisdiction.

Where subject persons avail themselves of this measure to verify the identity of the customer, a print-out or an electronic copy evidencing that all personal details listed in Section 4.3.1 (i) were verified, should be retained on file. The print-out or electronic copy should also make reference to the system used to transmit and read data. Where the data obtained by the subject person only allows the partial verification of the personal details listed in Section 4.3.1(i), verification cannot be considered as having been completed and it would be necessary to use additional means of identity verification to fulfil one's obligations.

By way of example, it would be permissible for a subject person to use e-IDs or BankIDs in use within Scandinavian countries to verify the identity of a customer so long as the e-ID or BankID meets the criteria set out above. Other similar e-ID systems have also been developed or are being developed by other EU countries. Equally acceptable would be electronic identification and trust services developed within the context of Regulation (EU) No 910/2014.

4.3.2 Identification and Verification of Customers other than Natural Persons

The following sections set out how a customer other than a natural person is to be identified and verified. The extent of the identification and verification measures to be carried out is to be determined by adopting a risk-based approach, depending on the risk profile of the respective customer. In cases where the customer is a well-known, reputable organisation with a long history within a particular industry and substantial public information is available about it, standard evidence may well be sufficient to meet the CDD measures required to be carried out. However, where the subject person is entering into a business relationship or undertaking an occasional transaction with a customer that poses a higher than normal risk of ML/FT, additional CDD measures in the form of EDD should be applied by the subject person on a risk sensitive basis.

The measures outlined hereunder are to be applied in the same manner independently of the jurisdiction where the customer is registered or established. However, the particular jurisdiction may influence the reliability of the information obtained through company or similar registers. Subject persons should be aware that the type of documentation issued by registries, and standards of control over the same, may vary between different countries. Particular care should also be taken to ensure that the documents obtained have not been forged or tampered with, but are authentic.

Subject persons should also bear in mind that the systems in certain jurisdictions may be less transparent than in others and the documentation emanating from registries situated in such jurisdictions may not be sufficient to fulfil the identification and verification requirements laid out in the PMLFTR as further explained hereunder. Subject persons have therefore to consider taking additional measures to address these aspects.
Subject persons should moreover ensure that any documentation obtained for verification purposes is in a language that is understood by the subject person and its officers or employees carrying out the verification process. Where this is not the case, appropriate steps should be taken to ensure that the document does provide the necessary evidence to verify the identity details of the customer. Translations of any such documents should be reduced in writing and retained on file.

4.3.2.1 When the Customer is a Company

(i) Identifying a company

The subject person is required to first identify the company by gathering the following information:

(a) the company's official full name;
(b) the company's registration number;
(c) the company's date of incorporation or registration; and
(d) the company's registered address or principal place of business.

(ii) Verifying a company

The subject person must verify the information obtained on the company by referring to appropriate independent and reliable sources. It is up to the subject person to ascertain, following careful consideration of the risk posed by the customer, the appropriate sources. Documents which may be referred to by subject persons include, but are not limited to:

(a) the certificate of incorporation;
(b) a certificate of good standing (which is not older than three (3) months);
(c) a company registry search;
(d) the most recent version of the Memorandum and Articles of Association or other constitutive document;
(e) audited financial statements, annual returns, and/or tax returns for the previous or current year; and/or
(f) bank statements which are not older than six (6) months.

Original documents and documents downloaded from official registers are considered to provide the highest level of reliability. Where an original document is viewed, subject persons are required to keep either the original itself or a true copy of the document, signed and dated by an officer of the subject person, on file or in electronic form. Subject persons may also retain a scanned copy of the document by making use of the electronic system set out under Section 4.3.1.1(iii). Copies downloaded from the official registry website would similarly have to be retained by the subject person, together with a record of when and from which website the documents were downloaded.

Where documents are obtained in copies, subject persons should consider, based on the risk assessment carried out by the subject person, whether additional checks and safeguards should be applied to be satisfied of the robustness of its verification measures. This may include having the documents duly certified by the company's officials or by any of the persons referred to under Section 4.3.1.2(i)(b), as far as they are deemed to be reliable.

The subject person is also required to verify the legal status of the company. This should be done by confirming that the company has not been or is not in the process of being dissolved, struck off, wound up or terminated. The verification of such legal status is to take place either through a company registry search or by obtaining official registry documentation such as a good standing certificate. This documentation may be obtained either in original or as a certified true copy of the original, with the certification carried out by any one of the persons referred to in the preceding paragraph. If a search is carried out, then the subject person is to retain a record of the search and of the results it yielded.

(iii) Identifying the directors of a company

Once the verification is complete, the subject person must identify all the directors of the company.

In the case of directors who are natural persons identification consists in collecting the identification details referred to in Section 4.3.1(i).These can be collected by referring to the same sources that can be used to verify the identity of the company, such as:

(a) the list of directors contained in the most recent version of the Memorandum and Articles of Association,
(b) by performing a company registry search provided that the officers of the company are listed therein;
(c) by referring to a good standing certificate which is not more than three (3) months old, or
(d) by obtaining a copy of the directors' register of the company.

In the case of a corporate director(s), subject persons are required to obtain details of the corporate director's:

(a) official full name;
(b) registration number;
(c) date of incorporation or registration; and
(d) registered address or principal place of business.

It is important to note that the PMLFTR do not require subject persons to verify the identity of the directors but only to identify them. However, should an individual identified as a director be also acting as the company's agent as explained in Section 4.2.1 above or be also identified as one of the company's beneficial owners under any of the circumstances referred to in Section 4.2.2 above, then the subject person would also need to verify the director's identity and, where applicable, ensure that he is authorised in writing to act on behalf of the company.

(iv) Understanding the ownership and control structure

Subject persons are required to establish the ownership and control structure of the company. Whilst some structures are clear and easily understandable, other structures might be more complex and the use thereof without an obvious legitimate commercial purpose should give rise to concern and a possible increased risk of ML/FT. Subject persons should therefore undertake appropriate checks and gather information to be able to understand the ownership and control structure, and determine who is the customer's beneficial owner.

In order to comply with this obligation subject persons must obtain from the customer and maintain on file or in electronic form an explanation of the ownership and control structure of the company, as well as a corporate structure chart showing the ownership structure to the extent that would be required to determine who the beneficial owner is. Both the explanation and the structure chart should contain sufficient detail to allow the subject person to understand how the beneficial owner is linked to the customer and to allow eventual verification of the same as explained hereunder.

Once these are obtained, subject persons should then conduct independent research to verify the information on such corporate structure by consulting online commercial databases, company registries, relevant audited accounts or by obtaining certification by any of the persons referred

under Section 4.3.1.2(i)(b). The reliability of the measures to be adopted in the verification of the structure should be assessed by the subject person on a risk sensitive basis.

(v) Identifying and verifying the beneficial owners

Having established who the beneficial owner is, the subject person must ensure that the customer provides it with the personal details listed in Section 4.3.1(i)(a) for the beneficial owner. The subject person has to then verify the beneficial owner's identity by applying any of the verification measures referred to in Section 4.3.1 which may be most appropriate to the circumstances of the case.

In the case of a business relationship the subject person must also take all reasonable measures to ensure that the customer keeps the subject person informed of any changes in the beneficial ownership, such as by including an obligation in a letter of engagement (or by means of an exchange of correspondence) on the customer to keep the subject person updated. This is not to say that the subject person is divested of its responsibility for ongoing monitoring as this includes also taking active steps to ensure that the information held by the subject person is current and valid, especially where circumstances indicate that there has been a change in beneficial ownership.

Subject persons may also make reference to any Beneficial Ownership Registers which are maintained by Member States or other third countries. However, this is not to be considered as a substitute for the carrying out of CDD but as a tool to be used on risk-sensitive basis to assist the subject person to corroborate the information obtained.

There might be situations where no beneficial owner as defined in Table 7 part (a)(i) and (ii) of Section 4.2.2 can be identified.[48] In such cases, to the extent that the subject person has exhausted all means to identify a beneficial owner and it does not have any suspicions that there is anyone else that may fall to be so considered, subject persons are required to treat those persons who hold the position of senior managing officials of the company as beneficial owners and to identify and verify their identity accordingly. This would involve identifying and verifying the identity of the directors or persons occupying similar positions that effectively manage the company.

The subject person is obliged by the PMLFTR to keep a record of the actions taken to identify the beneficial owner as aforesaid, and why it was necessary to consider the senior management officials as beneficial owners.

4.3.2.2 When the Customer is a Listed Company

Where the customer is a listed company, i.e. it has its securities admitted to trading on a regulated market, subject persons may, to the extent that the requirements set out in this section are met,

[48] Second proviso of Regulation 2(1)(a) of the PMLFTR.

limit themselves to carrying out the measures referred to in Section 4.3.2.1 (i) and (ii), and refrain from carrying out the measures referred to in Section 4.3.2.1 (iii) to (v) hereabove.

To this end, the subject person has to establish whether:

(a) The company's securities are traded either on an EEA regulated market within the meaning of MiFID[49] or on a non-EEA regulated market. If the regulated market is located within the EEA, the subject persons has to document how it has ascertained the status of the regulated market. A full list of all regulated markets authorised within the EU is available on the following website:

https://registers.esma.europa.eu/publication/searchRegister?core=esma_registers_upreg

If the market is outside the EEA, the subject person has to ascertain that the jurisdiction where the said market is located is a reputable one and then establish that the market is subject to regulation in a manner similar to what is provided for within the EEA.

(b) The company is subject to disclosure requirements which ensure adequate transparency of ownership information. This can be assumed to be the case when the company's securities are traded on an EEA regulated market. Where the trading is taking place on a non-EEA regulated market, the subject person has to determine whether the company is subject to disclosure obligations which are contained in international standards and are equivalent to the specified disclosure obligations in the EU. The subject person should ensure that as a minimum the company is subject to specified disclosure obligations which are consistent with the specified articles of (i) the Prospectus Directive[50], (ii) the Transparency Obligations Directive[51], and (iii) the Market Abuse Directive[52] and with EU legislation made under the specified articles.

Subject persons are to note that prior to exercising the discretion allowed under this Section, they should ensure that no regulatory action has been taken either by the relevant supervisory authority or by the regulated market against the listed company for breaches of its disclosure requirements. Should this prove to be the case, the grounds for the application of this exemption would no longer subsist and the subject person would have to carry out all the measures set out in Section 4.3.2.1 as well as consider whether any such circumstances have an impact on the customer risk assessment.

Subject persons must retain on file records of the assessment they carried out and of the conclusions reached. Moreover, they should ensure that they review the position from time to time so as to ensure that there were no changes that would no longer allow the subject person to exercise the discretion allowed under this section (e.g.: delisting of the company).

[49] Directive 2014/65/EU on markets in financial instruments.
[50] Directive 2003/71/EC on the prospectus to be published when securities are offered to the public or admitted to trading and amending Directive 2001/34/EC, as amended from time to time.
[51] Directive 2013/50/EU on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market, as amended from time to time.
[52] Regulation (EU) No 596/2014 on market abuse (market abuse regulation).

4.3.2.3 When the principal is a commercial partnership

(i) Identifying a commercial partnership

The same procedure applicable to a company more or less applies to a commercial partnership. The subject person is required to first identify the partnership by gathering the following information, where applicable:

(a) the partnership's official full name;
(b) the partnership's registration number;
(c) the partnership's date of incorporation or registration; and
(d) the partnership's registered address or principal place of business.

(ii) Verifying a commercial partnership

The subject person must verify the information obtained on the customer by referring to appropriate independent and reliable sources. It is up to the subject person to ascertain, following careful consideration of the risk posed by the customer, the appropriate sources. Documents which may be referred to by subject person include, but are not limited to:

(a) the certificate of incorporation;
(b) a good standing certificate (which is not to be older than three (3) months);
(c) a registry search;
(d) the most recent version of the partnership agreement or other constitutive document;
(e) audited financial statements, annual returns, and/or tax returns for the previous or current year; and/or
(f) bank statements which are not older than six (6) months.

Original documents and documents downloaded from official registers are considered to provide the highest level of reliability. Where an original document is viewed, subject persons are required to keep a true copy of the document, signed and dated by an officer of the subject person, on file or in electronic form. Subject persons may also retain a scanned copy of the document by making use of the electronic system set out under Section 4.3.1.1(iii). Copies downloaded from the official registry website would similarly have to be retained by the subject person, together with a record of when and from which website they downloaded the documents from.

Where documents are obtained in copies, subject persons should consider, based on the risk assessment carried out by the subject person, whether additional checks and safeguards should be applied to be satisfied that adequate verification of the details of the customer has been made. These measures include obtaining documents duly certified by one of the general partners or an officer occupying a similar position, or by any of the persons referred to under Section 4.3.1.2(i)(b).

The subject person is also required to verify the legal status of the partnership. This should be done by confirming that the commercial partnership has not been or is not in the process of being

dissolved, struck off, wound up or terminated. The verification of such legal status is to take place by either making reference to a company registry search or by obtaining official registry documentation such as a good standing certificate. The said documentation may be obtained either in original or as a certified true copy of the original, with the certification carried out by any one of the persons referred to in the preceding paragraph. If a search is carried out, then the subject person is to retain a record of the search and of the results it yielded.

(iii) Identifying the persons vested with administration and representation of the commercial partnership

Once the verification is complete, the subject person must identify all the persons vested with the partnership's administration and representation.

In the case of partners who are natural persons, identification consists in collecting the identification details referred to in Section 4.3.1(i). These can be collected by referring to the same sources that could be used to verify the identity of the commercial partnership, such as:

(a) the list of partners contained in the most recent version of the partnership agreement or other constitutive document;
(b) by performing a registry search provided that the partners are listed therein;
(c) by referring to a good standing certificate which is not more than three (3) months old, if one is available, or
(d) by obtaining a copy of the appropriate register of the partnership that indicates who the persons vested with the partnership's administration and representation are.

In the case of corporate partners, subject persons are required to obtain details of the corporate partner's:

(a) official full name;
(b) registration number;
(c) date of incorporation or registration; and
(d) registered address or principal place of business.

It is important to note that the PMLFTR do not require subject persons to verify the identity of the partners but only to identify them. However, should an individual identified as a partner be also acting as the partnership's agent as explained in Section 4.2.1 above or be also identified as one of the partnership's beneficial owners under any of the circumstances referred to in Section 4.2.2 above, then the subject person would also need to verify the partner's identity and, where applicable, ensure that he is authorised in writing to act on behalf of the commercial partnership.

(iv) Understanding the ownership and control structure

Subject persons are required to establish the ownership and control structure of the partnership. Whilst some structures are clear and easily understandable, other structures might be more complex and the use thereof without an obvious legitimate commercial purpose should give rise to concern and a possible increased risk of ML/FT. Subject person should therefore undertake

appropriate checks and gather information to be able to understand the ownership and control structure, and determine who the customer's beneficial owner is.

In order to comply with this obligation subject persons must obtain from the customer and maintain on file or in electronic form an explanation of the ownership and control structure of the partnership, as well as a corporate structure chart showing the ownership structure to the extent that would be required to determine who the beneficial owner is. Both the explanation and the structure chart should contain sufficient detail to allow the subject person to understand the link between the beneficial owner and the customer, and to verify the same as further set out hereunder.

Once these are obtained subject persons should then conduct independent research to verify the information on such corporate structure by consulting online commercial databases, company registries, relevant audited accounts or by obtaining certification by any of the persons referred under Section 4.3.1.2(i)(b). The reliability of the measures to be adopted in the verification of the structure should be assessed by the subject person on a risk sensitive basis.

(v) Identifying and verifying the beneficial owners

Having established who the beneficial owner is, the subject person must ensure that the customer provides it with the personal details listed in Section 4.3.1(i)(a) for the beneficial owner. The subject person has to then verify the beneficial owner's identity by applying any of the verification measures referred to in Section 4.3.1 which may be most appropriate in the circumstances.

In the case of a business relationship the subject person must also take all reasonable measures to ensure that the customer keeps the subject person informed of any changes in the beneficial ownership, such as by including an obligation in a letter of engagement (or by means of an exchange of correspondence) on the customer to keep the subject person updated. This is not to say that the subject person is divested of its responsibility for ongoing monitoring, as this includes also taking active steps to ensure that the information held by the subject person is current and valid, especially where circumstances indicate that there has been a change in beneficial ownership.

Subject persons may also make reference to any Beneficial Ownership Registers which are maintained by Member States or other third countries.. However, this is not to be considered as a substitute for the carrying out of CDD but as a tool to be used on risk-sensitive basis to assist the subject person to corroborate the information obtained.

There might be situations where no beneficial owner as defined in Table 7 part (a)(i) and (ii) under Section 4.2.2 can be identified. In such cases, to the extent that the subject person has exhausted all means to identify a beneficial owner and it does not have any suspicions, subject persons are required to treat those persons who hold the position of senior managing officials of the partnership as beneficial owners and to identify and verify their identity accordingly. This would involve identifying and verifying the identity of the general partners that effectively manage the commercial partnership.

The subject person is obliged by the PMLFTR to keep a record of the actions taken to identify the beneficial owner as aforesaid, and why it was necessary to consider the customer's senior management officials as the beneficial owners.

4.3.2.4 When the Customer is a Foundation or Association

(i) Identifying a foundation or association

The same procedure applicable to a partnership more or less applies to a foundation or association. The subject person is required to first identify the foundation or association by gathering the following information:

(a) the foundation or association's official full name;
(b) the foundation or association's registration number, if applicable;
(c) the foundation or association's date of registration, if applicable;
(d) the nature, object and purpose of the foundation or association (e.g. discretionary foundation, fixed interest foundation, foundation set up by will, association set up to promote the interests of a particular group etc.); and
(e) the foundation or association's registered address.

(ii) Verifying a foundation or association

The subject person must verify the information obtained on the customer by referring to appropriate independent and reliable sources. It is up to the subject person to ascertain, following careful consideration of the risk posed by the customer, the appropriate sources. Documents which may be referred to by subject persons include, but are not limited to:

(a) the certificate of registration;
(b) a good standing certificate, if available, which is not to be older than three (3) months;
(c) a suitable registry search, where possible;
(d) the most recent version of the constitutive document;
(e) audited financial statement, annual returns, and/or tax returns for the previous or current year; and/or
(f) bank statements which are not older than six (6) months old.

Original documents and documents downloaded from official registers are considered to provide the highest level of reliability. Where an original document is viewed, subject persons are required to keep either the original itself or a true copy of the document, signed and dated by an officer of the subject person, on file or in electronic form. Subject persons may also retain a scanned copy of the document by making use of the electronic system set out under Section 4.3.1.1(iii). Copies downloaded from the official registry website would similarly have to be retained by the subject person, together with details of when and from which website the documents were downloaded.

Where documents are obtained in copies, subject persons should consider, based on the customer risk assessment carried out by the subject person, whether additional checks and

safeguards should be applied to be satisfied of the robustness of its verification measures. This may include having the documents duly certified by the foundation's administrators or by any of the persons referred to in Section 4.3.1.2(i)(b).

The subject person is also required to verify the legal status of the foundation or association. This should be done by confirming that the foundation or association has not been or is not in the process of being dissolved, struck off, liquidated or wound up. The verification of such legal status may take place by making reference to a registry search, if the foundation or association is registered in an appropriate registry, and such a search is possible, or by obtaining official registry documentation such as a good standing certificate. The said documentation may be obtained either in original or as a certified true copy of the original, with the certification carried out by any one of the persons referred to in the preceding paragraph. If a search is carried out, then the subject person is to retain a record of the search and of the results it yielded. The subject person could also consider requesting a signed declaration from the administrators of the foundation/association confirming the legal status.

It is up to the subject person to ensure, in accordance with its risk assessment (and bearing in mind, amongst other matters, the risk posed by the particular relationship to be established, the governing law of the foundation/association, the country of residence of the administrator and also the complexity of the structure) that appropriate measures are adopted to verify the existence of the foundation/association. Subject persons should bear in mind that documents and sources vary in their degree of reliability.

(iii) Understanding the ownership and control structure

Subject persons are required to establish the ownership and control structure of the foundation/association.[53] Whereas in some structures the beneficiaries have a fixed interest and are named, other structures might be more complex as the beneficiaries may be unnamed and may form part of a discretionary class of beneficiaries, or they may also not even be aware of the fact that they may benefit from the foundation.

For the purpose of establishing the beneficial ownership and control structure subject persons should obtain and maintain on file or in electronic form an explanation of the beneficial ownership and control structure of the foundation or association from the customer and verify such information by requesting the appropriate documentation, extracts thereof or declarations from the administrator.

In the case of purpose foundations and associations, subject persons are only required to establish the control structure of these entities.

[53] Regulation 7(1)(b) PMLFTR: "in the case of a body corporate, foundations, trusts and similar legal arrangements, the taking of reasonable measures to understand the ownership and control structure of the customer".

(iv) Identifying and verifying the beneficial owners

In the case of a foundation or an association, the PMLFTR consider the following as beneficial owners:

(a) the founder;
(b) the administrator or administrators;
(c) the guardian, protector or members of the supervisory council, where applicable;
(d) the beneficiaries or the class of beneficiaries as may be applicable; and
(e) any other natural person exercising ultimate control over the foundation by means of direct or indirect ownership or by other means.

Subject persons should not confuse the term 'beneficial owners' with the 'beneficiaries' of a foundation (in terms of the applicable law regulating foundations), as the latter covers exclusively those persons who can benefit from the structure (whether actually or potentially) while for AML/CFT purposes the term covers all of the above.

To the extent that all beneficial owners are individuals, the subject person has to ensure that the administrator discloses the identity of the beneficial owners by providing the personal details listed in Section 4.3.1(i). The subject person must then verify the identity of the same by applying any of the verification of identity measures set out in Section 4.3.1(ii) which may be most appropriate in the particular circumstances. Where for the purposes of point (a) to (c) above, a subject person can only identify and verify a body corporate, a body of persons or a legal arrangement, the subject person need not identify and verify who are the natural persons behind the same. In these circumstances, identification and verification can be carried out as indicated in Section 4.3.2. It is only where the beneficiary (as provided under point (d) above) is a body corporate, a body of persons or a legal that a subject person has to identify and verify the beneficial owners of the said body corporate, body of persons or legal arrangement as set out in Section 4.3.2.

Subject persons may also make reference to any Beneficial Ownership Registers which are maintained by Member States or other third countries. However, this is not to be considered as a substitute for the carrying out of CDD but only as a tool to be used on a risk-sensitive basis by the subject person to fulfil its CDD obligations.

In the case of purpose foundations and associations, subject persons must establish the purpose for which the foundation or association is set up or operates, which may be determined by referring to the constitutive document. In the case of a private foundation, situations may arise where the beneficiaries of a foundation are designated by particular characteristics or class and have, therefore, not yet been determined, and are not identified by name, the PMLFTR stipulate that the subject person need only identify and verify the identity of the beneficiaries at the time of pay-out or at the time the beneficiaries exercise their vested rights.[54]

[54] Regulation 8(4) of the PMLFTR.

Within the context of a private foundation, situations may arise where the beneficiaries are identified in the foundation deed but it may prove to be difficult to obtain verification of identity. Reference is being made to private foundations where either the beneficiary is not aware of his entitlement or the right to benefit from the foundation is subject to the discretion of the founder or to the realisation of a pre-determined condition. In these instances, the subject person can rely on the information contained in the foundation deed to identify the beneficiaries and seek on a risk sensitive basis to obtain such additional information as may be necessary to establish an adequate risk profile, and then obtain the rest of the identification details and verify the identity of the beneficiaries at the time of pay-out or at the time the beneficiaries exercise their vested rights.

Where the subject person has entered into a business relationship with the foundation or association, the subject person must also take all reasonable measures to ensure that the same keeps the subject person informed of any changes to the purpose of the foundation or association, or the beneficiaries, such as by including an obligation in a letter of engagement (or by means of an exchange of correspondence) on the customer to keep the subject person updated. This is not to say that the subject person is divested of its responsibility as carrying out ongoing monitoring includes also taking active steps to ensure that the information held by the subject person is current and valid, especially where circumstances indicate that there has been a change in beneficial ownership.

4.3.2.5 When the Customer is a Trust/Trustee

Trusts vary considerably in nature and in size. Whilst there are trusts set up for purely commercial transactions (such as employee benefit trusts and share option structures, unit trusts operating as collective investment schemes, trusts operating in the context of syndicated loans or to hold securities), there are also trusts which are set up to safeguard the interests of vulnerable persons (such as spendthrifts, persons with special needs or some disability, the aged and frail etc.) or under testamentary arrangements. CDD measures to be applied by the subject person will need to be proportionate to the risks that the trust of different sizes, areas of activity and nature of the business being conducted, present.

Where a trust has no legal personality, as is the case with trusts governed by Maltese law, the trustees entering into the business relationship with the subject person, or undertaking an occasional transaction through the subject person, in their capacity as trustees of the particular trust, would be considered to be the customers for CDD purposes. In cases where the trust has a separate legal personality, the trust should be categorised as the customer for the purposes of undertaking CDD measures and the trustees would be the persons vested with the administration of the trust (similar to directors in the case of companies and administrators in the case of foundations that have legal personality). Nonetheless, the obligations outlined in this section would be applicable in both instances.

(i) Identifying the trust

The subject person is required to identify the trust by obtaining the following information:

(a) the full name of the trust;
(b) the nature, object and purpose of the trust (e.g.: discretionary trust, testamentary trust, bare trust);
(c) the country of administration and the proper (or applicable) law; and
(d) in jurisdictions where the trust has legal personality, the registration number, if applicable.

(ii) Verifying the trust

The details obtained on the trust must be verified by making reference to appropriate independent and reliable sources. Verification should be undertaken by either requesting a copy of the trust instrument from the trustee (if possible, bearing in mind that trusts typically relate to rather personal or private matters) or an extract of the relevant parts of the trust instrument. Alternatively, verification can be carried out by obtaining a signed declaration by the trustee containing the information listed in paragraphs (a) to (d) above. Where trusts are registered in an official registry, another alternative available to the subject person is to make reference to these registers though particular attention has to be made to any limitations on registration therein which may limit the quality and reliability of the information reported.

It is up to the subject person to ensure, in accordance with its customer risk assessment (and bearing in mind, amongst other matters, the risk posed by the particular relationship to be established, the governing law of the trust, the country of residence of the trustee and also the complexity of the structure) that appropriate measures are adopted to verify the existence of the trust. Subject persons should bear in mind that documents and sources vary in their degree of reliability.

Where documents are obtained in copies, subject persons should consider, based on the risk assessment carried out by the subject person, whether additional checks and safeguards should be applied to be satisfied of the robustness of its verification measures. This may include obtaining documents duly certified by the trustee or any of the persons referred to in Section 4.3.1.2(i)(b) above, as far as they are deemed to be reliable.

(iii) Identifying and verifying the beneficial owners

For the purpose of the PMLFTR, within the context of trusts, the term beneficial owner covers:

(a) the settlor;
(b) the trustee or trustees;
(c) the protector, members of a supervisory council, guardian or enforcer where applicable;
(d) the beneficiaries or the class of beneficiaries as may be applicable; and
(e) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means (refer to Section 4.2.2.2).

Subject persons should not confuse the term 'beneficial owners' with the 'beneficiaries' of the trust as the latter term covers exclusively those persons who can benefit from the structure (whether actually or potentially) while for AML/CFT purposes the beneficial owners are all the persons indicated in (a) to (e) above. Moreover, it is equally important to note that the individuals referred to in paragraph (e) above, where present, may not be named in the trust deed itself.

To the extent that all beneficial owners are individuals, the subject person has to ensure that the trustee discloses the identity of the beneficial owners by providing the personal details listed in Section 4.3.1(i). The subject person must then verify the identity of the same by applying any of the verification of identity measures set out in Section 4.3.1(ii) which may the most appropriate in the specific circumstances of the case. Where for the purposes of points (a) to (c) above, a subject person can only identify a body corporate, a body of persons or a legal arrangement, the subject person need not identify and verify who are the natural persons behind the same. In these circumstances, identification and verification can be carried out as indicated in Section 4.3.2. It is only where the beneficiary (as listed under point (d) above) is a body corporate, a body of persons or a legal arrangement that a subject person has to identify and verify the beneficial owners of the said body corporate, body of persons or legal arrangement as set out in Section 4.3.2.

In carrying out the identification of the beneficial owners, subject persons may also make reference to Beneficial Ownership Registries which are maintained by Member States or other third countries. However, particular attention has to be made to any limitations on registration therein which may limit the quality and reliability of the information reported. Moreover, consulting these registers is not to be considered as a substitute for the carrying out of CDD but as a tool to be used on a risk-sensitive basis to assist the subject person to carry out the same.

In the case where the beneficiaries of the trust are designated by particular characteristics or class and have, therefore, not yet been determined, and are not identified by name, the PMLFTR stipulate that the subject person need only identify and verify the identity of the beneficiaries at the time of pay-out or at the time the beneficiaries exercise their vested rights.[55]

It is acknowledged that situations may arise in which the beneficiaries may be identified in the trust deed but they may either be unaware of their entitlement under the trust or their actual benefit from the trust depends on the trustee's discretion or the realisation of a pre-determined condition. In these circumstances, a subject person may opt to identify the beneficiaries on the basis of the information contained in the trust instrument, or any other document used to verify the trust, and seek on a risk sensitive basis to obtain such additional information as may be necessary to establish an adequate risk profile. The subject person would then eventually collect any additional identification information that may become necessary and carry out verification of identity one an actual pay-out is made.

In the case of purpose trusts, subject persons must establish the purpose for which the trust is set up or operates, which may be determined by referring to the constitutive document. In the case of a business relationship the subject person must also take all reasonable measures to

[55] Regulation 8(4) of the PMLFTR.

ensure that the trustee keep the subject person informed of any changes to the nature, purpose or objects of the trust, or changes to the beneficiaries or the trustees, such as by including an obligation in a letter of engagement (or by means of an exchange of correspondence) on the customer to keep the subject person updated.

This is not to say that the subject person is divested of its responsibility as carrying out ongoing monitoring includes also taking active steps to ensure that the information held by the subject person is current and valid, especially where circumstances indicate that there has been a change in beneficial ownership.

4.3.3 The Agent

As already stated in Section 4.2.1, the person requesting a subject person to establish a business relationship or to carry out an occasional transaction may not be the customer but the agent of the customer. In these circumstances, the subject person is obliged not only to identify and verify the customer as set out in the sections hereabove but must also carry out the following additional measures.

(i) Identifying and verifying the agent

Depending on the nature of the agent, identification of the agent and verification of its identity is to be carried out as set out in the sections hereabove. However, subject persons are to note that where the agent is a legal entity, the subject person does not have to:

(a) Establish the agent's ownership and control structure;
(b) Identify who are the agent's beneficial owners; and
(c) Identify and verify the identity of the legal entity's officers and/or employees who provide instructions to the subject person.

(ii) Authorised to act on behalf of the customer

The subject person has to ensure that the agent is duly authorised in writing to act for and on behalf of the customer. He is therefore to obtain and retain on file either the original or a copy of the authorisation granted by the customer to the agent.

In this regard, the subject person should also seek to understand the rationale behind such arrangement and why the customer did not seek to establish the business relationship or carry out the occasional transaction directly himself.

4.4 The purpose and intended nature of the business relationship and the Customer's Business and Risk Profile

Introduction

In terms of Regulation 7(1)(c) of the PMLFTR, subject persons are required to assess and, where appropriate, obtain information and/or documentation on the purpose and intended nature of the business relationship. In addition, subject persons are also required to establish the business and risk profile of the customer. These requirements entail gathering and analysing information to:

Determine whether a service and/or product being provided makes sense in the customer's situation and profile;

(a) Assess the customer's intention in acquiring a particular service and/or product;
(b) Contribute to its customer risk assessment and ensure that the customer falls within the subject person's risk appetite;
(c) Determine the appropriate risk mitigating measures to be adopted; and
(d) Carry out meaningful ongoing monitoring as it will be able to understand and identify the expected behaviour, including the expected nature of transactions or activities, of the customer throughout the business relationship.

4.4.1 Purpose and Intended Nature of the Business Relationship

Subject persons have to understand why a customer is requesting its services and/or products and how the same is expected to be used in the course of the business relationship.

The purpose of certain business relationships can be self-evident given the nature and purpose of the service and/or product required (e.g.: a customer opening an account on a gaming website. Other relationships may require a subject person to assess and, where necessary, obtain information and/or documentation from the customer in order to truly understand why the business relationship is being set up.

> Example: A foreign beneficial owner setting up a company in Malta for which the subject person is also to provide directorship services – the subject person should seek to determine the purpose behind the company's incorporation in Malta, what it's activities are to be and other background information.

In all cases, subject persons should have a good understanding of how the business relationship will be used, in order to carry out proper monitoring, as well as to be able to determine that the product or service requested makes sense in view of the profile of the customer. Opening a bank account to be used in the context of a commercial activity would require the subject person understanding the nature of this commercial activity (e.g. product or service provided, where is it established, main markets targeted etc.).

4.4.2 The Customer's Business and Risk Profile

The additional obligation resulting from Regulation 7(1)(c) is that of establishing the customer's business and risk profile. Risk has already been considered in some detail in Chapter 3 but in this particular instance, a subject person is additionally required to collect information that will allow him to further strengthen its customer risk assessment as well as have an idea of what he can expect to take place in the course of a business relationship in terms of activity and/or funds transacted using its services and/or products.

To this end, a subject person must collect information on and, where necessary, back it up with documentation such as:

(a) Information on the nature of and details concerning the business/occupation/employment of the customer;
(b) Any other activity in addition to (i) above from which the customer derives his **wealth** (e.g.: inheritance);
(c) The expected **source and origin of the funds** to be used throughout the business relationship; and
(d) The anticipated level and nature (including expected value and frequency of transactions) that is to be undertaken throughout the relationship.

Notwithstanding the above list, certain information may not be relevant in all scenarios and relationships. For instance, gathering information on the anticipated level and nature of activity in the case of long-term insurance policies with fixed monthly *premia* may be unnecessary as it would not add any value, but gathering such information in connection with an investment account is crucial for understanding the frequency and level of investment that the customer is expected to carry out. Similarly, in cases where, for instance, a customer is investing money which is claimed to have been accumulated over time, information on the current business/occupation/employment would certainly need to be complemented with information on the source that generated such wealth (e.g.: previous employment, inheritance or business profits). In other instances, it may be possible for the subject person not to collect information required for the purposes of understanding the customer's business and risk profile if they are able to rely on statistical data as explained further on hereunder.

Thus, the kind of information gathered will vary depending on the risk profile of the customer and the service or product being requested. The level of information to be obtained, and whether such information should be backed up by documents, will depend on the risk assessment of the particular case at hand. Moreover, where the collection of such information is deemed relevant, subject persons are not to limit themselves to obtaining information of a generic nature – a mere reference to 'business', 'employment' or 'inheritance' would never be deemed sufficient to meet this obligation independently of the risk presented.

In carrying out this exercise, subject persons should be risk-sensitive in their approach, and should nevertheless remain mindful of a number of principles, particularly those relating to the protection of their customer's personal data. Ideally, subject persons should refrain from requesting data (including information and documentation) that is disproportionate, excessive or irrelevant. Disproportionate or excessive requests include anything that is too instrusive when other, less instrusive data would fulfill the same purpose. Irrelevant data includes anything that

does not add any value to the business and risk profile, does not serve to mitigate any risks, or does not provide any reassurance relevant to the ML/FT risks.

4.4.3 The Source of Wealth and the Source of Funds

The information items referred to in (i) and (ii) above constitute what is usually termed as the customer's 'source of wealth', i.e. the economic activity or activities which generate the customer's wealth. This may be comprised of, for instance, income through employment or business, or inheritance. The term 'source of funds' refers to the activity, event, business, occupation or employment generating the funds used in a particular transaction, or to be used in future transactions.

Whereas the source of wealth is usually identified at the beginning of the business relationship and the information thereon is updated from time to time when new material developments arise in the course of the business relationship, subject persons are required to identify the source of funds of individual transactions in accordance with the obligation of ongoing monitoring as set out below. Information on a customer's source of wealth and expected source of funds collected at the outset of a business relationship will assist the subject person in further understanding the actual ML/FT risk it is exposed to, especially when it comes to the customer risk factor.

The extent and level of detail of the information required as to the source of wealth and the expected source of funds, and whether and how much documentation should be requested to substantiate the information provided by the customer, would depend on the customer risk assessment. Ultimately, a subject person should be able to form a reasonable conclusion that the customer's wealth has been accumulated legally, and that subsequent funds that will be used to carry out transactions in the course of a business relationship are legitimate. In all cases, subject persons should be aware of the data collection principles outlined above and should refrain from requesting information or documentation which is excessive or irrelevant in view of the particular customer profile.

The collection of information on a customer's source of wealth and expected source of funds will assist the subject person in the carrying out of its ongoing monitoring obligations as explained hereunder. Where the subject person detects activities or transactions which appear to be unusual when considered vis-à-vis any such information, the subject person is to collect information, and if necessary supporting documentation, on the actual source of funds used to finance the unusual activity or transaction.

While establishing a customer's source of wealth and his source of funds are express requirements in the case of a business relationship, it should be borne in mind that determining a customer's source of wealth and source of funds may still be required in the context of an occasional transaction. Where the ML/FT risk within an occasional transaction is assessed to be high, and therefore requiring the taking of enhanced due diligence, it is very likely that the most effective measure that can be taken is to query how the funds being used have been acquired and whether this makes sense considering the customer's source of wealth. In any such

circumstances, subject persons would therefore still be expected to establish a customer's source of wealth and source of funds, unless they apply alternative measures that can be shown to be equally effective to address the risks identified.

4.5 Ongoing monitoring

4.5.1 Overview of the duty to conduct ongoing monitoring

Once a business relationship is formed, Regulation 7(1)(d) of the PMLFTR requires subject persons to monitor the same. This requirement comprises two key elements:

(a) Scrutiny of Transactions

The scrutiny of transactions consists in using the subject person's knowledge of the customer (including the information gathered on the purpose and intended nature of the business relationship and the customer's business and risk profile) to identify any transactions that are unusual. The term unusual includes transactions which are unusual by their very nature (as they are suspicious, illogical, unnecessarily complex, or unreasonable), as well as those which are inconsistent with the customer's profile or are significantly different to what is usually carried out or requested by the customer. Moreover, the PMLFTR expressly require subject persons to examine the purpose and background of all complex and unusually large transactions, and unusual patterns of transactions, which do not have any apparent or economic lawful purpose, and increase the degree and the nature of ongoing monitoring in order to determine whether the transactions are suspicious.[56]

An unusual transaction should serve as a red flag or a trigger event for the subject person to assess the situation and request additional information or documentation to be able to establish whether the transaction is suspicious and ought to be reported in terms of Regulation 15 of the PMLFTR, or whether there are legitimate explanations, such as changes in the activity carried out by the customer, in which case the subject person may need to update the customer risk assessment, the CDD information and documentation it holds and/or enhance the CDD measures it is applying to the particular business relationship. Ongoing monitoring thus complements and builds upon the initial customer due diligence measures carried out during the customer on-boarding, so as to further ensure that the services and/or products of the subject person are not misused for ML/FT purposes.

(b) Keeping information, documents and data held on the customer up-to-date

Subject persons have an obligation to ensure that information, documents or data relative to the customer, as well as any assessment thereof, remain up-to-date and relevant, whether it is through the periodic review and updating thereof or following certain changes in the business relationship, i.e. a trigger event.

[56] Regulation 11(9) PMLFTR.

Trigger events may include the provision of additional services and/or products to an already existing customer or changes to the activities carried out by the customer, such as changes in amount of periodic investments or changes in a company's trading or commercial activities.

This ensures that information and documentation is current and valid, and the customer risk assessment actually reflects the real ML/FT risk arising from a business relationship. In turn, the subject person would be in a better position to adjust any CDD or other mitigating measures, including the level of ongoing monitoring, to address the actual ML/FT risks.

4.5.2 Transaction Monitoring

4.5.2.1 The purpose of transaction monitoring

Through the monitoring of customer transactions or activities, subject persons should be in a better position to:

(a) Identify behaviour or transactions which diverge from the usual pattern of transactions, do not fit within the customer's profile, or are otherwise not in line with what is normally expected from the customer, and which therefore need to be questioned in further detail;
(b) Identify suspicious activity in relation to which a STR is to be filed with the FIAU;
(c) Determine whether the initial risk assessment requires updating, and whether, in view of the updated risk assessment or other considerations, the business relationship remains within the risk appetite of the subject person and, if so, understand whether the level of CDD needs to be adjusted in view of any changes from the initial risk understanding.

4.5.2.2 Identifying unusual transactions

In terms of Regulation 7(2)(a) transaction monitoring comprises the scrutiny of transactions undertaken in the course of a business relationship to ensure that these are consistent with the subject person's knowledge of the customer and of his business and risk profile. The following is a (non-exhaustive) list of factors that can be used to detect transactions that are unusual, i.e. that present a divergence from how the product or service is usually used or from the expected or known transactional pattern of the customer:

(a) A significant change in the value of individual transactions or in the overall volume or frequency of transactions;
(b) The carrying out of a number of transactions in rapid succession one to the other such as the purchase and immediate resale of immovable property, securities etc. or the deposit and withdrawal in rapid succession of funds/securities on an account;

(c) A change in the geographical destination or origin (or other form of connection) of a transaction and/or a change in the usual parties that a customer transacts with;
(d) A possible change in the source of funds of the customer.

These factors are especially important when one considers the express obligation imposed on subject persons to examine the purpose and background of complex and unusually large transactions, and unusual patters of transactions, which do not have any apparent or economic lawful purpose. However, in this case regard must also be had to the amounts involved in the transactions. Even if these may be within the normal pattern of transactions carried out by the customer, should the amount involved be unusually large, the subject person would still have an obligation to understand the purpose and nature of such a transaction.

Assessing unusual transactions

Determining whether there is a reasonable explanation for an unusual transaction requires the collection of information and/or documentation which show that there is a legitimate reason for that particular transaction or for that divergence from the customer's known pattern of activity or transactions. For this purpose, a subject person may need to request information and/or documentation on one or a combination of the following:

(a) The source of funds of that transaction;
(b) Any new operational activities;
(c) Any significant relevant changes relating to the customer, such as a change in occupation; and
(d) Any other information that the subject person deems reasonably necessary to be satisfied that the funds are derived from legitimate sources.

As explained earlier on in this document, the level of data to be obtained should allow the subject person to come to a reasonable conclusion on the legitimacy of the transaction, but should not be excessive, disproportionate or irrelevant, and the requests should make sense in the context of the transaction and the customer.

Where notwithstanding the information and/or documentation received, the subject person is not satisfied with the explanations provided or has doubts as to the veracity of the documentation provided, the subject person has to consider whether there are sufficient grounds to file a STR. At times, customers may become uncomfortable when faced with demands for more information or documentation. This may be understandable. However, where the customer displays an unreasonable reluctance to cooperate, subject persons should similarly consider filing a STR.

By way of example, a Company Service Provider (i.e. the subject person) is providing directorship services to a company (i.e. the customer). Through the business and risk profile, the subject person had established that the customer's business activities will take place within the EU. Eventually, through ongoing monitoring systems, the subject person detects a number of transactions to and from non-EU jurisdictions. These transactions are flagged through the ongoing monitoring procedure and the customer is requested to to explain the reason for these transactions. The customer explains that it sought new markets for its products and services, and had managed to obtain a foothold in these third countries. To support this information, the

customer also makes available a series of agreements and related invoices concluded with other entities situated in these third countries.

Following due consideration of the explanations and documentation provided by the customer, including independent checks on the non-EU country entities with which the customer concluded agreements, it is determined that the customer's business has legitimately expanded to these countries. The subject person's risk assessment considers these jurisdictions not to be high risk and thus decides that the relationship still falls within its risk appetite. Nevertheless, the subject person updates the business and risk profile of the customer to reflect these developments.

Had the subject person found the explanation provided by the customer to be unconvincing or the documentation to present signs of forgery, the conclusion would have been different as the subject person would also have had to consider whether there were any grounds to submit a STR.

4.5.2.3 How to conduct transaction monitoring

Transaction monitoring can take place in a number of ways. Any determination as to when and how to conduct the same will depend, amongst other factors, on the activity or business carried out by the subject person, the volume of such activity, the number of clients, whether business is conducted solely remotely, and the risk ratings ascribed to customers. It is therefore possible that the most effective manner in which to carry out transaction monitoring require the adoption of more than one of the methods described hereunder.

Transactions can be monitored:

(a) *In real time (**pre-transaction monitoring**), whereby transactions or activities are reviewed as they take place or prior to finalization.*

Pre-transaction monitoring is more commonly applied in face-to-face scenarios and allows more control and reassurance, as suspicious or unusual transactions may be detected prior to execution and put on hold for further determination, where possible. In such cases it is crucial that persons dealing directly with customers are, as far as reasonably possible, in a position to detect such transactions by, for instance, being aware of the trigger events or red flags associated with the product or service, or even understanding the expected transactions or use of a particular business relationship.

Pre-transaction monitoring can also be applied in non face-to-face situations where transactions are not carried out instantaneously but allow for receipt of an order and its subsequent execution at different times.

Pre-transaction monitoring is particularly suited as an EDD measure for high risk clients and transactions, which would be allowed to transact upon the scrutiny of all or selected prospective transaction/s.

(b) *After the event (**post-transaction monitoring**), where transactions and patterns are reviewed after execution.*

Certain relationships or services do not easily permit transactions to be monitored and flagged in real time. Nevertheless, subject persons are still expected to monitor the relationship, assess any unusual or suspicious transactions and take any necessary action, including filing a STR when necessary, even after the event. Post-transaction monitoring is also an essential tool in detecting any patterns of transactions that raise suspicion and/or do not match the customer's profile.

Subject persons should keep in mind that pre-transaction monitoring alone may not always be suitable to detect unusual or suspicious transactions. For instance, a customer depositing a large amount of cash by affecting a number of deposits each at different branches of the same bank would not raise any suspicion with the tellers at the respective branches. A proper post-transaction monitoring system would however link the individual transactions carried out by the same person and trigger an alert.

Thus, although a subject person may be able to stop a face-to-face transaction from being executed until a determination has been reached, an effective transaction monitoring system would ideally be complemented by adequate post-transaction monitoring.

As regards how to detect unusual or suspicious transactions, there are a number of methods and systems that can be adopted and which, depending on the particular circumstances of the subject person's activities, are equally valid. As already highlighted above, an effective monitoring system may require the adoption of more than one of the methods referred to hereunder. Transaction monitoring can therefore be carried out:

(c) On the basis of a customer's specific profile

As explained in section 4.4 above, the business and risk profile built on the customer should allow a subject person to understand what kind of transactions or behaviour are expected through the course of the business relationship. This means that the subject person has defined or is aware of the set of parameters or factors within which transactions are considered normal for that particular customer, and which therefore do not require further assessment. Thus, a subject person would not necessarily need to carry out further assessment on transactions to and from a set of jurisdictions, or of a particular value and frequency or combination thereof etc., as such transactions or behaviour would be consistent with the subject person's knowledge of the customer. However, once there are variations that fall outside these pre-set parameters, the subject person would be expected to question those variations.

(d) By comparing against peer group information

Subject persons may adopt systems whereby customers of the same characteristics and risk rating are grouped and their statistics are extracted and utilised to create the profile of an average customer within that group for particular products or services. Transactions and behaviour of individual customers may then be compared against the average or expected transactions of that peer group profile such that anything falling outside would trigger an alert for further assessment by the MLRO.

Comparing peer group information is only possible where the subject person has a sufficiently wide customer-base from which to obtain substantial statistical data. Alternatively, depending

on the activity of the subject person, it may be possible to create an average customer profile based on official economic indicators such as average national income, average disposable income etc., issued by national public bodies or reputable financial institutions.

Subject persons are to note that such a system would not be ideal in high-risk scenarios, which already present characteristics that fall outside the norm and require more targeted ongoing monitoring measures.

(e) On the basis of detection rules

Detection rules comprise a set of thresholds, scenarios and other parameters against which individual transactions as well as series of transactions over time are analysed. When a pre-defined detection rule is met, an alert is raised for further assessment by the MLRO.

In order to be effective, detection rules must be relevant to the particular product or service being offered and to the business and risk profile of the customer. Detection rules would need to be periodically tested and fine-tuned to ensure on the one hand that transactions and patterns are actually being detected and that on the other hand they are not generating too many false positives. Similarly, detection rules would need to be updated to reflect changing trends and typologies, particularly with respect to terrorism financing.

These rules would need to take into account trigger events and red flags that are relevant to the services or activities of the subject person, as well as a number of other factors and/or combinations thereof. The following are some examples of what may need to be factored into detection rules:

(a) The specific product or service being offered;
(b) The customer's risk rating;
(c) The anticipated level and value of transactions as determined through the business and risk profile;
(d) The anticipated jurisdictional connections as determined through the business and risk profile;
(e) The value of transactions when taking into account the customer's background, occupation, and claimed source of wealth/source of funds;
(f) The jurisdictional connections which the subject person;
(g) The distribution channels (such as face to face or remote transactions);
(h) Whether a transaction is in cash or not;
(i) Whether a dormant account has suddenly become active.

Depending on the subject person's activity, the system may need to be configured to take into account combinations of rules. For instance, a system may be set to raise an alert when transactions in or out of specific jurisdictions reach a particular frequency within a period of time, regardless of the value. This may be useful in detecting transactions that may be related to terrorist financing.

Automated Monitoring Systems

It is up to the subject person to determine whether a system should be automated or whether manual monitoring would equally yield the required results. Such a decision would depend on the size of the subject person, the number of clients and transactions, the level of risks to which it is exposed, the costs incurred, and so on. With that said it is expected that subject persons processing hundreds of transactions daily adopt automated systems, unless they can provide sufficient justification as to how transactions are being monitored effectively and efficiently. Such subject persons may find that automated monitoring systems permit more accurate, detailed reports on alerts.

The following questions may be relevant when considering the automated system to be adopted:

(a) Whether the system generates or permits the creation of a report demonstrating the reasons why an alert was raised and which rules or parameters were considered;
(b) Whether the system can be adapted with relative ease and efficiency to cater for changes, new trends and typologies;
(c) Whether the system has functionalities to learn from previous false positives and fine-tune its operations.

Subject persons are expected to be able to demonstrate a clear understanding of certain relevant aspects of the system, namely the kind of scenarios, typologies and detection rules applied, how the system is compatible with the products or services offered by the subject person, and how it can be adjusted to match different profiles or adapt to changes in the relationship, among others. Subject persons would also need to know whether and how a system maintains an audit trail of the alerts raised.

Regardless of the systems and methods adopted to carry out transaction monitoring, subject persons must carry out periodic tests and reviews to assess the effectiveness of the alerts being generated, and should moreover be able to demonstrate a good understanding of their operation.

a) Ongoing monitoring of high-risk scenarios

Adopting a risk-based approach towards the application of AML/CFT obligations invariably means that subject persons must apply a stricter level of ongoing monitoring of high-risk relationships to mitigate the risks of ML/FT.

Adjusting the procedures to cater for high risk customers involves increasing the frequency and nature of the transaction monitoring carried out. This may mean:

(a) Carrying out regular reviews of transactions to detect any warning signs or patterns;
(b) Applying stricter or more stringent detection rules;
(c) Applying lower transaction value thresholds;
(d) Giving more weighting to factors such as higher value transactions and dealings with other jurisdictions;
(e) Adjusting the thresholds for different services and products within the same relationship;
(f) Increasing the level of control by placing higher-risk customers under more vigilant watch;
(g) Consider the application of pre-transaction monitoring.

Subject persons should identify those scenarios which would constitute suspicious or unusual activity within a high risk scenario. In such cases, subject persons should as far as reasonably possible use pre-transaction monitoring procedures, in order to ensure that transactions in high risk scenarios can be appropriately scrutinized prior to execution.

Training

The training of employees plays a vital role in the effectiveness of a subject person's ongoing monitoring systems. Employees should be properly trained to identify unusual or suspicious transactions and activities which may be related to ML/FT, and the red flags associated with the particular customer, service or product.

Employees dealing with customers directly, particularly when it comes to transactions that take place on a face to face basis, must be knowledgeable in AML/CFT measures, the subject person's AML/CFT policies and procedures as well as in the recognition of red flags and dubious or suspicious transactions. Such employees are best positioned to recognize and detect suspicious or unusual actions and flag them for further assessment prior to execution, where this is permitted.

In this regard, reference should be made to Chapter 7 on the nature of training to be provided to employees and officials of subject persons.

4.5.3 Ensuring that documents, data and information held on the customer are kept up-to-date

In carrying out their ongoing monitoring obligations, subject persons are also tasked with '*ensuring that the documents, data or information held by the subject person are kept up-to-date*'.[57] The documents, data or information (hereinafter collectively referred to as 'information') referred to in this section comprises the information obtained in fulfilment of CDD obligations, particularly those required under Regulation 7(1)(a)-(c) and Regulation 7(3).

Purpose

Business relationships are not static, and the circumstances surrounding it and the customers themselves are very likely to change over time. The customer risk assessment as well as the initial CDD measures and any other mitigating measures carried out, would have all been based on the information obtained on the customer prior to the establishment of the business relationship.

Such information must therefore remain relevant, accurate and sufficient if the subject person is to have a clear understanding of the ML/FT risks it is exposed to and that the measures it has put in place are actually effective. Hence why it is essential that subject persons adopt policies and procedure to keep information up-to-date. Moreover, changes which affect the risk profile and, possibly the customer risk assessment, should lead the subject person to update its customer risk assessment accordingly.

[57] Regulation 7(2)(b) PMLFTR

Ensuring that information is kept up-to-date should not therefore be considered as a requirement to carry out afresh the CDD measures that would have been applied at the inception of the business relationship, unless the subject person has doubts as to the information collected as reflected in Regulation 7(7) of the PMLFTR.

Information Monitoring Methods

Updating can be carried out through one or a combination of methods. The following are some examples of the methods most commonly used, but it does not exclude the possibility that there may be others that are equally effective. It is up to the subject person to determine the best approach towards keeping information up-to-date, depending on a number of factors relating to the subject person itself (size, number of customers, type of services offered, resources, etc.), and the customer base (risk rating, range of products offered), among other considerations. The methods adopted may also vary to better address the circumstances presented by different customer groups or services.

Trigger events

At times, updating may be prompted by certain trigger events. For instance, an assessment of an unusual transaction or pattern of transactions carried out in accordance with the previous section may indicate that there has been a (legitimate) change in the business relationship or in certain relevant circumstances of the customer, and the business and risk profile may need to be adjusted to ensure that all relevant factors are being taken into account. This may entail obtaining new information or documentation to substantiate the new circumstances.

By way of example, a customer may have been requested to provide information on the source of funds following a gradual but significant increase in transaction value. The subject person subsequently determines that the customer, only known to be a student, has graduated and has set up a small consultancy office which is bearing fruit. This new information on the background (occupation) of the customer is considered to affect the customer's profile, which would need to be updated accordingly. Moreover, the subject person would have to consider whether its customer risk assessment and the mitigating measures adopted on the basis of the same are still valid or if they need to be revisited to better address the new level of ML/FT risk posed by the particular business relationship.

Other times, updating would be necessary in light of a request for a new product or service which presents different ML/FT risks. In such cases the subject person would need to consider whether the information held is sufficient or whether it would be best to request more detailed information on, for instance, the anticipated source of funds. A request for information received from the FIAU or the Police on a particular customer may also be a trigger for the subject person to take a closer look at how it had risk assessed and rated the given customer and what it knows about him.

Trigger events can also be applied in relation to the updating of documentation which have a set expiry date such as identification documents. A customer who has been inactive for a

considerable period of time is unlikely to pose any ML/FT risk and therefore even if the documentation used to verify his identity may have expired, requesting fresh copies would not be addressing any particular risk. However, if the customer attempts to once more make use of the subject person's services or products, any activity should be made subject to the customer providing copies of fresh identification documents prior to any such activity taking place.

Periodic Reviews

Another method that may be applied to ensure that information is up-to-date is that of periodic reviews. Depending on the level of risk, subject persons may set up a schedule to review the information they hold on file at regular intervals even in the absence of an event that may point at a change in the given business relationship. Periodic reviews may be particularly useful when it comes to the documentation collected for verification of identity purposes, where the subject person sets out a schedule for the review of the same and requests updated copies where it results that this has expired. As this process necessarily needs to be risk-based, the timeframe for the review of business relationships considered to present a high risk of ML/FT should be more frequent than those deemed to be low risk.

Subject persons may take the following factors into consideration when it comes to deciding how frequently information needs to be updated, and to which extent:

Frequency

(a) The customer's risk rating;
(b) The kind of information to be updated (e.g.: a remote entity may determine that the residential address should not be updated frequently as long as the customer is transacting from within the same jurisdiction);
(c) Whether there are any risks that may be mitigated through updating.

Extent

(a) The factors listed above;
(b) The relevance of the information with respect to CDD and AML/CFT;
(c) The necessity of the information to be updated.

It should be noted that not all information adds value to the business and risk profile or serves to mitigate any ML/FT risks, in which case subject persons should consider whether the information is actually necessary. *By way of example, requesting updated documentation evidencing the subject person's change in occupation may not be necessary where the customer has retained the same risk rating and transaction patterns.*

Processing of personal data

While subject persons are obliged at law to keep information, data and documentation up-to-date, they are to keep in mind a number of principles particularly those relating to the processing of personal data. Requests for information should not be excessive or disproportionate, especially when other, less intrusive methods may suffice to fulfil the purpose of the obligation. Subject

persons should consider discarding documents which are no longer relevant for AML/CFT purposes and which are not needed under record keeping obligations.

4.6 Timing of Due Diligence Procedures

This part of the Implementing Procedures deals with the various scenarios when the subject person would usually be required by the PMLFTR to carry out the CDD measures provided for in Regulation 7(1)(a) to (c). These are provided for under Regulations 7(5) to (7) of the PMLFTR, which require the application of CDD measures to:

(a) New customers when establishing a business relationship;
(b) Customers when carrying out an occasional transaction;
(c) Existing customers at appropriate times and on a risk-sensitive basis, including at times when the subject person becomes aware that the relevant circumstances surrounding a business relationship have changed;
(d) Existing business relationships whenever doubts arise about the veracity or adequacy of the previously obtained customer identification information, data or documentation; and
(e) Situations where the subject person has knowledge or suspicion of proceeds of criminal activity, money laundering or the funding of terrorism, regardless of any derogation, exemption or threshold.

Regulation 8 of the PMLFTR then specifies the moment in time when these measures are to be applied within the above situations. While a subject person would usually be expected to apply the CDD measures in the above situations at the moment in time indicated in the PMLFTR, the risk-based approach allows subject persons to vary the applicability and/or timing of the measures depending on the risk of ML/FT identified.

Thus, even where the exceptions provided for under this Section providing for a delay in the carrying out of CDD do not find application, subject persons are still allowed to vary the timing of the said measures on the basis of risk. In this regard, subject persons should therefore have regard to what is provided in Section 4.8 on Simplified Due Diligence.

4.6.1 Timing of CDD when establishing a business relationship

Regulation 8(1) of the PMLFTR requires subject persons to verify the identity of the customer and, where applicable, the identity of the beneficial owner when the establishment of a business relationship. Therefore, when a customer seeks to establish a business relationship, subject persons are required to apply CDD measures when the prospective customer takes active steps to benefit from a service or a product provided by the subject person and at all times prior to any product or service being provided to the customer.

In practice, requiring the customer to provide documentation for the purposes of verification in the context of a preliminary meeting or where initial enquiries are still being made, may not

always be realistic and reasonable. For example, where a subject person receives general enquiries on the tax regime applicable in Malta or a request for a quote, it would be premature for the subject person to carry out the identification and verification of identity of the possible customer.

However, where the same person takes active steps that show that there is an intention to establish a business relationship, absent circumstances that justify a delay in the carrying out of CDD measures, the subject person is required to complete the same. A delay may for example be justified, in so far as verification of identity is concerned, when the subject person assess the business relationship to be a low risk one.

This does not mean that subject persons cannot take steps that may eventually facilitate the carrying out of the CDD measures. Giving a prospective customer prior notice of what would be required in the event that it takes a decision to establish a business relationship with the subject person may eventually facilitate the carrying out of the same. Thus, during preliminary meetings, it may be advisable to inform prospective customers that the subject person's Customer Acceptance Policy requires the prospective customer to provide the necessary CDD documentation immediately, prior to the establishment of that business relationship.

Exceptions when CDD may be carried out after the establishment of a business relationship

(i) Specific exceptions in relation to certain circumstances

Notwithstanding the obligation to complete verification procedures **prior to** the establishment of a business relationship, the PMLFTR provide that verification procedures may be completed **after** the establishment of a business relationship where it is necessary so as not to interrupt the normal conduct of business. However, this exception is subject to the following two conditions being met:

(a) The risk of ML/FT is low; and
(b) The verification procedures have to be completed as soon as is reasonably practicable after the establishment of the business relationship.[58]

Subject persons are to note that the low risk of ML/FT does not here refer to the overall risk of the business relationship which would result following the carrying out of the *customer risk assessment,* but rather the risk within the initial phase of the business relationship. By way of example, the use of some products within the initial phase of a business relationship may be so limited in values that the business relationship at that very point in time will present a low risk of ML/FT independently of any other factors.

In the event that CDD measures are applied after the establishment of a business relationship, subject persons should record the reasons for deferring their application.

(ii) Specific exceptions applicable in relation to long-term insurance business

[58] Regulation 8(2) of the PMLFTR.

In terms of Regulation 7(9) of the PMLFTR, subject persons providing long-term insurance business have, in addition to identifying and verifying the identity of the customer, and where applicable, the beneficial owner, to carry out the following CDD measures on the beneficiaries of long-term insurance policies:

(a) where the beneficiaries are specifically named natural persons, legal entities or arrangements, subject persons have to identity such beneficiaries;
(b) where the beneficiaries are designated by characteristics, class or other means, subject persons have to obtain sufficient information concerning those beneficiaries to be able to identify them at the time of payout;
(a) where the beneficiaries assign any of their rights vested under the policy, subject persons have at the time of becoming aware of the assignment, identify the natural persons, legal entities or arrangements receiving for their own benefit the value of the policy assigned; and
(b) verify the identity of the beneficiaries at the time of pay-out.

Thus, while beneficiaries have to be identified when the business relationship is being established, the PMLFTR provide for the possibility that verification takes place after the establishment of the same. And this notwithstanding what has been stated so far. However, verification of identity must always take place at or before the time of payout (i.e. prior to the funds being transferred to the beneficiary).

In cases where the beneficiary under a long-term insurance policy assigns all or part of his rights under the said policy to a third party, the subject person has to:

(a) identify the assignee (as the new beneficiary) as soon as the subject person becomes aware of the assignment; and
(b) verify the identity of the assignee at the time of payout at the latest, but always prior to any funds being transferred to the assignee.

(iii) Specific exceptions in relation to the opening of accounts

Notwithstanding the general principle and the exception under paragraph (i) above, subject persons carrying out relevant financial business may open an account (including accounts that permit transactions in transferable securities) prior to the completion of the verification process.[59] This exception is subject to the condition that adequate safeguards are put in place such that no transactions, apart from the initial transfer of funds necessary to open the account, are to be carried out through the account until the verification procedures have been satisfactorily completed.

By way of example, a subject person carrying on the business of banking under the provisions of the Banking Act[60] may open a bank account for the customer prior to the completion of the verification process, provided that safeguards are put in place so as to ensure that no transactions

[59] Regulation 8(3) of the PMLFTR.
[60] Cap 371 of the Laws of Malta.

are carried out through that account until the verification procedures are satisfactorily completed.

(iv) Specific exceptions in relation to certain legal entities and legal arrangements which administer and distribute funds

There may be other situations, particularly in the area of trusts, foundations and similar legal arrangements, where it may not be possible to identify and verify the identity of the beneficiary at the time of the establishment of the business relationship since the beneficiaries are simply designated by particular characteristics or class and not (specifically) named as beneficiaries[61].

In such cases, at the establishment of the business relationship (such as the setting up of the trust) the subject person is only required to gather sufficient information concerning the class or characteristics of beneficiaries (which information one would expect be contained in the trust instrument) in order to be able to establish if the beneficiaries, once they are determined, are actually entitled to receive the distribution. Having established as much, subject persons are to carry out identification and verification of identity of the beneficiaries. The verification of their identity may be delayed up until the time of payout (i.e. prior to the funds being transferred to the beneficiary) or at the time the beneficiaries seek to exercise their vested rights.

Furthermore, if the beneficiary assigns any of its rights, the assignee has to be identified as soon as the subject person becomes aware of such assignment. Here again, the verification of the identity of the assignee may, however, be delayed up until the payout.

Apart from the above, there may be other situations where a subject person encounters one or more impediments to the carrying out of CDD measures vis-à-vis the beneficiaries. This may include instances where the beneficiaries may not even be aware that they have been designated as beneficiaries. In such cases, identification can still be carried out on the basis of the personal details contained in the trust instrument and/or obtained from the settlor/trustee. However, verification of identity can then be delayed up until payout as explained hereabove.

The same reasoning can be applied to beneficiaries who have not yet received any distribution under the trust or where the distribution is subject to one or more conditions being met or to the trustee's discretion, and the risk of ML/FT is considered to be low. Even in these cases, it is possible for verification of identity to be delayed until pay-out as explained hereabove.

4.6.2 Timing of CDD when an occasional transaction is carried out

Regulation 8(1) of the PMLFTR requires subject persons to verify the identity of the customer, and where applicable, the identity of the beneficial owner, before the carrying out of an occasional transaction. Therefore, when a customer seeks to carry out an occasional transaction, subject persons are required to apply CDD measures when the prospective customer takes active steps

[61] Regulation 8(4) of the PMLFTR.

to benefit from a service or a product provided by the subject person and at all times prior to any product or service being provided to the customer.

On the other hand, where a customer merely seeks to obtain information from the subject person, such as, for instance, the general conditions under which a subject person would be ready to provide its services or products, the subject person would not be required to carry out any CDD measures. Such obligation would only arise once the customer actually takes active steps to engage the subject person to provide its services or products to carry out the occasional transaction.

Occasional transactions may vary in nature and therefore, depending on the case at hand, subject persons are to apply suitable CDD measures. For instance, in the case of a transfer of funds through the services of a money remitter where the service is to be provided immediately, CDD measures have to be applied, and documentation collected, prior to the carrying out of the occasional transaction.

4.6.3 Timing of CDD in case of suspicion of ML/FT

Regulation 7(5)(c) of the PMLFTR provides that subject persons are required to carry out CDD measures when they know or suspect that a customer, may have been, is, or may be engaged in ML/FT, or that a transaction involves the proceeds of criminal activity. In such instances, any exemption, exception or other change in timing or extent of CDD measures to be carried out on the customer is **not applicable** and the subject person has to carry out CDD to the extent that is reasonably practicable.

4.6.4 When the subject person doubts the veracity or adequacy of CDD documentation

Subject persons must repeat CDD measures immediately when doubts arise regarding the veracity or adequacy of previously obtained customer identification information, data or documentation. In addition, the subject person must also consider whether the customer risk assessment needs to be revised in line with the subject person's policies and procedures on Customer Risk Assessments and if the situation merits the filing of a STR with the FIAU.

4.6.5 Timing of CDD in relation to existing customers

The PMLFTR require subject persons to apply CDD measures to existing customers at appropriate times on a risk-sensitive basis, including when the subject person becomes aware that changes have occurred in the relevant circumstances surrounding the business relationship. In terms of Regulation 7(6) of the PMLFTR, subject persons have to re-assess and review the CDD carried out with respect to existing customers/business relationships under two scenarios.

Scenario One - Re-assessing and reviewing CDD measures on a risk sensitive basis

Under this first scenario the subject person is required to assess and review the CDD measures applied to all customers with which it already had an established business relationship upon the coming into force of a revised version of the PMLFTR, any Implementing Procedures or any amendments thereto. In this manner it can determine whether the risk management procedures and CDD applied on all existing customers are in line with the requirements of the revised or amended version of the PMLFTR and/or any Implementing Procedures or any amendments thereto. In the event that any shortfalls are found, the subject person would have to take action to remedy the situation and bring the situation in line with the new applicable requirements.

Thus, where:

(a) the customer would be categorised as presenting the same level of ML/FT risk within the subject person's risk management procedures under both the old and the revised versions of the PMLFTR and of the Implementing Procedures;
(b) the subject person has sufficient CDD documentation and information on file to meet the requirements under the revised PMLFTR and Implementing Procedures (i.e. the CDD carried out is commensurate to the risk identified); and
(c) the CDD documentation and information on file as well as the nature and level of ongoing monitoring carried out is sufficient to mitigate the ML/FT risks which the customer presents,

the subject person would not need to undertake any additional measures.

On the other hand, where any one or more of the conditions set out above are not met, the subject person is required to review its business relationship with the customer on a risk sensitive basis to determine what action is to be undertaken to ensure that the risk-based approach and CDD measures are being applied in an appropriate manner. In such circumstances, the subject person should consider giving priority to business relationships which are rated as presenting a higher risk of ML/FT following the application risk assessment procedures outlined in Chapter 3. Subject persons should also consider taking any additional actions upon certain trigger events (e.g.: where the customer approaches the subject person for a new service or product, or prior to the carrying out of another transaction), even if this is not in keeping with the subject person's review plan.

This risk-based revision should therefore lead the subject persons to determine what AML/CFT measures need to be repeated on such customers to ensure that they are adhering to their obligations under the revised version of the PMLFTR, any Implementing Procedures or any amendments thereto. It is important that any such review be undertaken within a reasonable period of time.

Scenario two - Changes in the circumstances relative to the business relationship

Subject persons are also required to review the business relationship when there are changes in its circumstances which would give rise to a change in the ML/FT risk posed by the customer and therefore lead to a different categorisation of the customer. In such circumstances subject persons have to consider whether the CDD measures applied have to be updated to mitigate effectively the new level of risk they are exposed to and carry out the necessary changes.

By way of example, these changes may arise in the context of ongoing monitoring, where the subject person notes changes in the transaction patterns of the customer, changes in the payment method used or changes in the jurisdiction links of the customer. In such cases, the subject person is first required to understand whether such changes result in a change in the risk profile of the customer. If there is a change in the risk level posed by the customer, then the CDD measures applied on such customer also need to be revised, especially if the risk of ML/FT has increased. Moreover, reference should also be made to Section 3.5 of these Implementing Procedures, as the customer risk assessment would also need to reflect any such changes and be updated accordingly.

It is also possible that a change in the circumstances of a given customer will not result in a change in the risk level to which the subject person is exposed but leads to a change in the risk factor/s that had led to the business relationship being considered as presenting a given level of risk. In these circumstances it would be important for the subject person to consider whether the CDD measures applied originally are sufficiently adequate to address the new risk factors or whether new CDD measures have to be applied so as to counter and hence mitigate the new specific risk factor/s identified.

4.6.6 Acquisition of the business of one subject person by another

Where a subject person acquires the business of another subject person or of a third party[62], in whole or in part, it is not necessary to undertake CDD measures anew on all existing customers, provided that the records of all customers are acquired with the business and that the subject person is satisfied that the procedures adopted by the previous subject person or third party, including its customer assessment risk procedures, were in line with the provisions of the PMLFTR and the Implementing Procedures. This should not be limited to an evaluation of the policies and procedures adopted and applied by the subject person or third party whose business is being acquired but should also include taking a sample of customers to ensure that the said policies and procedures were actually being implemented in practice.

In the event that the records of the customers are not all obtained or the procedures adopted by the previous subject person or third party were not in line with the provisions of the PMLFTR and the Implementing Procedures, CDD measures must be undertaken on a risk sensitive-basis, as soon as reasonably practicable. In such cases, the subject person should assess the extent of such deficiencies and consider whether:

(a) they should repeat CDD measures on all customers;
(b) only particular CDD measures need to be repeated; and
(c) which customers are affected.

Subject persons are to note that the exclusion from carrying out CDD measures does not extend to ongoing monitoring, which obligation has to be met as from the day on which the subject person acquires another subject person's or third party's customers.

[62] For the definition of a "third party" refer to Regulation 12(2) of the PMLFTR.

Subject persons transferring their business, whether in whole or in part, still have record-keeping obligations in relation to the customers they are transferring. However, in this case subject persons may fulfil their record-keeping obligations by adopting one of the following options:

(a) the subject person transferring the business can opt to pass on the documentation collected for CDD purposes, while retaining a copy of such documents; or
(b) the subject person transferring the business can opt to pass on the documentation collected for CDD purposes without retaining any copies thereof. Such subject persons should however ensure that they retain the CDD information required in accordance with the provisions under Regulation 7(1)(a) to (c), as updated in terms of Regulation 7(2)(b). If this option is adopted, the transferor passing on the documents would need to enter into a written agreement with the subject person to whom the business is being transferred in order to ensure that all CDD documentation being passed on would be made available immediately upon request.
(c) It is also to be noted that all other records concerning the business relationship and all records of transactions carried out by the customer in question would need to be retained by the subject person transferring the business.

4.7 Failure to complete CDD measures laid out in Regulation 7(1)(a) to (c)

Where a subject person is unable to comply with paragraphs (a) to (c) of Regulation 7(1) of the PMLFTR, the subject person shall:

(a) not carry out any transaction through the account;
(b) not establish the business relationship or carry out an occasional transaction; and
(c) terminate the business relationship with the customer.

In addition, subject persons are to consider whether a STR should be filed with the FIAU. It is important to highlight that the reluctance of the customer to provide CDD documentation on its own should not be automatically equated to a suspicion of ML/FT. The subject person should consider all factors and information it has at its disposal. If after this assessment, the subject person determines that there are grounds giving rise to a suspicion of ML/FT, then it has to submit a STR to the FIAU.

Prior to applying the measures under paragraphs (a), (b) and (c) above, the subject person should consider whether such actions may frustrate efforts at analysing or investigating suspected instances of ML/FT. In that event, or where taking the measures under paragraphs (a) to (c) above is impossible, the subject person should carry on with the business and immediately inform the FIAU of the circumstances.

Subject persons might be in a situation where they are unable to fulfil their obligations under Regulation 7(1)(a) to (c)when they are already in possession of customer's funds. In this instance, the action to be taken by the subject person will hinge upon whether the subject person has a suspicion of ML/FT or otherwise. Thus, if after considering all factors and information at its disposal, the subject person determines that:

(a) There are grounds giving rise to a suspicion of ML/FT, then it has to submit a STR to the FIAU and act in accordance with the provisions relative to the suspension of execution of transactions envisaged under Article 28 of the PMLA.
(b) There are no grounds to suspect ML/FT, the subject person has to determine whether there are any other reasons to hold onto the funds which are still on the customer's account and, if there are none, remit the funds back to the customer.

Whenever a subject person is remitting funds, it has to:

(a) Remit the funds to source using the same channels used to receive the funds; and
(b) To the extent that this may be possible, indicate in the script/instructions accompanying the funds that these are being remitted due to its inability to complete CDD.

In the event that the subject person is unable to remit the funds to source using the same channels, it will inevitably have to request fresh instructions from the customer. If these instructions give rise to a suspicion, it should submit a STR and suspend the remittance in line with Article 28 of the PMLA.

It should be clear that the remittance of any funds would not be possible where an order or directives or notice has been issued in terms of the PMLA, the Criminal Code or the PMLFTR which prohibits the subject person from releasing funds.

Finally, it is to be noted that the PMLFTR provide that subject persons carrying out a relevant activity under paragraph (a) and (c) of the definition of 'relevant activity', which refer to:

(a) members of the accountancy profession;
(b) auditors;
(c) tax consultants; and
(d) notaries and other independent legal professions;

shall not be bound to apply the measures indicated above provided that such subject persons are acting in the course of ascertaining the legal position of their client or performing their responsibilities of defending or representing their customer in, or concerning, judicial proceedings, including advice on instituting or avoiding proceedings.

4.8 Simplified Due Diligence

Regulation 10 of the PMLFTR provides for the application of SDD. The application of SDD is **not an exemption** from carrying out CDD but rather a variation of the extent and timing of CDD to be applied in view of the lower risk of ML/FT that the circumstances present. When applying CDD measures subject persons are therefore allowed, in a way that is commensurate to the low risk they have identified, to adjust:

(i) The timing of CDD. An example would be where the product, service or transaction sought has features that limit its use for ML/FT purposes, in which case subject persons can decide

to postpone the verification of identity or other CDD measures until a pre-determined threshold or other triggering event is reached;

The quantity of information and/or documentation obtained for verification of identity and other CDD measures. An example would be where the product, service or transaction sought can have only one particular use and therefore the subject person can assume the nature and purpose of the business relationship;

(ii) The quality of information/documentation obtained for verification and other CDD measures. An example would be where the product, service or transaction sought has features that limit its use for ML/FT purposes, subject persons can adjust the source of information obtained for CDD purposes, such as by accepting information obtained from the customer rather than an independent source to establish the customer business and risk profile. This would not be acceptable to verify of the customer's own identity;

(iii) The frequency and intensity of ongoing monitoring. An example would be where:

(a) the frequency and/or intensity of transaction monitoring is varied by for example monitoring only transactions that meet or exceed a given threshold. Where firms choose to do this, they must 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. Having said that, subject persons should ensure that the level of ongoing monitoring is always sufficient to a degree that the subject person can determine whether the circumstances on the basis of which it was decided to apply SDD are still current.

(b) the frequency of CDD updates and reviews of the business relationship is adjusted, for example, to take place 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. Subject persons must make sure that this does not result in a *de facto* exemption from keeping CDD information and documentation up-to-date.

Where a subject person determines that SDD measures may be applied and one of the characteristics on which such a determination is made is the restrictions, limitations or characteristics of the service or product being offered, the subject person must also have mechanisms in place in order to avoid the possible circumvention or nullification of the said restrictions, limitations or characteristics.

By way of example, if a product like an account or policy is considered to be low risk as it is capped up to a low value amount, the subject person should have mechanisms in place which prevent a customer from depositing amounts in excess of the applicable capping or from opening multiple accounts to circumvent the mentioned capping.

In applying any of the above-mentioned variations in timing and extent of CDD measures, subject persons have to ensure that:

(a) the variation in the extent and timing of CDD does not result in a *de facto* exemption from CDD measures;
(b) any threshold or event set for triggering CDD measures is set at a reasonably low level (although with regard to terrorist financing, subject persons should note that a low threshold alone may not be enough to reduce risk and thus particular care should be exercised when providing services or products that are particularly susceptible of being misused for terrorist financing purposes);
(c) they have systems in place to (i) detect when the threshold has been reached or/and event has materialised and (ii) prevent by-passing any restrictions, limitations or characteristics applicable to the product or service; and
(d) they do not vary, defer or delay any CDD measures they cannot vary, defer or delay under any EU Regulations, the PMLFTR, these Implementing Procedures or any other binding instrument, order or directive.

Moreover, subject persons are, as a minimum, **always required** to identify the customer as per Section 4.3.1 and/or 4.3.2 and carry out a sufficient degree of ongoing monitoring to ensure that the circumstances on the basis of which it was decided to apply SDD are still applicable. Therefore, when applying SDD, the subject person is still required to undertake ongoing monitoring of the business relationship with the customer in order to ensure that the ML/FT risk posed by the customer remains low and in order to be able to identify any suspicion of ML/FT.

The information which the subject person obtains when determining to apply SDD measures must enable the subject person to be reasonably satisfied that the risk associated with that particular business relationship is low. It must also be sufficient to give the subject person enough information about the nature of the business relationship to identify any unusual or suspicious transactions. Importantly, subject persons are to note that SDD does not exempt an institution from reporting suspicious transactions to the FIAU.

Moreover, the rest of the CDD measures and an increased level of ongoing monitoring are to be carried out or applied whenever the business relationship is no longer deemed to represent a low risk of ML/FT or the subject person has a suspicion of ML/FT. Whenever this occurs, subject persons are to ensure that the risk rating of that business relationship is changed accordingly and SDD is no longer applied.

4.8.1 Particular Situations in which SDD may be applied

The PMLFTR no longer set out specific circumstances which allow the application of SDD. Instead Regulation 10(1) allows subject persons to apply SDD measures in circumstances which fall within either of the following two categories:

(i) In relation to activities or services that are determined by the FIAU to represent a low risk of ML/FT, having taken into consideration the findings of any national risk assessment and any other relevant factors as may be deemed appropriate; and

(ii) where, on the basis of a risk assessment carried out in accordance with Regulation 5(1) of the PMLFTR, the subject person determines that an occasional transaction or a business relationship represents a low risk of ML/FT.

Thus, subject persons enjoy discretion on when SDD can be applied as long as any decision to apply one or more SDD measures is justified on the basis of their business and customer risk assessments. The low risk factors mentioned in Chapter 3 can provide some indicators as to when SDD may be permissible. Moreover, the Risk Factor Guidance issued by the ESAs and referred to in Chapter 3 above, provides a series of scenarios which can be considered as low risk and the accompanying measures that can be applied.

The following are some examples of situations which in normal circumstances are deemed to present a low risk of ML/FT:

Customers carrying out Relevant Financial Business or Listed Companies

In determining whether a business relationship presents a low risk of ML/TF, and therefore the extent to which it is appropriate to apply SDD measures, a subject person can take into account, *inter alia*, whether the customer is a:

(i) subject person carrying out relevant financial business or a third party established in an EEA State or in another low-risk jurisdiction carrying out an equivalent activity and subject to equivalent AML/CFT requirements and supervision as those required by Directive (EU) 2015/849; or
(ii) entity that meets the conditions set out in Section 4.3.2.2 above.

In such cases, where the customer risk assessment results in the business relationship or occasional transaction as being low risk, the application of SDD may involve refraining from carrying out any measures in relation to the beneficial owners and the customer's ownership and control structure. CDD may therefore be limited to the identification and verification of the customer, and a sufficient level of ongoing monitoring of the relationship.

In determining whether SDD should be applied when servicing corporate customers indicated in this section, the subject person should carry out background checks on the entity to determine that it meets the criteria set out above. This would involve:

(a) checking for any publicly available regulatory or supervisory adverse information; and
(b) obtaining evidence that the customer institution is licensed or authorised to conduct financial and/or banking business. This could take place by:

- consulting public registries, websites maintained by supervisory and regulatory authorities;
- requesting information directly from the customer;
- checking with another office, subsidiary, branch or correspondent bank operating in the same country of the customer.

Subject persons should record the steps they have taken to check that their customer meets the conditions to be considered as generally low risk.

Client Accounts

Persons who hold client money or other assets in pooled accounts (whether in a bank account or through a securities holding) may themselves be subject to AML/CFT measures. Where this is the case, they are expected to have already carried out CDD measures in respect of the assets' beneficial owners. Thus, subject persons carrying out a relevant financial business, with whom such client accounts are held can consider applying SDD measures, provided that all of the following conditions are met:

(a) the business relationship with the holder of the pooled account presents a low risk of ML/FT taking into account the account holder's business, the types of customers the holder's business serves and the jurisdictions the holder's business is exposed to, among other considerations;
(b) the holder of the account is a subject person or is otherwise a third party established in the EEA or in a reputable jurisdiction which is subject to equivalent AML/CFT requirements and supervision as those required by Directive (EU) 2015/849;
(c) it is determined that the holder of the pooled account applies robust and risk-sensitive CDD measures to its own customers and, where applicable, to their beneficial owners;
(d) the information on the identity of the persons on whose behalf monies are held in the pooled account is made immediately available to the subject person upon request; and
(e) there is no adverse information on the customer.

Subject persons may reasonably apply a similar approach to client accounts which only contain the funds of a single beneficial owner.

In such cases, the subject person may decide not to ask for any information and documentation on the identity of the assets' beneficial owner/s and limit itself to applying CDD measures to the account holder and carrying out a sufficient level of ongoing monitoring.

Public Sector Bodies

In respect of customers who are local or overseas governments (or their representatives), supranational organisations, government departments, state-owned companies or local authorities, the approach to identification and verification may be tailored to the circumstances of the customer, reflecting the subject person's determination of the level of ML/FT risk presented. Where the subject person determines that the business relationship presents a low risk of ML/FT, SDD measures may be applied. Public sector bodies include state supported schools, colleges and universities.

For the avoidance of doubt, subject persons must make a distinction between state-owned entities and bodies engaged in public administration. Bodies engaged in public administration may involve different revenue/payment streams from that of most businesses and are typically funded from government sources, or from some other form of public revenues. State-owned businesses, on the other hand, may engage in a wide range of activities, some of which might

involve higher risk factors, leading to a different level of CDD being appropriate. Such entities may be partly publicly funded or may derive some or all of their revenues from trading activities.

Furthermore, in determining the level of ML/FT risk presented, subject persons are required to assess the jurisdictional risk and more specifically the government's standing of the said public bodies.

By way of example, a government department of a jurisdiction listed by FATF as a high-risk and non-cooperative jurisdiction should not be rendered as representing a low degree of ML/FT risk and hence should not be subject to SDD. The same may apply to other jurisdictions which may not necessarily be listed by FATF, but for instance are characterised by corruption, political instability or civil unrest.

4.8.2 Circumstances where SDD cannot be applied

The PMLFTR prohibit the application of SDD where the subject person knows or suspects that a customer may have been, is, or may be engaged in ML/FT, and where he knows or suspects that funds originate from criminal activity. In such circumstances, even though the customer or the product qualifies for SDD, the SDD procedure would not be able to be applied and the subject person is required to carry out EDD measures and, file an STR with the FIAU.

Furthermore, even if a business relationship or occasional transaction may present all the elements of a low risk situation, whenever the law expressly requires the application of EDD measures in accordance with Section 4.9, SDD measures cannot be applied. By way of example, if the product is a low risk product but the customer is a PEP, or has links with a non-reputable jurisdiction, even though the product poses a low risk of ML/FT, the subject person is still required by law to apply appropriate and risk-based EDD measures given that the customer is a PEP or coming from a non-reputable jurisdiction.

Subject persons are reminded that whenever the activities or services are no longer determined by the FIAU to represent a low risk of ML/FT in terms of Regulation 10(1)(a) or the risk assessment no longer indicates a low risk of ML/FT in terms of Regulation 10(1)(b), they are to refrain from applying SDD and vary the level of CDD accordingly. For this to be done, subject persons are to always carry out sufficient ongoing monitoring to be able to detect unusual and suspicious transactions, as well as to be able to detect any changes which may require the subject person to revisit the customer's risk assessment and as a result, the level of CDD being applied.

It is to be noted that the Risk Factor Guidelines issued by the ESAs and referred to in Section 3 contain a series of scenarios in which SDD can or cannot be applied, together with possible measures to be undertaken. Subject persons carrying out relevant financial business are to consider this document whenever considering whether a situation presents a low risk of ML/FT and the measures to be undertaken. Situations corresponding to those considered in these Guidelines and in terms of which SDD is not considered possible should not be treated as low risk by subject persons unless significant divergent circumstances subsist that justify a reconsideration of the resulting ML/FT risk.

4.9 Enhanced Due Diligence

Subject persons must apply **EDD** measures on a risk-sensitive basis in those situations which, by their nature, represent a higher risk of ML/FT. In essence, EDD measures are **additional measures** to the CDD measures set out in Regulation 7, which are to be applied in order to ensure that the higher risks presented by certain customers, products, services or transactions are better monitored and managed to avoid any involvement in ML/FT.

Whereas the PMLFTR provide for SDD measures to be applied on an optional basis, it is mandatory for EDD measures to be applied in any situation that presents a higher risk of ML/FT and in any other situation where the application of such measures is mandated by law. Regulation 11 of the PMLFTR provides an exhaustive list of what these situations are and, with respect to those situations where the application of EDD is required in terms of law independently of the actual risk presented, it also lists the actual measures to be undertaken. In situations which are otherwise deemed to be high risk, the EDD measures are largely left to the discretion of the subject person, the only requirement being that they are appropriate to manage and mitigate the high risk of ML/FT[63].

In either context, the identification and verification of the identity of the customer and, where applicable, of the beneficial owner, as well as in the case of a business relationship obtaining information on its purpose and intended nature (refer to Sections 4.3 and 4.4), are important to ensure that the subject person:

(i) is well informed and understands the risks which would enable the subject person to take appropriate mitigating measures; and
(ii) is able to carry out proper ongoing monitoring, thus detecting misuse of the product or service being provided by the subject person.

Subject persons are expected to gather additional information and/or documentation (as appropriate) which is more thorough and detailed with respect to those business relationships or transactions which pose a higher risk of ML/FT. In practice, under a risk-based approach, it will not be appropriate for every product or service provider to know their customers equally well, but the subject person's information demands need to be proportionate and appropriate to the respective ML/FT risk.

When someone becomes a new customer, or applies for a new product or service, or where there are indications that the risk associated with an existing business relationship might have increased, the subject person should, depending on the nature of the product, service or transaction for which they are applying, request information as to the customer's residential status, employment and salary details, and other sources of income or wealth (e.g. inheritance, divorce settlement, property sale), in order to decide whether to accept the application or continue with the relationship. The subject person should consider whether, in some circumstances, evidence of source of wealth or income should be required (for example, if the source of wealth is given to be an inheritance, the subject person is to obtain a copy of the will).

[63] Regulation 11(2) of the PMLFTR.

Subject persons should also determine the level of ongoing monitoring that should be carried out on a particular customer depending on the risks posed by the customer and/or the activities of the customer. The extent of additional information sought, and of any monitoring carried out in respect of any particular business relationship, or class/category of business relationship, will depend on the ML/FT risk that the customer, or class/category of business relationship, is assessed to present to the subject person.

A subject person should have a clear policy regarding the escalation of decisions to senior management concerning the acceptance or continuation of high-risk business relationships.

4.9.1 Situations presenting a High Risk of ML/FT

Regulation 11 requires the application of EDD in relation to the following situations:

11(1)(a): In relation to activities or services that are determined by the FIAU to represent a high risk of ML/FT, having taken into consideration the findings of any national risk assessment and any other relevant factors as may be deemed appropriate.

In the event that the FIAU determines that a particular scenario represents a high risk of ML/FT, and therefore warrants the application of EDD measures, the subject person is to apply EDD measures irrespective of whether the subject person has classified the customer or business relationship as not representing a high risk in line with the standard customer and business risk assessments carried out by the subject person in accordance with Chapter 3. By way of example, when the Government of Malta launched an investment registration scheme, the FIAU issued corresponding AML/CFT guidance which laid down a number of EDD measures that were to be applied by specific subject persons.

11(1)(b): Where, on the basis of the risk assessment carried out in accordance with Regulation 5(1) of the PMLFTR, the subject person determines that an occasional transaction, a business relationship or any transaction represents a high risk of ML/FT;

Subject persons should here refer to Chapter 3 of these Implementing Procedures which provides guidance on how subject persons are to assess the risks posed by their particular business, services or activities and the risks posed by specific customers. In the event that the results of the customer risk assessment indicates that a business relationship or an occasional transaction represent a high risk of ML/FT, EDD measures should be applied.

In this regard, subject persons carrying out relevant financial business are to have regard to the Risk Factor Guidance issued by the ESAs and referred to in the context of Chapter 3. When faced with situations analogous to the ones described in the said Guidance as requiring the application of EDD measures, subject persons have to consider adopting the said measures or ones which are equally effective to mitigate the risk of ML/FT.

The said Guidance should also be taken into consideration by subject persons carrying out relevant activity as it is possible that they will encounter situations which present risks of the same

nature. Thus, the measures set out in the Guidance document to counter the said risks may be equally applicable by subject persons even if they do not carry out relevant financial business.

11(1)(c): When dealing with natural or legal persons established in a non-reputable jurisdiction as defined in Regulation 2 of the PMLFTR, other than branches or majority-owned subsidiaries which comply with group-wide policies and procedures as required under Regulation 6 of the PMLFTR in which cases EDD is to be applied when these present a high risk of ML/FT

Identifying situations which would require the application of EDD in terms of the above, requires having an understanding of a number of concepts, namely:

(a) "Dealing with Natural or Legal Persons" – subject persons are to interpret the term "dealing" in as wide a manner as possible. Thus, it is not only the entering into a business relationship or the carrying out of an occasional transaction that has to be considered as "dealing" but also for example the carrying out of transactions within the context of a business relationship which have links with non-reputable jurisdictions. When transactions are concerned, attention should be paid to the source of funds, the parties to the transaction, the accounts through which funds are to flow etc.

(b) "Established" – subject persons should here must have regard to connecting factors such as the citizenship or residency in the case of a natural person or the jurisdiction of registration, incorporation or licensing in the case of legal persons. The main place of business of the natural or legal person has to also be considered as a possible link. The same applies with regards to the person's source of wealth, i.e. if the activities which have generated or are generating the person's wealth are located in non-reputable jurisdictions. Having citizenship on its own need not be automatically equated with the natural person being established in the non-reputable jurisdiction if the individual has no other links with the jurisdiction concerned.

(c) "Non-Reputable Jurisdiction" - subject persons are here required to refer to Section [8.1] of these Implementing Procedures which deals with the concept of 'non-reputable third-countries' and how to assess whether a jurisdiction is reputable or otherwise.

Notwithstanding the above, subject persons are not required to carry out EDD measures in cases where the natural or legal person established in a non-reputable jurisdiction is a branch or a majority-owned subsidiary which complies with group-wide policies and procedures as set out in Section 8.2. This exemption would however not find application if, in line with the risk assessment carried out by the subject person, the scenario is still considered to represent a high risk of ML/FT.

In so far as non-reputable jurisdictions are concerned, the proviso of Regulation 11(2) of the PMLFTR also makes reference to non-reputable jurisdictions in respect of which an international call for counter-measures has been made. The proviso states that when undertaking occasional transactions for, or establishing a business relationship with, or acting in the course of a business relationship with, a natural or legal person established in a non-reputable jurisdiction in respect of which there has been an international call for counter-measures, prior to the establishment of

the business relationship or the undertaking of an occasional transaction, subject persons have to:

(a) apply EDD measures; and
(b) inform the FIAU of the proposed business relationship, occasional transaction or transaction to take place within an already existing business relationship prior to the same actually taking place.

In such cases the FIAU may, in collaboration with the relevant supervisory authority, require the subject person:

(a) not to establish the business relationship,
(b) not to continue such business relationship,
(c) not to undertake an occasional transaction; or
(d) to apply any other counter-measures as may be adequate under the circumstances.

The subject person should here refer to Section 8.1 which provides further guidance, particularly when it comes to those jurisdictions listed in FATF public statements and EU legal acts identifying countries which have strategic AML/CFT deficiencies and to which counter-measures apply.

4.9.2 Situations in which EDD is prescribed by law

4.9.2.1 Correspondent Relationships

EDD measures have to be applied whenever subject persons carrying out relevant financial business seek to establish a cross-border correspondent relationship, with respondent institutions situated in a country other than a Member State. For the purposes of the PMLFTR, a correspondent relationship can therefore also be considered to subsist between subject persons other than credit institutions as long as they carry out relevant financial business.

This results from the very definition of "correspondent relationship" provided in Regulation 2(1) of the PMLFTR which refers to:

> (a) the provision of banking services by one bank as the correspondent to another bank as the respondent, including providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services; and
>
> (b) the relationship between and among institutions carrying out relevant financial business and activities equivalent thereto, including where similar services to those under paragraph (a) are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers.

The **correspondent banking relationships** referred to in paragraph (a) above cover the provision of banking-related services by one credit institution ("the correspondent bank") to another credit institution ("the respondent bank"). The possible nature of these banking-related services is

indicated in the same paragraph. Through such a correspondent banking relationship, the respondent bank would be able to provide its own customers with cross-border products and services which it cannot provide on its own, typically due to the lack of an international network.

In a correspondent banking relationship, the correspondent bank (i.e. the subject person) would therefore be acting as agent for the respondent bank by processing and/or executing payments or other transactions for the end-benefit of the respondent bank's customers (and vice-versa) with whom it would usually have no direct relationship. Correspondent banking does not include one-off transactions or the mere exchange of SWIFT Relationship Management Application (RMA) keys[64] in the context of non-customer relationships, but rather is characterised by its (expected) ongoing, repetitive nature. The scope of a relationship and extent of products and services supplied will vary according to the needs of the respondent, and the correspondent's ability and willingness to supply them.

The other correspondent relationships referred to in paragraph (b) above relate to relationships established between subject persons carrying out relevant financial business for the purpose of providing services equivalent or similar to those provided within the context of a correspondent banking relationship. Thus, these relationships may still be established so as to facilitate the transfer of funds pertaining to the respondent institution's customers but they may also involve services provided in relation to assets other than funds such as securities.

Given the nature of a correspondent relationship, the correspondent institution (i.e. the subject person) is deemed to be establishing a business relationship with the respondent institution and not the respondent institution's customers. To this end CDD measures in terms of Regulation 7 have to be applied on the respondent institution and, in addition thereto, in cases where the respondent institution is established in a jurisdiction other than a Member State, Regulation 11(3) also requires that the following additional measures be applied:

(a) *gather sufficient information about the respondent institution to fully understand the nature of the respondent's business and to determine from publicly available information:*
   (i) the reputation of the institution; and
   (ii) the quality of supervision of that institution.

   The amount of information and/or documentation to be gathered by the subject person will vary depending on the risks posed by the respondent institution. In this regard, the information to be obtained in relation to the nature of the business of the respondent institution would include the type of respondent (i.e. kind of relevant financial activity or equivalent activities), the business model and the type of products, services and transactions which the respondent offers, and the reputability of countries where the respondent operates.

[64] The SWIFT RMA is a messaging capability enabling SWIFT members to exchange messages over the network and can create a non-customer relationship in particular cases of cash management, custody, trade finance, exchange of messages with payments and securities markets infrastructure entities, e.g., exchanges depositories.

When assessing the reputation and the quality of the supervision of the respondent institution, its parent undertaking or other companies within the same group, subject persons should have regard, amongst other matters, to the regulatory status (if any) of the respondent institution, the AML/CFT regime to which it is subject and to the supervisory record of the respondent (i.e. whether the respondent has been subject to any ML/FT investigations or regulatory enforcement measures). Subject persons are to also consider other factors that might affect the respondent's risk profile, such as whether the history of the business relationship with the respondent gives rise to concern, for example because the amount of transactions are not in line with what the correspondent would expect based on its knowledge of the nature and size of the respondent.

As regards the quality of supervision, regard should be had to any assessments, such as FATF and other FSRBs mutual evaluation reports, carried by national authorities or international bodies on the level and quality of supervision applicable in the jurisdiction where the respondent institution is established and to which laws it is subject. Thus, use may be made of information already collected to determine whether a jurisdiction is reputable or otherwise.

Subject persons may make use of publicly available information to understand the nature of the business of the respondent institution, its reputation and the quality of supervision on that institution.

(b) *it assesses the adequacy and effectiveness of the institution's measures, policies, controls and procedures for the prevention of ML/FT.*

There are various measures which can be carried out to fulfil this requirement. These measures, which may either be applied independently of each other or cumulatively, are the following:

(1) the correspondent institution obtains a copy of the AML/CFT procedures manual of the respondent institution and assesses the adequacy and effectiveness of the respondent institution's AML/CFT measures, policies, controls and procedures on the basis of the measures set out in the PMLFTR and these Implementing Procedures; or
(2) the correspondent institution develops a brief questionnaire with specific questions covering the legal obligations and the internal procedures applied by the respondent institution to meet these obligations; or
(3) the correspondent institution requests a declaration from the respondent institution on the adequacy of its internal controls, possibly certified by its supervisory authority.

(c) *it obtains prior approval of senior management for the establishment of new correspondent relationships;*

Obtaining the approval of senior management means having the approval of an officer or employee of the correspondent institution with sufficient knowledge of the subject person's ML/FT risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not be a member of the board of directors or equivalent body. The

approval of senior management should be clearly documented and made available if required by the FIAU.

What will constitute senior management will depend on the size, structure and the nature of the subject person and it is possible that this decision be also taken by an internal committee of the correspondent institution. By requiring senior management approval, subject persons will ensure that they are not entering into a business relationship without applying the necessary controls.

(d) *it documents the respective responsibilities of each institution for the prevention of ML/FT;*

The correspondent institution must ensure that the AML/CFT measures that each institution is to carry out and the responsibilities of each institution are clearly set out and documented. Thus, although it is not necessary that the two institutions reduce their respective responsibilities into a detailed formal document, there must be some form of documentation clearly setting out the responsibilities of the respective institutions.

(e) *it is satisfied that, with respect to payable-through accounts, the respondent institution has verified the identity of and performed ongoing due diligence on the customers having direct access to the accounts of the respondent institution and that it is able to provide relevant CDD data upon request.*

Payable-through accounts are correspondent accounts that are used directly by the respondent institution's customers to carry out transactions on their own behalf. Given the higher risk of ML/FT presented by this form of correspondent relationship, the correspondent institution is expected to determine who, apart from the respondent institution, is making use of said account.

This can be done by (i) obtaining written confirmation from the respondent institution that it will assume responsibility to carry out CDD on such persons, including identification and verification of identity of any of its customers who is granted access to the said account; and (ii) carry out random and spontaneous checks to ascertain that appropriate AML/CFT measures are being undertaken.

Correspondent relationships have to be also subject to a degree of ongoing monitoring. This may be carried out in a number of ways, including, but not limited to, the following:

(a) *Conducting ongoing monitoring of the respondent institution* – such as undertaking periodical reviews of the CDD information and documentation obtained on the respondent institution. The frequency of review will depend on the level of risk associated with the respondent institution. Where such reviews reveal a change in the risk posed by such respondent institution, the subject person should consider adjusting its risk assessment of the respondent institution and, if appropriate, obtain additional information and/or documentation to support the adjustment in the risk assessment.

(b) *Ongoing monitoring of transactions* – such monitoring is required in order to be able to detect any changes in the respondent institution's transaction patterns or activity. For more

information in relation to the type of transaction monitoring to be undertaken by the subject person, refer to Section 4.5.

(c) *Targeted transaction monitoring* – the monitoring of transactions depending on unique risk factors (e.g. location of the customers of the respondent institution, high number of STRs filed, where the payment flows are inconsistent with the stated purpose of the account etc.). The level and nature of transaction monitoring will vary, depending on the risks and the nature of the correspondent services being provided. For example, if the main purpose of the correspondent relationship is to process international wire transfers on behalf of the respondent institution's customers, the focus of account monitoring could be how well the respondent institution is implementing sanctions screening.

(d) *Enhancing the level of ongoing monitoring and request for information about transactions* – in the event that the subject person flags any unusual activity, the subject person should have internal processes to further review the activity and be able to request information and/or documentation from the respondent institution to be able to clarify the situation and possibly clear the alert.

In the context of correspondent relationships, a customer risk assessment is important from a number of perspectives:

(a) In relation to those correspondent relationships where the EDD measures to be applied are mandated by law, the customer risk assessment will allow the correspondent institution to calibrate the intensity and frequency of the EDD measures described above, including ongoing monitoring, as well as identify any additional risks that may require additional EDD measures to be applied so as to be mitigated in an effective manner.

(b) In relation to any other correspondent relationship that does not fall within the ambit of Regulation 11(3) of the PMLFTR, the customer risk assessment will lead the subject person to understand the actual risk presented by the said relationship and, where the ML/FT risk identified is high, allow the correspondent institution to determine the EDD measures that should be applied – the subject person must therefore still determine if the correspondent relationship is a business relationship to which Regulation 11((1)(b) finds application even though Regulation 11(3) may not be applicable thereto.

Where a revision of the customer risk assessment becomes necessary, the subject person should consider how the CDD measures may, within the limits allowed by law, be recalibrated to better address the revised risk level. In the case of correspondent relationships, the risk factors to be considered are to include, but not be limited to, the following:

(a) *the respondent's place of establishment* – the jurisdiction where the respondent institution and/or its parent undertaking is headquartered may increase or decrease the risk of ML/FT and therefore subject persons should evaluate the degree of risk presented by the jurisdiction in which the respondent and/or its parent undertaking is/are based;

(b) *the respondent's ownership and control structure* – the location of the shareholders, their corporate legal form and/or lack of transparency of the ultimate beneficial owners are

indicative of the risk the respondent institution presents. Subject persons should therefore consider whether the respondent institution is publicly or privately owned; if publicly held, whether its shares are listed or otherwise, on an exchange or regulated market in a reputable jurisdiction with a satisfactory regulatory regime and if privately owned, the identity of any beneficial owners and controllers. Subject persons should also consider the experience of the management team. Similarly, the location and experience of management may indicate additional concerns, as would unduly frequent management turnover. The involvement of PEPs in the management and/or control structure may also increase ML/FT risk;

(c) *the respondent's business and customer base* – the type of business activities undertaken by the respondent institution as well as the type of customer base the respondent institution has will have a bearing on the risk posed by the respondent institution. Involvement in certain business segments that are recognised internationally as particularly vulnerable to ML/FT or corruption, may present additional concerns. By way of example, a respondent bank which derives a substantial part of its income from customers located in high risk jurisdictions or from customers who deal in certain sectors which are more vulnerable to ML/FT, present a higher risk of ML/FT;

(d) *downstream correspondent clearing* – when the respondent bank is itself a downstream correspondent clearer, subject persons shall, on a risk sensitive basis, take reasonable steps to understand the type of risks posed by the customers of the respondent bank.

(e) In addition to the above, it is to be noted that subject persons carrying out relevant financial business are prohibited from entering into, or continuing, correspondent relationships with shell institutions. Moreover, the PMLFTR also require these subject persons to take appropriate measures to ensure that they do not enter into, or continue, a correspondent relationship with a respondent institution which is known to permit shell institutions to use its accounts. In this regard, it is pertinent to keep in mind that any interested subject person needs to make adequate checks to assess the extent to which any respondent institution it has entered into a correspondent relationship with permits shell institutions to use their accounts, and need to also maintain a record of such verifications.

4.9.2.2 Politically Exposed Persons

PEPs pose a high risk of ML/FT due to the position they occupy and the influence they exercise. PEPs may abuse of their prominent functions for private gain, such as by being involved in corrupt practices, accepting bribes or abusing or misappropriating public funds. These crimes generate proceeds which would need to be laundered. Certain PEPs in certain positions may also be exposed to the possibility of being involved in FT. The application of EDD measures is therefore necessary to mitigate the potential risks of ML/FT that arise when a subject persons deals with PEPs.

Similarly, family members or persons known to be close associates of PEPs may, as a result of this connection, also benefit from, or be used to facilitate, abuse by the PEP of his position and

influence. Therefore EDD measures are required also with regards to family members or persons known to be close associates of PEPs.

Regulation 11(5) of the PMLFTR requires that subject persons have appropriate AML/CFT risk management procedures which enables them to determine whether a customer or a beneficial owner (current or prospective) is a PEP, and subsequently to carry out EDD measures both when establishing or continuing business relationships with, or undertaking occasional transactions for a PEP. Specific EDD measures are moreover outlined under Regulation 11(6) to cover scenarios where PEPs are beneficiaries of long-term insurance policies. Regulation 11(8) of the PMLFTR stipulates that these same obligations apply to family members and persons known to be close associates of a PEP.

Whilst EDD measures are to be applied on PEPs, their family members and persons known to be close associates thereof, this is not to be interpreted as meaning that whenever any such individual is establishing a business relationship or carrying out an occasional transaction, such business relationship or occasional transaction is connected to ML/FT.

Subject persons are therefore required to carry out EDD measures which are commensurate and proportionate to the risks posed. However, subject persons are not required to turn away any prospective customers or close a business relationship on the basis that the prospective customer or the customer, or beneficial owner, is a PEP (or a family member or person known to be a close associate of a PEP).

It should be made clear however that if after collecting all the necessary information and documentation on the prospective customer, customer or its beneficial owner, and conducting a customer risk assessment, the subject person determines that the prospective business relationship or occasional transaction falls outside its risk appetite (because the risks posed are higher than they can effectively mitigate), the subject person has to decline or close the business relationship, or not carry out the occasional transaction.

(a) Who qualifies as a PEP?

Regulation 2(1) of the PMLFTR defines a PEP as a natural person who is or has been entrusted with a prominent public function, other than middle ranking or more junior officials. While middle ranking or more junior officials are not considered as holding prominent public functions and therefore are not considered as requiring the application of EDD measures in terms of Regulation 11(5), this does not exclude the possibility that EDD measures may still have to be applied where it is determined that a high risk of ML/FT subsists in accordance with Regulation 11(1)(b).

The PMLFTR does not provide a definition of what constitutes a '*prominent public function*' as this may vary depending on a number of factors such as the type, size, budget, powers and responsibilities associated with a particular public function and the organisational framework of the government or international organisation concerned, and other factors that are considered as part of the risk assessment.

The PMLFTR do, however, provide a non-exhaustive list of public functions which are considered as prominent public functions and would therefore render the holder thereof a PEP. This includes:

(a) Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers, and Parliamentary Secretaries;
(b) Members of Parliament or similar legislative bodies;
(c) Members of the governing bodies of political parties;
(d) Members of the superior, supreme, and constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
(e) Members of courts of auditors, or of the boards of central banks;
(f) Ambassadors, *charge d'affaires* and other high ranking officers in the armed forces;
(g) Members of the administrative, management or supervisory boards of state-owned enterprises;
(h) Anyone exercising a function equivalent to those set out in paragraphs (a) to (f) above within an institution of the European Union or any other international body.

This list is by no means an exhaustive one and subject persons are required to assess on a case by case basis whether a particular public function presents characteristics which would fall within the definition of a '*prominent public function*' in terms of the PMLFTR and these Implementing Procedures. The same public function may in one case or country lead to its holder being considered a PEP, while in another situation or country this may not be the case. By way of example, the positions and powers assumed by a mayor of a large city or head of a region in a foreign jurisdiction might not necessarily be equivalent to those assumed by a Maltese mayor and therefore a mayor may be treated differently depending on the jurisdiction concerned.

It is important to note that the PMLFTR do not distinguish between local and foreign PEPs and thus any person entrusted with a prominent public function whether in Malta, or in any other jurisdiction (including persons entrusted with a prominent public function in a supranational institution or within inter-governmental bodies such as the European Union and the United Nations), is considered to be a PEP and the subject person is required to carry out the EDD measures specified in Regulation 11(5) and (6) on such customer.

In the Maltese context the prominent public functions indicated in the PMLFTR which would render their holder a PEP should be understood as follows:

(i) *Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers and Parliamentary Secretaries* – means the President of the Republic of Malta, the Prime Minister and all ministers and parliamentary secretaries;

(ii) *Members of Parliament or similar legislative bodies* – means the Speaker and all Members of the House of Representatives of the Republic of Malta;

(iii) *Members of the governing bodies of political parties* – the term 'political parties' should be limited to those political parties which are represented in the House of Representatives. Persons falling within this category would include individuals entrusted with the management and administration of such a political party and does not include paid up members or regional or town representatives;

(iv) *Members of the superior, supreme, and constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances* – in the local context this means all Judges and. Magistrates of the Courts of Malta and Gozo;

(v) *Members of courts of auditors, or of the boards of the central banks* – means the Auditor General, the Deputy Auditor General, the Governor and Deputy Governor of the Central Bank of Malta;

(vi) *Ambassadors, charge d'affaires and high ranking officers in the armed forces* – all ambassadors and *charges d'affaires* of foreign jurisdictions in Malta as well as all Maltese ambassadors and *charges d'affaires* abroad. Honorary Consuls are not to be considered as PEPs. The Commander and Deputy Commander of the Armed Forces of Malta also fall within this category;

(vii) *Members of the administrative, management or supervisory boards of state-owned enterprises* – means members of the administrative, management or supervisory boards of commercial entities and companies in which the Government of Malta has an ownership interest or control of more than 50%.

It must be reiterated that the above list of who should be considered as a PEP in Malta is not exhaustive and represents only the list of prominent functions set out in the PMLFTR as interpreted in the local context. There are other public functions in Malta that can be considered as being "prominent" public functions which are not indicated above and which would qualify their holder to be considered as a PEP. Such prominent public functions would also include:

- Permanent secretaries within all the Government ministries;
- Chiefs of staff within all the Government Ministries; and
- The Commissioner and Deputy Commissioners of Police.

All Maltese individuals who are entrusted with a prominent public function equivalent to the above in a EU institution or other international body would be considered PEPs – such as the Maltese EU Commissioner, Maltese Members of the European Parliament, Maltese Members of the European Court of Auditors and of the European Court of Justice.

It is therefore emphasised that subject persons are required to assess on a case by case basis whether a particular office presents characteristics which would fall within the definition of a '*prominent public function*'.

With respect to the term 'family members' of PEPs, Regulation 11(8) of the PMLFTR defines the term as including:

(a) the spouse, or any person considered to be equivalent to a spouse;
(b) the children and their spouses, or persons considered to be equivalent to a spouse; and
(c) the parents.

The list of "family members" **is not an exhaustive list** and therefore subject persons should consider whether other family relationships in specific circumstances may be considered to be similar to those under the indicative list in the PMLFTR.
With respect to the term 'persons known to be close associates', the PMLFTR provide under Regulation 11(8) that the term means:

(a) a natural person known to have:

(1) joint beneficial ownership of a body corporate or any other form of legal arrangement;
(2) or any other close business relations,

with that PEP.

(b) a natural person who has sole beneficial ownership of a body corporate or any other form of legal arrangement that is known to have been established for the benefit of that PEP.

In the case of personal relationships, the social, economic and cultural context may also play a role in determining how close those relationships generally are. This process can even become more difficult when seeking to form a view on the status of close family members, such as children and their spouses, who may, in certain circumstances, be quite distant or estranged from their parent/s or other relative having a PEP-status. For the assessment of risk, it is the links between the close associate and/or family member with the PEP that determine the level of risk.

(b) How to determine that a person is a PEP?

Regulation 11(5) of the PMLFTR requires subject persons to maintain risk management procedures to determine whether a customer or a beneficial owner is a PEP. This requirement is not only applicable to prospective customers but also to existing customers, given that existing customers, or their family members or close associates, may become PEPs at a point in time in the course of an ongoing relationship.

Subject persons should therefore ensure that their risk management procedures incorporate a mechanism as to how ascertain when an existing customer becomes a PEP. This procedure should be incorporated within the ongoing monitoring systems of the subject person.

In determining whether the customer or a beneficial owner is a PEP, subject persons may:

(i) rely on publicly available information; or
(ii) obtain such information directly from the customer or beneficial owner; or
(iii) use commercial databases.

In relation to the publicly available information, subject persons should consider and assess the reliability of the sources being relied upon. Subject persons should consider referring to different sources rather than relying solely on one particular source, especially in higher ML/FT risk scenarios. All searches undertaken by the subject person should be duly documented and retained by the subject person.

Information obtained in terms of point (ii) above may be obtained from the customer' in response to a question posed in the application (or on-boarding) form where this forms part of the subject person's procedures. Alternatively, subject persons may develop a questionnaire with specific reference to criteria that identify PEPs (including for the avoidance of doubt, family members and persons known to be close associates of the PEP). Such a questionnaire would be required to be completed and signed accordingly by the customer and, where applicable, the beneficial owner. This questionnaire should be signed by the customer and the beneficial owner, where applicable.

On the basis of the risk procedures referred to in Chapter 3, subject persons should determine whether the use of commercial databases or other sources to confirm the information provided by the customer is necessary. Prior to making use of any commercial databases, subject persons should understand how a commercial database is populated and how it is able to detect and flag PEPs, family members and persons known to be close associates of PEPs, and hence determine whether such a commercial database would be adequate to assist the subject persons in identifying PEPs, family members and persona known to be close associated as required by the PMLFTR.

The application of EDD to PEPs, their family members and close associates is mandatory as long as a PEP remains entrusted with a prominent public function, as defined above, and for at least a subsequent 12 month period from when he ceases to be so entrusted. This however shall not mean that a subject person shall cease to carry out EDD measures upon the lapse of 12 months, where dealing with a person who was a PEP is still considered to expose the subject person to a high risk of ML/FT. Subject persons are at all times required to ensure that the CDD measures applied are commensurate to the risks of ML/FT posed by a particular business relationship or occasional transaction, and hence to apply EDD measures where a high risk of ML/FT is identified.

(c) EDD measures to be applied in relation to PEPs

Regulation 11(5) and (8) of the PMLFTR require subject persons to apply specific EDD measures in relation to PEPs, their family members and persons known to be close associates.

Since not every PEP poses the same risk of ML/FT, subject persons are required to assess and determine the level of ML/FT risk posed by that particular PEP, family member or person known to be a close associate. Subject persons should therefore assess the different types of risks it is exposed to (geographical, product/service/transaction, customer, delivery/distribution channel/interface) and determine, based on the customer risk assessment undertaken by the subject person, the level of EDD measures required in each particular case.

It is important to point out that, by classifying a business relationship or occasional transaction involving a PEP, family member or person known to be a close associate of the PEP as low risk, the subject person is not, however, exempt from applying the EDD measures set out in Regulation 11(5) of the PMLFTR. This notwithstanding, in cases where a business relationship or occasional transaction involving a PEP, is considered to pose a low risk, the subject person may apply a lighter level of EDD measures than in a higher risk case.

The following characteristics might suggest that a business relationship or an occasional transaction involving a PEP is of a low risk:

(a) customer is seeking to have access to a product/service/transaction which has been assessed by the subject person to pose a low risk (such as products, services or transactions which under other circumstances would qualify for SDD);
(b) customer does not have executive decision-making responsibilities (e.g. an opposition member of the House of Representatives, or a member of the party in government but with no ministerial office);
(c) the PEP is subject to rigorous disclosure requirements (such as registers of interests, independent oversight of expenses etc); and
(d) the PEP is entrusted with a prominent public function in a jurisdiction where information indicates that the jurisdiction shows the following characteristics (therefore, the subject person should assess the jurisdiction separately):

- low levels of corruption;
- political stability, and free and fair elections;
- strong state institutions;
- strong compliance with AML/CFT rules;
- a free press with a track record for probing official misconduct;
- an independent judicial and criminal justice system free from political interference;
- a track record for investigating political corruption and taking action against wrongdoers;
- strong traditions of audit within the public sector;
- legal protections for whistleblowers; or
- well-developed registries for ownership of land, companies, etc.

On the other hand, the following characteristics might suggest a PEP is of a higher risk:

(a) where the customer is seeking to have access to a product, service or transaction which is capable of being misused to launder the proceeds of corruption or bribery;
(b) personal wealth or lifestyle inconsistent with known legitimate sources of income or wealth;
(c) credible allegations of financial misconduct; and
(d) the PEP is entrusted with a prominent public function in a jurisdiction where there is a higher risk of corruption and where information is available indicating that the jurisdiction shows the following characteristics (therefore, the subject person should assess the jurisdiction separately):

- high levels of corruption;
- political instability;
- weak state institutions;
- weak AML/CFT defences;
- armed conflict;
- non-democratic forms of government;
- widespread organised criminality;
- political economy dominated by a small number of people or entities with close links to the state;

- lack of a free press where journalistic investigation is constrained;
- a judicial and criminal justice system vulnerable to political interference;
- lacking expertise and skills related to book-keeping, accountancy and audit, particularly in the public sector;
- law and culture antagonistic to the interests of whistleblowers;
- weaknesses in the transparency of registries of ownership of land, companies, etc.; or
- human rights abuses.

Moreover, the following characteristics might suggest a family member or a close associate of a PEP poses a higher risk:

- wealth derived from the granting of government licences (such as mineral extraction concessions, licence to act as a monopoly provider of services, or permission for significant construction or other projects);
- wealth derived from preferential access to the privatisation of former state assets;
- wealth derived from commerce in industry sectors associated with high-barriers to entry or a lack of competition, particularly where these barriers stem from law, regulation or other government policy;
- wealth or lifestyle inconsistent with known legitimate sources of income or wealth;
- credible allegations of financial misconduct (e.g. facilitated, made, or accepted bribes);
- appointment to a public office that appears inconsistent with personal merit.

When undertaking additional CDD measures on PEPs, their family members or persons known as close associates, subject persons must apply all the EDD measures set out in Regulation 11(5) of the PMLFTR, namely:

(a) *obtaining senior management approval;*

Obtaining the approval of senior management means having the approval of an officer or employee of the correspondent institution with sufficient knowledge of the subject person's ML/FT risk exposure and sufficient seniority to take decisions affecting its risk exposure. Such officer or employee need not be a member of the board of directors or equivalent body. The approval of senior management should be clearly documented and made available if required by the FIAU.

What will constitute senior management will depend on the size, structure and the nature of the subject person and it is possible that this decision be also taken by an internal committee of the institution. By requiring senior management approval, subject persons will ensure that they are not entering into a business relationship without applying the necessary controls.

The establishment of a business relationship, or a continuation thereof, or the undertaking of an occasional transaction, where the customer is a PEP, or with family members or persons known to be close associates of PEPs, require the prior approval of senior management, irrespective of the risk they pose. This notwithstanding, the level of escalation within the subject person's

structure will vary depending on the risk posed by the customer, as well as the entity structure and the level of delegation within the subject person's structure.

When considering whether to approve a PEP relationship, senior management should base their decision on the level of ML/FT risk the subject person would be exposed to if it entered into that relationship and how well equipped it is to manage that risk effectively.

(b) *taking adequate measures to establish the source of wealth and funds involved:*

Subject persons must in any case take adequate measures to establish:

- the source of wealth; and
- the source of funds

of the customer, in order to satisfy itself that it does not handle the proceeds from corruption or other criminal activity associated with PEPs. However, the extent of information and/or documentation to be requested by the subject person will vary depending on the risk posed by the customer.

In case of lower risk situations, the subject person may take less intrusive and less exhaustive steps to establish the source of funds and source of wealth of the PEP, family members or known close associates of the PEP. In such cases, the subject person may use information already available to the subject person (such as transaction records) or may rely on publicly available information and is not required to make further inquiries unless the subject person identifies certain anomalies from the information available to him.

It is necessary to seek source of wealth information but in all lower risk cases, especially when dealing with products, services or transactions that carry a lower risk of ML/FT, subject persons can minimise the amount of information they collect and how they verify the information provided.

In higher risk situations, subject persons are required to be more intrusive and rigorous, and should not rely on information provided by the customer in order to establish the source of funds and source of wealth of the PEP, family members or known close associates of the PEP. Subject persons shall refer to additional and multiple sources of information such as asset and income declarations, which some jurisdictions expect certain senior public officials to file and which often include information about an official's source of wealth and current business interests.[65]. Subject persons should also be aware that some jurisdictions impose restrictions on their PEP's ability to hold foreign bank accounts or to hold other office or paid employment. As part of its EDD measures, subject persons should consider, on a risk sensitive basis, whether the information regarding source of wealth and source of funds should be evidenced or verified. For example, for

[65] The World Bank has compiled a library on various countries' laws about disclosure of officials' income and assets. See http://publicofficialsfinancialdisclosure.worldbank.org/about-the-library

source of wealth or funds from inheritance, a copy of the will could be requested, or if from a sale of property, evidence of transfer of legal title could be sought.

For further information in relation to source of funds and source of wealth reference should be made to Section 4.4.

(c) *conducting enhanced ongoing monitoring*.

For low risk customers, the subject person is required to undertake less frequent reviews than higher risk customers. In the case of low risk customers, the subject person would be required to periodically review the CDD measures undertaken at the establishment of the business relationship and update the CDD documentation and information as appropriate. Subject persons would also be required review and where necessary update the CDD documentation and information obtained at the commencement of the business relationship when a new product, service or transaction is requested. Similar the regularity and extent of transaction monitoring should be less in the case of low risk customers, while ensuring that the subject person is all times able to detect suspicious or unusual types of transactions and activities.

For higher risk customers, a subject person's ongoing monitoring should be conducted more regularly (in some case prior to the carrying out of each and every transaction) and more thoroughly, and a closer analysis should be undertaken on the transactions and their origin. Subject persons should also regularly consider whether the business relationship with such customers should be maintained. For further information on ongoing monitoring reference should be made to Section 4.5.

In all cases subject persons should be able to identify suspicious or unusual transactions and should ensure that any new or emerging information that could affect the customer's risk assessment is identified in a timely manner and taken into consideration.

Subject persons should remember 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. Subject persons shall have appropriate systems and or procedures in place to ensure that they are able to detect when existing customers become PEPs, family members or close associates thereof. It is for this reason that an automated system of checks against publicly available information, or through specialist PEP databases of commercial service providers, would be useful in this respect, especially in the case of medium or large entities that have a considerable number of client and ongoing relationships.

4.9.2.3 EDD measures in the case of long-term insurance business

In the case of long-term insurance business, subject persons shall take reasonable measures to determine whether the beneficiaries of a policy and, where applicable, the beneficial owner of such beneficiary, are PEPs, their family members or known close associates, which measures shall

be taken no later than the time of payout or the time of the assignment, in whole or in part, of the policy.[66]

Therefore, not later than the time of payout, or the time of the assignment, subject persons are first expected to check whether there is any involvement of PEPs, family members or known close associates in the transaction. In the event that the beneficiary of the policy or, where applicable, the beneficial owner of the beneficiary are PEPs, family members or known close associates, senior management approval is required before proceeding with the payout under the policy. Moreover, subject persons are required to scrutinise the relationship with the policy holder to ensure that the policy would not have been misused to channel funds to the PEP (e.g. a long-term insurance is set up and withdrawn within a short period of time, or there seems to be no apparent or logical sense for the particular customer to be a beneficiary in a policy). Subject persons should be careful to assess the logical and economic rationale of the entire set up. The extent of the checks to be undertaken will vary depending on the level of risk which the customer poses.

4.9.2.4 Complex and unusually large transactions

Regulation 11(9) requires subject persons to, as far as reasonably practicable, examine the purpose and background of all complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. The degree and nature of the monitoring of such transactions and the business relationship within which such transactions are being undertaken shall be increased in order to ascertain whether such transactions or activities are suspicious of ML/FT activities.

This obligation requires subject persons to pay special attention to the following transactions:

(a) complex and unusually large transactions that have no apparent economic or lawful purpose;
(b) large transactions that have no apparent economic or lawful purpose;
(c) unusual patterns of transactions that have no apparent economic or lawful purpose; and
(d) transactions which are particularly likely, by their nature, to be related to ML/FT.

Unusual activity also includes anything that causes the subject person to doubt the identity of the customer (including beneficial owners) or anything that causes the subject person to doubt the good faith of the customer (including beneficial owners).

Unusual transactions may vary in nature and therefore there is no exhaustive list of transactions which are to be deemed as unusual. The below is a non-exhaustive list of unusual transactions:

(a) transactions or instructions which have no apparent legitimate purpose and appear not to have a commercial rationale;
(b) transactions, instructions or activity that involve apparent unnecessary complexity;
(c) where the transaction being requested by the customer is out of the ordinary range;
(d) the extensive use of non-cooperative tax jurisdictions where the customer's needs are inconsistent with the use of such services;

[66] Regulation 11(6) of the PMLFTR.

(e) unnecessary routing of funds through third party accounts;
(f) customer is not forthcoming with information about the transaction, activities relating to the transaction, reasons for the transaction, source of funds, CDD documentation, etc.;
(g) the size or pattern of the transactions is out line with expectations for that customer;
(h) where the customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period of time where such short duration was not expected;
(i) unusual investment transactions with no discernible purpose;
(j) extreme urgency in requests from the customer, particularly where they are not concerned by large transfer fees or early repayment fees; and
(k) transfers to or from high risk jurisdictions which are not consistent with the customer's expected activity.

Unusual transactions are detected either when carrying out ongoing monitoring of the business relationship, when establishing a new business relationship, when requested to carry out an occasional transaction or during ongoing communications with the customer, or when receiving instructions from the customer.

In such cases, subject persons are expected to perform EDD measures by making enquiries with the customer, asking the questions one would reasonably ask in the circumstances, performing appropriate scrutiny, and gathering additional information on the transaction and activities of the customer, including examining the purpose and background of such transactions.

Where a subject person identifies unusual activity, it has to perform 'appropriate scrutiny' of the activity and to obtain EDD. Appropriate scrutiny of the activity may involve making enquiries of the customer and asking the questions an honest man would reasonably ask in the circumstances.

By obtaining the above information, on a risk-sensitive basis, the subject person should be able to conclude whether a particular transaction is suspicious, and if so, file an STR with the FIAU. If the activity does not give rise to suspicion of ML/FT but still is unusual or risky, subject persons should assess whether the customer's risk assessment should be updated or whether more frequent ongoing monitoring should be undertaken. In the event that the risk assessment on the customer results not falling within the risk appetite of the subject person, the subject person may consider terminating or declining the business relationship or the occasional transaction with the customer.

Subject persons should ensure that the examination of the purpose and background of all complex and unusually large transactions and all unusual patterns of transactions, is duly documented and recorded.

For further information on the ongoing monitoring and the examination of complex and unusually large transactions and all unusual patterns of transactions, subject persons should refer to Section 4.5.

4.10 Reliance on Other Subject Persons or Third Parties

4.10.1 Introduction

The PMLFTR permit subject persons to rely on the CDD measures carried out by **other subject persons** or by **certain other third parties** (hereinafter collectively referred to as entities), subject to a number of conditions. A reliance arrangement can be set up where a customer is being serviced by two or more entities, or is in contact with multiple entities to a transaction (as further explained hereunder), with each entity obliged to carry out CDD measures on the customer.

Having multiple entities carrying out CDD measures on the same customer does not necessarily mitigate the risk of ML/FT or add value to the AML/CFT efforts being undertaken, and perhaps only adds inconvenience to the customer, who would need to provide multiple sets of CDD documentation to each of the entities involved.

The following are examples of scenarios where subject persons are able to rely on CDD carried out by other entities:

(a) Subject person A enters into a business relationship with the customer of subject person B by accepting instructions given through subject person B on behalf of the customer (e.g.: Maltese company service provider in Malta sets up a company in Malta for the client of a company service provider in another jurisdiction);
(b) Subject person A and subject person B both act for the same customer in respect of an occasional transaction (e.g.: subject person A is a the customer's lawyer while subject person B is the customer's accountant and are both assisting him in the acquisition of an undertaking); or
(c) Subject person A and subject person B form part of the same group of companies but carry out different relevant activities;

In these scenarios, subject person A can rely on the CDD measures carried out by subject person B.

4.10.2 Scope

As specified in Regulation 12(1) of the PMLFTR, subject persons may only rely on the CDD measures undertaken by other subject persons or third parties in relation to:

(a) the identification and verification of a customer;
(b) the identification and verification of beneficial owner(s), where applicable; and
(c) information on the purpose and intended nature of the business relationship and on the business and risk profile.[67]

The obligation to carry out ongoing monitoring of the business relationship as provided in Section 4.5 continues to rest with the subject person, which means that the subject person cannot rely

[67] Regulation 7(1)(a)-(c) of the PMLFTR.

on another subject person or third party to scrutinize transactions and, subject to what is stated further on, to keep information, data and documentation up-to-date.

Regardless of any reliance carried out, **subject persons always remain ultimately responsible for compliance with their CDD requirements** under Regulation 7(1). This means that subject persons may need to consider whether the entity relied on, in addition to meeting the criteria listed in this section, is sufficiently able to manage the inherent risk in the process. At the same time, subject persons have to bear in mind that the customer does not necessarily present the same level of risk to them as to the other entity being relied upon. This may render the CDD measures undertaken by that entity insufficient or inappropriate when it comes to mitigating the ML/FT risks to which the subject person placing reliance is being exposed to.

Furthermore, the subject person must understand whether the measures carried out by the other entity to counter the risks of ML/FT are equivalent to those that the subject person placing reliance deems sufficient. In this regard, the subject person should, prior to entering into a reliance arrangement, ensure that it understands the type of CDD measures which the entity undertakes on its customers.

Such assessments should be put down in writing and documented accordingly.

Moreover, subject persons may only rely on CDD measures actually carried out by the entity relied on. Thus, it cannot rely on information, data or documentation obtained by that entity or to which it has access through other reliance arrangements; having a chain of reliance arrangements is not permissible.

In terms of Regulation 12(6) of the PMLFTR, the provisions permitting reliance do not apply to outsourcing or agency relationships where, on the basis of a contractual agreement, the outsourcing service provider or agent is to be regarded as part of the subject person. These contractual relationships are not be regarded as reliance arrangements as, in the case of outsourcing, the subject person is delegating fulfilment of its obligations to a third party service provider who has no relationship with the subject person's customer while in the case of an agency arrangement, the agent is merely an extension of the subject person not a separate and distinct entity with its own CDD obligations. Thus, in both instances it is the subject person who is considered as carrying out the CDD measures fulfilled either by the outsourced service provider or by its agent.

4.10.3 Entities that may be relied on

All subject persons may rely on the CDD measures carried out by:

(1) Persons falling within the definition of 'subject person' under the PMLFTR;
(2) Third parties being:

(a) Persons or institutions undertaking activities equivalent to 'relevant financial business' or 'relevant activity';
(b) Member organisations or representative bodies of such persons; or
(c) Other institutions or persons in an EU Member State or other third country;

As long as the persons listed under (2) above also:

(i) apply CDD requirements and record keeping requirements that are consistent with those laid down under the PMLFTR; **and**
(ii) have their compliance with AML/CFT obligations monitored in a manner which is consistent with Section 2 of Chapter VI of Directive (EU) 2015/849 (4th AML Directive).

Subject persons **may not** rely on third parties from a non-reputable jurisdiction, unless such third parties are branches or majority-owned subsidiaries of persons or institutions established in a Member State subject to national provisions implementing the 4th AML Directive and which comply fully with group wide policies and procedures equivalent to those listed in Regulation 6 of the PMLFTR.

Assessing consistency

When assessing whether a third party satisfies the conditions under points (a) and (b) above, subject persons should assess whether the requirements in the jurisdiction where the third party is established are similar to those imposed by the PMLFTR and these Implementing Procedures. In this regard, subject persons should consider the equivalence of the following matters, as a minimum:

(i) identification details of the customer and the beneficial owner (refer to Section 4.3.1);
(ii) instances where EDD measures should be applied (refer to Section 4.9);
(iii) timing of the application of CDD measures (refer to Section 4.6);
(iv) record keeping requirements, including retention periods (refer to Chapter 9);
(v) AML/CFT policies and procedures equivalent to those required under the PMLFTR and these Implementing Procedures; and;
(vi) that the effective implementation of the measures and requirements referred to above is subject to supervision by a supervisor or other appropriate body.

In applying a risk-based approach, subject persons may opt to extend their assessment by considering other factors over and above those required by the Regulations.

Furthermore, in order for the requirements to be deemed consistent, subject persons must also assess whether the relevant laws and regulations of that jurisdiction have been **effectively implemented** in that country. In this regard, subject persons would need to consider whether

there are any structural elements or other issues in that jurisdiction which hamper the proper implementation and enforcement of the AML/CFT laws and regulations..

In determining the equivalency or adequacy of CDD and record keeping requirements and supervision, regard has to be made to any FATF or FSRB Mutual Evaluation Reports which would present an assessment of a country's adherence and implementation of AML/CFT obligations and supervision.

In all cases, subject persons are expected to assess the subject persons or third parties being relied on, regardless of whether that entity is established within Malta, an EU Member State or a third jurisdiction. In doing so, subject persons may, on a risk-sensitive basis, take into consideration issues such as:

(a) any publicly available regulatory or supervisory adverse information on the entity being relied upon;
(b) the nature of the customer, the type of products or services being offered or transactions undertaken, and the value of the transactions;
(c) any known adverse experience with the entity relied upon to the extent that these may affect compliance by the subject person with its obligations;
(d) any other knowledge, whether obtained at the outset of the relationship or subsequently, that the subject person has regarding the standing of the entity.

It should generally be noted that subject persons may recognise and accept the outcome of the relevant CDD measures carried out in accordance with provisions equivalent to the PMLFTR, by third parties as explained above, even if the documents or data through which such requirements have been fulfilled are different to those under domestic requirements.

4.10.4 Carrying out reliance

The subject persons placing reliance should immediately obtain from the subject person or third party being relied on, the information required under Regulation 7(1)(a) to (c) of the PMLFTR. This means that regardless of the fact that the subject person is relying on another entity for the fulfilment of CDD requirements, the subject person must still obtain the **information** concerning the identity of the customer, the identity of the beneficial owner(s) (where applicable), and information on the purpose and intended nature of the business relationship and the customer's business and risk profile..

All this information must be obtained by the subject person before carrying out an occasional transaction or entering into a business relationship. This is due to the fact that, when placing reliance, the subject person must at least have the customer's (and beneficial owner's, where applicable) identification data on file to enable it to perform its customer risk assessment and also to comply with its ongoing monitoring obligations, where applicable.

Where reliance in accordance with Regulation 12 of the PMLFTR is being made, the subject person placing reliance is not obliged to receive copies of the identification and verification data and other relevant documentation obtained by the other subject person or third party being relied on for the above-mentioned purposes, unless the subject person requests the entity being relied on to provide such information. This is in line with the principle behind reliance; i.e. that multiple requests for documentation are not always necessary, and that one has relied on a reputable entity to carry out verification. It is to be further noted that in the case of verification data and/or documentation, the subject person has to rely on the entity with whom it has entered into a reliance arrangement even for keeping the same up-to-date as it would otherwise be impractical to seek updated documentation directly from the customer.

Should the subject person require such information and documentation it must be forwarded by the entity being relied on immediately upon request.[68]

4.10.5 The reliance agreement

Regulation 12(4) requires subject persons to **take adequate steps** to ensure that, upon request, the entity relied upon immediately forwards relevant copies of the identification and verification documents concerning the CDD measures undertaken.

In this regard, subject persons shall have a written and signed formal agreement with the entity, which would regulate the procedures and conditions concerning such requests, in order to ensure that the data is made available immediately.

Subject persons should also consider carrying out occasional tests to ensure that the entity being relied upon is in a position to provide the requested information and documentation and, moreover, to ensure, from time to time, that the CDD measures undertaken by the entity are satisfactory. Subject persons should also bear in mind that in the case of a request for information from the FIAU, the information is to be furnished by the subject person within 5 days from the request[69], regardless of whether the CDD measures were carried out by an entity being relied upon. This may need to be factored into the agreement, to ensure that the subject person remains in a position to fulfil its obligations at all times.

The agreement has to also provide for situations where the entity terminates its business relationship with the customer, or ceases to operate altogether, in order to ensure that the subject person is still in a position to fulfil its obligations at law, even where the reliance agreement ceases to be in force.

Finally, subject persons should also ensure that they remain in a position to fulfil their record keeping obligations, particularly in view of the retention periods stipulated in Regulation 13, and any extensions thereof.

[68] Regulation 12(4) of the PMLFTR.
[69] Regulation 15(8) of the PMLFTR.

The agreement must be retained by the subject person as part of its record keeping obligations, together with any copies of the documentation forwarded by the subject person or third party being relied upon.

4.10.6 When reliance is not permitted

Where the FIAU determines or is informed that a jurisdiction does not meet the criteria of a reputable jurisdiction, and the criteria for a third party, it shall, in collaboration with the relevant supervisory authorities, prohibit subject persons from relying on persons or institutions from that particular jurisdiction for the performance of CDD requirements. For further information on the notion of a 'non-reputable jurisdiction' subject persons should refer to Section 8.1.

CHAPTER 5 – REPORTING PROCEDURES AND OBLIGATIONS

Subject persons are required to have internal and external reporting procedures in place for the purpose of reporting to the FIAU any knowledge or suspicion of ML/FT, and any knowledge or suspicion that funds or property are the proceeds of criminal activity.

Throughout this chapter, whenever reference is made to knowledge, suspicion or reasonable grounds to suspect ML/FT, this shall also be deemed to include knowledge, suspicion and reasonable grounds to suspect that funds or property are the proceeds of criminal activity. References to knowledge or suspicion of ML/FT are to be deemed as also including references to reasonable grounds to suspect.

5.1 The Money Laundering Reporting Officer

5.1.1 The Role of the MLRO

Regulation 15 of the PMLFTR[70] requires a subject person to appoint one of its officers as MLRO, the core functions of whom are:

(a) Receiving reports of knowledge or suspicion of ML/FT or that a person may have been, is or may be connected with ML/FT from the subject person's employees;
(b) Considering such reports to determine whether knowledge or suspicion of ML/FT subsists or whether a person may have been, is or may be connected with ML/FT;
(c) Reporting knowledge or suspicion of ML/FT or of a person's connection with ML/FT to the FIAU; and
(d) Responding promptly to any request for information made by the FIAU.

5.1.2 Who Can be Appointed as MLRO

Not any officer of the subject person can be appointed as MLRO as in terms of the PMLFTR the officer appointed to this position has also to be of sufficient seniority and command:

(a) ***Officer of a Subject Person***

For the purposes of identifying an individual who can be appointed as MLRO, there must subsist an employment relationship between the officer and the subject person. Alternatively, an executive director, or anyone in an equivalent position in the case of subject persons set up other than as companies, can also be appointed as MLRO.

In addition the functions of a MLRO may not be:

- outsourced;
- carried out by a non-executive director of the subject person;

[70] Regulation 15(1)(a) of the PMLFTR.

- carried out by a person who only occupies the position of company secretary of the subject person and does not hold any other position within the organisation; or
- carried out by a person who undertakes internal audit functions within the organisation.

Notwithstanding the above, there are situations where the person appointed as MLRO need not be an officer in employment or an executive director of the subject person. These are:

(i) In the case of an insurance company managed by a company that is enrolled to act as an insurance manager in terms of the Insurance Intermediaries Act[71], it may enter into an arrangement with the insurance manager to have the duties attributable to the MLRO of the insurance company carried out by the MLRO of its manager;

(ii) In the case of a collective investment scheme that is subject to the PMLFTR and which does not have a physical operational set-up in Malta other than a registered address and a board of directors, does not engage any employees and is not involved in the acceptance and processing of subscriptions and the collection of funds from investors, to have the duties attributable to the MLRO of a collective investment scheme carried out by the MLRO of its administrator

The above outsourcing arrangement may only be entered into when (a) either the administrator is recognised under the Investment Services Act[72]; or (b) the administrator is subject to authorisation, licensing or recognition in a Member State or in third country other than a non-reputable jurisdiction, is subject to AML/CFT obligations consistent with the PMLFTR especially in relation to reporting and reporting procedures, and is supervised for compliance with these obligations.

(iii) In the case of a group comprising two or more subject persons which can avail themselves of the exemptions allowed in terms of Regulation 16(2)(b) and (c), the said subject persons may designate one of their employees as group-wide MLRO, with each individual subject person to consider whether the appointment of a designated employee is necessary to assist the MLRO to meet his functions effectively;

(iv) In the case of a group comprising two or more subject persons, it is possible for the employee of one subject person to be seconded with another subject person forming part of the same group to act as its MLRO. Where the group also includes an entity to which subject persons within the group have delegated fulfilment of their AML/CFT obligations, it is possible for an employee of sufficient seniority and command within the said entity to be seconded with a subject person within the group as its MLRO.

It is important that whoever is designated as the subject person's MLRO is present from where the activities of the subject person are being directed and the relative back office operations are being conducted. This to ensure that the MLRO has access to the necessary

[71] Cap 497 of the Laws of Malta.
[72] Cap 370 of the Laws of Malta

information to carry out his role effectively. Thus, it is not necessary for the MLRO to be present in Malta.

It is also relevant to point out that where an employee is acting as MLRO for two or more subject persons, it has to be ensured that these multiple appointments still allow the MLRO to fulfil his functions in an effective manner. Moreover, the person fulfilling MLRO duties has to be mindful of any ensuing conflicts of interest and/or confidentiality obligations. While there is no set number of appointments that one may accept as MLRO, the more appointments one holds and the more complex or voluminous the activities of the subject person concerned, the more difficult it will inevitably become for the MLRO to meet his obligations at law in a satisfactory manner.

(b) ***Sufficient Seniority and Command***

The MLRO must occupy a senior position within the institution where effective influence can be exercised on the subject person's AML/CFT measures, policies, controls and procedures and should not be precluded from posing effective challenge where necessary. Thus, the person occupying this position must be able to, where he deems it necessary, communicate directly with the Board of Directors.

The MLRO must also have the authority to act independently in carrying out his responsibilities and should have full and unlimited access to all records, data, documentation and information of the subject person[73] for the purposes of fulfilling his responsibilities.

Where the subject person is a sole trader or a sole practitioner with no employees or no persons working within his practice, the subject person has to carry out the functions of MLRO himself.

5.1.3 Appointment and Resignation of the MLRO

The appointment of a MLRO has to be notified to the FIAU through the submission of the MLRO Details Sheet which can be downloaded from the FIAU's website – http://www.fiumalta.org/submit-MLRO-details-sheet. There may be situations where the prior approval of a supervisory authority is required to proceed with the appointment of a MLRO. In this case, the FIAU should be notified only once the relevant supervisory authority issues the necessary approval.

In exceptional circumstances, where an existing MLRO resigns or is dismissed and a new MLRO is pending approval by a supervisory authority, the subject person should inform the FIAU of as much and provide the FIAU with the details of an employee who for the interim period will be assuming the role of reporting officer and to whom any requests or queries by the FIAU can be addressed. This employee may be a previously appointed designated employee.

[73] Regulation 15(1)(c) of the PMLFTR.

A subject person has to notify the FIAU of the resignation or removal of its MLRO as soon as reasonably practicable upon becoming aware of the proposed resignation or removal. The MLRO also has to notify the FIAU whether his departure was in any way linked to the implementation of the subject person's obligations under the PMLFTR and whether this had any regulatory implications which should be brought to the attention of the FIAU. This latter notification is to be made within **15 days** from the date of resignation or removal.

5.2 The Designated Employee

Given the functions that the MLRO has to carry out, it is imperative that he is available at all times. However, it is recognised that this is not always possible and that the volume of internal reports he may have to consider may undermine his effectiveness. To this end, subject persons are to consider whether there is the need to appoint a designated employee to assist and, if necessary, temporarily replace the MLRO.

The main purpose of a designated employee is to deputise for the MLRO. Therefore, each subject person can consider appointing one designated employee for such purpose. However, the FIAU will also consider, on a case by case basis, the possibility of allowing a subject person to appoint two or more designated employees, after taking into account the size and nature of the subject person and its activities. In any such instance, the subject person has to obtain prior approval from the FIAU.

Employees who only assists the MLRO through the processing of internal reports, collection of information, liaising with other units or sections with the subject persons etc. are not deemed to be acting as designated employees. Deputising for the MLRO is deemed to involve more onerous obligations and entails that the designated employee can in his own right determine that an STR is to be filed in those situations where the MLRO is absent. Thus, any reference to the MLRO in these Implementing Procedures is to be construed as referring also to the designated employee.

The appointment of the designated employee must receive the approval of the MLRO[74] and such appointed person shall work under the MLRO's direction. The appointment of the designated employee must be notified to the FIAU through the submission of the MLRO Details Sheet which may be downloaded from the FIAU website on http://www.fiumalta.org/submit-MLRO-details-sheet.

5.3 The Monitoring Function

The PMLFTR make reference to a general oversight function as well as to the possible creation of a day-to-day monitoring function:

(a) Day-to-Day Monitoring Function

[74] Regulation 15(1)(f) of the PMLFTR.

In terms of Regulation 5(5)(c), a subject person has to consider whether in view of the nature and size of its business there is a need to appoint an officer at management level whose duties are to include the monitoring of the day-to-day application of the measures, policies, controls and procedures adopted by the subject person to ensure compliance with its AML/CFT obligations.

In carrying out its business, a subject person may employ a considerable number of employees or structure its organisation in multiple units, offices or branches. Moreover, the business being carried out may itself involve a number of different activities. The same AML/CFT controls, policies measures and procedures would have to be applied and ensuring this is done in a uniform albeit flexible manner may prove impossible if there is no one officer charged with this responsibility.

Where a subject person considers this function to be necessary, it is left to the subject person to determine whether this function is to be also carried out by the MLRO or whether it would prove to be more effective if it is entrusted to a separate officer. In the latter case, it would be especially important that communications between the two be as good as possible to ensure the effectiveness of the subject person's AML/CFT controls, policies, procedures and measures.

Where the subject person opts to outsource its AML/CFT obligations in line with Chapter 6, the monitoring role would involve ensuring that the outsourced service provider is fulfilling its contractual obligations and carrying out the necessary controls, and to monitor the implementation of those AML/CFT obligations, if any, that have not been outsourced. In such a scenario, the subject person has to decide, based on the volume of oversight work involved, whether a dedicated monitoring function is necessary or whether such role could be equally handled by the MLRO.

Where the said function is entrusted to someone other than the MLRO, it has to be carried out by:

(i) an officer of the subject person; and
(ii) the said officer has to be at management level.

These two requirements are considered as being equivalent to the requirements for the appointment of a MLRO, i.e. an officer of the subject person having sufficient seniority and command, and are therefore to be construed in the same manner, including the restrictions on outsourcing.

The one exception relates to the possibility of having a group-wide monitoring function. In this case there would be no limitation arising from the non-disclosure requirements set out by Regulation 16 of the PMLFTR and the possibility of a group-wide monitoring function could be availed of independently of the activities carried out by the subject persons comprised therein. However, subject persons would have to consider whether it may be necessary to appoint employees within the individual subject persons included

within the group to assist the officer entrusted with the group-wide monitoring function so as to ensure its effectiveness.

Although the PMLFTR only provide a very generic description of what the duties and responsibilities of any such officer should be, it would be expected that the said officer would be responsible for:

- ensuring continued compliance with the requirements of the PMLFTR, FIAU Implementing Procedures or other guidance issued by the FIAU;
- day-to-day oversight of the subject person's AML/CFT measures, policies, controls and procedures;
- regular oversight reporting, including reporting of non-compliance, to senior management;
- addressing any FIAU feedback about the subject person's risk management performance or AML/CFT measures, policies, controls and procedures;
- contributing to designing, implementing and maintaining internal AML/CFT compliance manuals, policies, procedures and systems;
- conducting or seeing to periodic internal AML/CFT training for all relevant staff members and employees (refer to Chapter 7 of these Implementing Procedures).

While some of these duties can be delegated to other employees of the subject person, the officer entrusted with the monitoring function retains responsibility for implementing and assessing the ongoing operation of the subject person's AML/CFT measures, policies, controls and procedures.

As is the case with the MLRO, the appointment, removal or resignation of an officer to which the day-to-day monitoring function is entrusted has to be notified to the FIAU in the same manner as for the MLRO. However, in this case the subject person is to use the form available on the FIAU's website.

(b) General Oversight Function

Given that the subject person is ultimately responsible for ensuring compliance with its AML/CFT obligations, the PMLFTR provide that the board of directors or administrators, or any other equivalent body responsible for the management of the subject person, has to designate one of its members with responsibility to ensure that the subject person is fulfilling its AML/CFT obligations.

In view of the above, it is important that senior management provides the MLRO and its monitoring function sufficient resources, including appropriate staff and technological means, to ensure that they are able to carry out their obligations effectively.

5.4 Internal Reporting Procedures

The internal reporting procedures of a subject person have to clearly set out the steps to be followed when an employee of the subject person knows or suspects that a person or a

transaction is connected to ML/FT. Reference to the reporting obligations of an employee are also understood to be applicable to those officers of a subject person who may not have an employment relationship with the subject person (such as temporary or contract staff).

The procedures should clearly state that when an employee has any such information, he is to report the matter to the MLRO without delay. Therefore it is crucial that all employees are informed of the identity of the MLRO to whom the report is to be made, the procedure to follow and the information that has to be made available with the report.

Internal reports are to be submitted in writing, preferably using a standard template, together with all relevant information and documentation available to the employee so as to assist the MLRO in making a determination as to how best to proceed. The report should include details on the customer who is the subject of concern and as full a statement as possible of the information giving rise to the knowledge or suspicion.

Reporting lines should be kept as short as possible, ideally allowing an employee to report directly to the MLRO so as to ensure speed, confidentiality and quick access to the MLRO. However, it is acknowledged that in larger organisations this may not always be possible and may even prove to be counter-productive. In these cases, it is acceptable for the internal reporting procedures to provide for intermediate filtering stages. Thus, it is possible that a subject person's internal reporting procedures will provide for an employee to discuss the circumstances surrounding a particular customer or transaction with his immediate superior prior to determining whether to submit an internal report. Another option would be to have a specialised team who is to consider reports made by employees and forward to the MLRO only those which do contain the basis of knowledge or suspicion of ML/FT.

The same applies with regards to the use of software solutions to identify transactions or patterns of transactions which are unusual or exceed a given threshold as part of a subject person's ongoing monitoring systems. The reports generated by any such software solution need not be transmitted automatically to the MLRO for his consideration but may be further filtered and analysed, and only those transactions found to have an indication of knowledge or suspicion of ML/FT forwarded to the MLRO for his consideration.

However, when extending reporting lines in this manner, including situations where the subject person has outsourced ongoing monitoring to a third party, it is important that:

(a) The MLRO understands and is in agreement with the filtering criteria used and analytical methodology applied to identify those reports that he is to receive. Where reviews are carried out on the effectiveness of the procedures adopted by the subject person, these are to be made available to the MLRO with sufficient information to allow him to raise any concerns he may have in relation to these procedures and ensure these are considered and, if necessary, properly addressed.

(b) Where a decision is taken not to proceed with submitting an internal report to the MLRO, a written record is kept of the circumstances of the case and of the reasons why it was decided not to file an internal report. These records are to be available to the MLRO and,

if applicable, to the officer entrusted with the monitoring function and to the subject person's internal audit function. An internal audit function should not be here construed as necessarily being one carried out by an employee or officer of the subject person but may also involve an audit or review carried out by an external consultant. These records may provide important information on the effectiveness of a subject person's internal procedures and their review can lead to the eventual improvement of one's internal reporting procedures.

(c) Where a decision is taken not to forward a report to the MLRO, the employee who made the report has to be informed of the decision. If the employee still considers that the report should be escalated to the MLRO, the internal procedures should be such as to still enable the employee to submit the report directly to the MLRO.

It is possible that additional internal reports may have to be made following the submission of an initial report as the employee may notice further transactions or activities that give rise to knowledge or suspicion of ML/FT. These too need to be reported to the MLRO.

The MLRO must consider, without delay, every internal report he receives in order to determine whether or not the information contained in the report:

(a) does give rise to a knowledge or suspicion of ML/FT; or
(b) whether additional information is necessary to reach such a determination.

In the latter circumstances, the MLRO must collect and consider without delay any additional information and/or documentation he deems relevant to make the said determination, which may include:

(a) previous transactions, transaction patterns and volumes, previous patterns of instructions, the duration of the business relationship and CDD information;
(b) where applicable, other connected accounts and the existence of other relationships, including where the person suspected of ML/FT:
    (1) is a settlor, donor, contributor, protector, trustee or beneficiary of a trust, foundation, trust account or other trust or fiduciary relationship with the subject person; or
    (2) is a beneficial owner, director, shareholder or legal representative of a legal entity or other legal arrangement having a business relationship with the subject person; or
    (3) holds a power of attorney or has any fiduciary arrangements related to a business relationship with the subject person; and
(c) other information or documents which are reasonably accessible through public sources.

Failure by the MLRO to diligently consider all relevant material available to the subject person may lead to vital information being overlooked and the knowledge or suspicion not being disclosed to the FIAU. In view of this requirement, the MLRO should be granted unrestricted access to all relevant documentation.

The decision to file or not to file an STR must always be the MLRO's/designated employee's own decision, and should not be subject to the direction or approval of other parties within the subject person. This is not to say that in making a determination as to whether an internal report gives rise to knowledge or suspicion of ML/FT, the MLRO cannot seek assistance, including from external advisors. However, this has to be done discreetly, in an anonymised manner and restricted specifically to the matter requiring input from advisors, taking into consideration the non-disclosure obligations that subject persons have to adhere to.

If the MLRO concludes, for justifiable reasons, that an internal report does not give rise to knowledge or suspicion of ML/FT, the MLRO need not file a report with or otherwise inform the FIAU.[75] In this case, the MLRO must keep a written record of the internal report received, the assessment carried out, the outcome and the reasons why the report was not submitted to the FIAU. Upon request by the FIAU or the relevant supervisory authority acting on behalf of the FIAU, the MLRO will make such information available.

5.5 External Reporting Procedures

After considering the internal report and all the necessary documentation, where the MLRO or the designated employee determines that the subject person:

(a) knows,
(b) suspects; or
(c) has reasonable grounds to suspect that:
- a transaction may be related to ML/FT; or
- a person may have been, is, or may be connected with ML/FT; or
- ML/FT has been, is being, or may be committed or attempted,

the MLRO must file a STR with the FIAU as set out hereunder.[76] In so doing, the MLRO is not to disclose the name of the employee who made the internal report to the FIAU.

The PMLFTR require the MLRO to report to the FIAU when he has **knowledge**, **suspicion** or **reasonable grounds** to suspect ML/FT or that funds (regardless of the amount involved) are the proceeds of criminal activity. The same obligation to file an STR applies to a sole trader or sole practitioner with no employees or no persons working within his practice, who has a similar knowledge, suspicion or reasonable grounds to suspect.

A brief explanation of these three concepts is provided below:

(i) Knowledge

Being an objective criterion, the existence of knowledge of ML/FT is not difficult to ascertain as a person either knows something or does not. If for any reason the MLRO, or any other employee of the subject person, is aware or is in possession of information that indicates

[75] Regulation 15 (6) of the PMLFTR.
[76] Regulation 15(3) of the PMLFTR.

that any of the above activities may have taken place, are taking place, or will be taking place, the MLRO should immediately proceed with filing a STR with the FIAU.

(ii) Suspicion

Suspicion of ML/FT is more subjective than knowledge and in order to determine its existence the MLRO must rely on objective criteria, which differs depending on the circumstances. For instance, an unemployed customer of a bank depositing considerable amounts of money into his bank account should raise the suspicion of the bank. In this case the objective element is the fact that the person is unemployed and although the bank does not have any concrete evidence that the money derives from an illegal activity there are objective indications pointing to such a possibility. Another objective element on which suspicion may be based, which is specifically referred to in the PMLFTR,[77] is the situation where the subject person is unable to complete customer due diligence due, for instance, to the unwillingness of the applicant for business to provide the required documentation or information. In such a case, the PMLFTR require the subject person to consider filing a report with the FIAU.

Certain pronouncements by the courts in the United Kingdom may be of assistance in determining what constitutes 'suspicion' for the purposes of the PMLFTR and the degree of suspicion that is required for an STR to be made:

"***A degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not***".

"***Although the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation***."

In ***R v Da Silva*** [2006] 4 All ER 900, the UK Court of Appeal stated the following:
"***It seems to us that the essential element in the word 'suspect' and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice. But the statute does not require the suspicion to be 'clear' or 'firmly grounded and targeted on specific facts***".

Furthermore in ***Shah & Another v HSBC Private Bank (UK) Limited*** [2012] EWHC 1283 (QB)., the UK High Court held that "[t]***o be a suspicion rather than a mere feeling of unease it must be thought to be based on possible facts, but the sufficiency of those possible facts as a grounding for the suspicion is irrelevant…***"

The Court in this case further stated that:

"Parliament intended suspicion as a subjective fact to be sufficient (1) to expose a person to criminal liability for money laundering and (2) to trigger disclosures to the authorities.

[77] Regulation 8(5) of the PMLFTR.

Parliament did not require, in addition, that the suspicion be based upon "reasonable" or "rational" grounds. There are good practical reasons for this. Unlike law enforcement agencies, banks have neither the responsibility nor the expertise to investigate criminal activity to satisfy themselves that the grounds for their suspicion are well founded, reasonable or "rational"."

A transaction which appears *unusual* is not necessarily *suspicious*. Even customers with a stable and predictable transactions profile will have periodic transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. So the unusual is, in the first instance, only a basis for further enquiry which may in turn require judgment as to whether it is suspicious.

(iii) Reasonable Grounds to Suspect

The requirement to file a STR goes beyond "suspicion" and also includes the obligation to report when "reasonable grounds to suspect" exist. This implies that a further obligation to report arises where, on the basis of objective facts or circumstances, a reasonable person would have inferred knowledge or formed the suspicion that ML/FT existed or that funds were the proceeds of criminal activity.

It should also be kept in mind that a transaction may not be suspicious at the time, but suspicions may arise later, in which case the obligation to file a STR still arises.

Any disclosures should be made to the FIAU as soon as is reasonably practicable, but **not later than five (5) working days** from when the knowledge or suspicion of ML/FT first arises or from the existence of reasonable grounds to suspect ML/FT.

The five (5) working days, which are referred to in Regulation 15(3) of the PMLFTR, shall be deemed to start to run in accordance with the provisions of the following paragraphs:

(a) in cases where, subsequent to the receipt of an internal report, the MLRO determines, on the basis of additional information and/or documentation other than what is contained in the internal report received by the MLRO, that there is knowledge or suspicion of ML/FT, the five (5) working day period shall start to run from when such a determination is made by the MLRO;

(b) notwithstanding the provisions of paragraph (a), where the subject person is in possession of information that constitutes a reasonable ground to suspect ML/FT, the five (5) working days shall start to run from when the subject person came into possession of or became aware of that information, independently of when the same information was brought to the attention of the MLRO.

Timing is an aspect that should be clearly considered by subject persons when drawing up their internal reporting procedures, especially if they include intermediate filtering levels.

STR are to be submitted to the FIAU through the FIAU website (http://www.fiumalta.org) using the provided template. Guidance on STR reporting is also provided on the FIAU's website. In

exceptional cases, where subject persons do not have access to IT systems to submit STRs online, manual submissions are also accepted. In completing this report MLROs should seek to provide as much detail as possible together with the relevant identification and other supporting documentation.

For the avoidance of any doubt, in those circumstances where the STR is not filed electronically but submitted to the FIAU in paper format, the physical act of submitting an STR need not be undertaken by the MLRO himself; his responsibility is that of making a reasoned determination as to whether a STR must be submitted or otherwise. Therefore the submission itself may be done by any employee of the subject person who is acting under the responsibility of, or answers to, the MLRO.

It is important to keep in mind that subject persons must file STRs only with the FIAU and with no other supervisory authority.

5.6 Actions After Reporting

Upon receipt of a STR the FIAU sends an acknowledgement to the subject person and the process for assessing the STR is then initiated by the FIAU's Analysis Section.

In the course of the analysis of the STR, the FIAU may require further information and, in terms of the PMLFTR, it can request such information from the subject person filing the STR or any other subject person.[78] When the FIAU makes a request for information to a subject person, that subject person has to comply with the request as soon as is reasonably practicable but not later than **five (5) working days** from when the demand is first made,[79] unless the subject person makes representations justifying why the requested information cannot be submitted within the said period of time. The FIAU can, at its discretion and after having considered such representations, extend such time as is reasonably necessary to obtain the information. The subject person shall then submit the information requested within the extended time limit. Subject persons should make a request under this provision with caution and only where absolutely necessary as its frequent use could hinder the FIAU in the conduct of its duties.

It should be noted that in terms of the proviso to Regulation 15(8) of the PMLFTR, the FIAU may, following the submission of an STR or when it deems necessary, demand that the information be submitted within a shorter period of time.

If once an STR is filed the subject person decides to maintain the business relationship with the customer who is the subject of the STR, the subject person should:

(a) classify the customer as a **high-risk customer;** and
(b) remain vigilant and monitor the activities of that customer to a larger extent.

[78] Regulation 15(8) of the PMLFTR.
[79] *ibid*.

It is to be noted that in such circumstances subject persons should not automatically report to the FIAU every transaction carried out by that customer after the STR has been filed. Subject persons should analyse the circumstances of the case and where necessary consider passing on additional information to the FIAU. For instance, if a customer who has been subject to an STR receives his monthly salary into the same account through which a suspicious transaction was deemed to have been carried out, the subject person would not be expected to report such a transaction. However, if a transaction similar to the transaction which had been reported to the FIAU were to be carried out, such transaction is likely to give rise to a further suspicion and would therefore be reportable.

Additionally, before taking any decision related to a customer and services provided thereto, which may have an impact on the analysis or any future investigation, it would be advisable to hold discussions with the FIAU prior to carrying out such transactions to ensure that the steps taken by the subject person do not hinder the analysis or the investigation. This may involve the return of funds to the customer or the termination of the business relationship.

Subject persons filing an STR with the FIAU may request feedback from the FIAU on the progress of the analysis of the STR. The FIAU may also, on its own motion, provide feedback to subject persons making an STR. When giving feedback, the FIAU will provide the reporting subject person such information as it considers to be of interest to the subject person in order to enable that subject person to regulate its affairs and to assist it to carry out its duties under the PMLA and the PMLFTR. Subject persons must treat feedback information with utmost confidentiality.

5.7 The obligation to refrain from carrying out a transaction that appears to be suspicious

In accordance with Regulation 15(4) of the PMLFTR, where subject persons know or suspect that a transaction that is still to be carried out is or may be related to proceeds of criminal activity or the funding of terrorism, the subject person, upon informing the FIAU thereof in terms of Section 5.5 above, must, in terms of Article 28 of the PMLA, refrain from carrying out the transaction. In such cases subject persons shall provide the FIAU with all the information concerning the transaction. Therefore subject persons are required to delay the transaction to allow the FIAU time to consider whether or not to oppose the execution of the transaction.

This notwithstanding, Regulation 15(5) states that where it is not possible for subject persons to refrain from carrying out a transaction which is known or suspected to be related to ML/FT prior to informing the FIAU, subject persons shall carry out the transaction and inform the FIAU immediately after the transaction is effected. However, it is important to note that the impossibility to do so must be due either to the nature of the transaction (e.g. the system used to process the transaction does not allow at any point human interference such as automated clearing or settlement systems) or because refraining from executing the transaction is likely to frustrate efforts for investigating or pursuing the beneficiaries of the suspected criminal activity.

This obligation is mirrored in article 29 of the PMLA which states that where the subject person is unable to inform the FIAU before the transaction is executed either because it is not possible to delay executing the transaction due to its nature or because delay in executing the transaction could prevent the prosecution of the individuals benefitting from the suspected ML/FT, subject

persons shall carry out the transaction and shall inform the FIAU immediately afterwards giving the reasons why the FIAU was not so informed before executing the transaction.

In these two provisions, besides the failure to inform the FIAU because of the likelihood of frustrating investigation and prosecution efforts, the law states that it is only in cases where it is not possible to refrain from executing the transaction that the subject person may carry out the transaction and this impossibility must arise from the nature of the transaction itself.

5.8 Delaying the Execution of a Suspicious Transaction

Under Article 28 of the PMLA the FIAU itself may oppose the execution of a transaction which it knows or suspects to be related to ML/FT. This power may be exercised by the FIAU when it becomes aware of a prospective transaction which may be linked to ML/FT through:

(a) information provided by a subject person;
(b) information provided by a foreign FIU; or
(c) any other information in its possession.

Where the FIAU considers it necessary to oppose the execution of a suspicious transaction, a notification of such opposition is to be made to the subject person concerned by any written means. In those cases where the FIAU opposes the execution of the transaction following the receipt of information from a subject person, the notification of opposition shall be made to the subject person by not later than one (1) working day following the day on which the information was received by the FIAU.

Within this one (1) working day, the subject person is prohibited from carrying out the transaction in question. If after the passage of one (1) working day following notification to the FIAU the subject person has not received notification from the FIAU to suspend the same transaction, the subject person can proceed with executing the transaction.

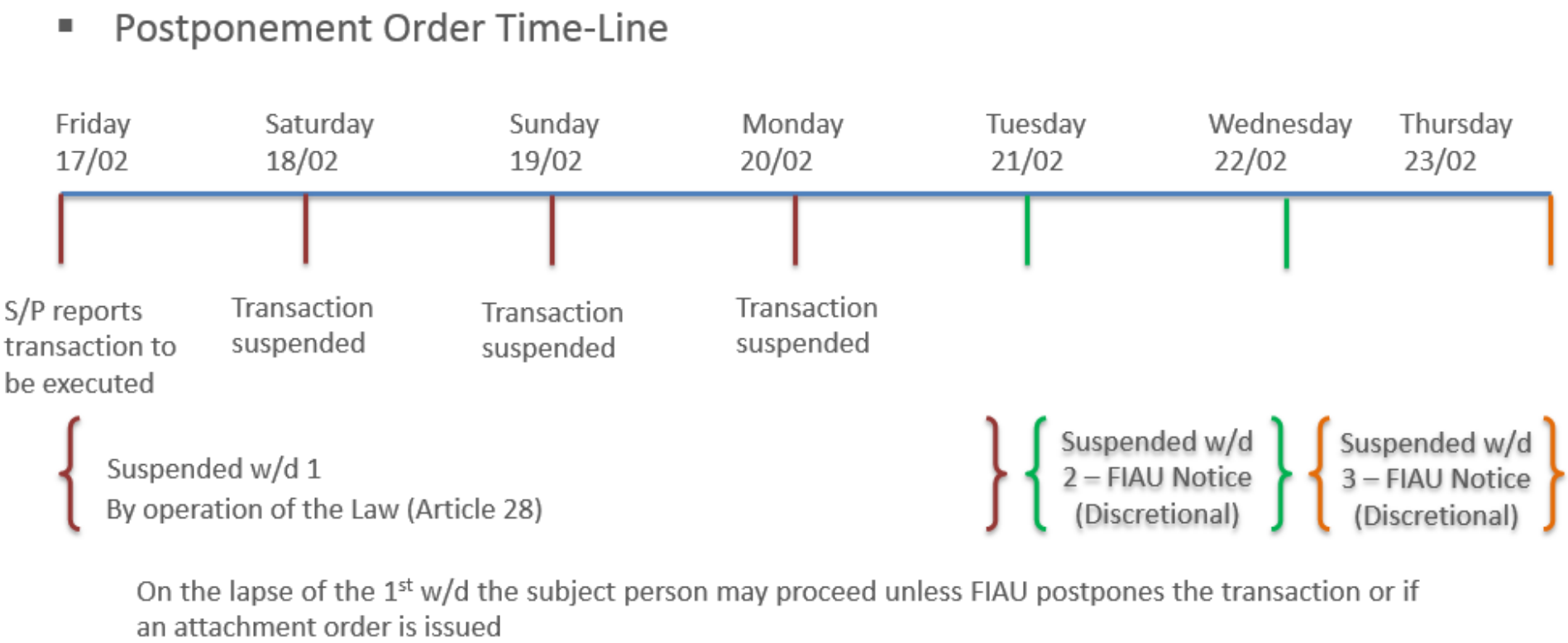
Where the FIAU suspends the execution of the transaction, the suspension shall last for a period of one (1) working day, following the day of notification of the opposition by the FIAU. The FIAU may however authorise the execution of the transaction before the expiration of this period, by any written means.

In terms of Article 28(3) of the PMLA, the FIAU may, if it considers it necessary, extend the period of suspension by a further one (1) working day. Where the FIAU decides to extend the period of suspension it should notify the subject person in writing before the previous one (1) working day suspension period expires. In practice, therefore, in terms of Article 28, a transaction may be delayed by a maximum of three (3) working days, following the day the subject person notifies the FIAU. The diagram hereunder provides a time line of a postponement order's issue and application.

Subject persons may only proceed with the execution of a transaction which has been opposed by the FIAU once the respective suspension period expires. This obligation not to execute a

transaction opposed by the FIAU prevails over any legal or contractual obligation to which the subject person might be subject.

Figure 6 - Postponement Order Time-Line



Subject persons should also be aware that an attachment order issued by the competent court may be served on the subject person while a transaction is suspended by the FIAU. In such cases the subject person would be bound by the attachment order and thus would not be able to execute the transaction even after the expiry of the suspension period in terms of Article 28 of the PMLA.

Where the FIAU does not oppose the execution of a transaction reported by a subject person or the respective suspension period lapses without there being any other legal impediment to the execution of the transaction, it is left to the discretion of the subject person whether to proceed or otherwise with the execution of the said transaction and article 28 does not require the FIAU to authorise the execution of the transaction in question.

5.9 Monitoring Orders

In terms of Article 30B of the PMLA, the FIAU may demand that a subject person monitors transactions or banking operations suspected of being related to ML/FT. Such power may be exercised by the FIAU when it:

(a) receives a STR; or
(b) when from information in its possession the FIAU suspects that:
- any subject persons may have been used for any transactions suspected to involve ML/FT; or
- property is being held by a subject person that may have derived directly or indirectly from, or constitutes the proceeds of, criminal activity or from an act or acts of participation in criminal activity.

A monitoring order can only be made for a specified period of time. Throughout its duration the subject person is required to monitor the transactions or, in the case of banks, banking operations:

(a) carried out through one or more accounts in the name of any natural or legal person suspected of a ML/FT offence; or
(b) carried out through one or more accounts suspected to have been used in the commission of a ML/FT offence; or
(c) which could provide information about a ML/FT offence or the circumstances thereof.

The FIAU may issue such a monitoring order before, during or after the commission of the ML/FT offence referred to above. Subject persons are required to communicate to the FIAU the information resulting from the monitoring and the FIAU may use that information for the purpose of carrying out its analysis and reporting functions.

5.10 Professional Privilege

By virtue of Regulation 15(9), auditors, accountants, tax advisors, notaries and members of the legal profession are exempt from the duty to report suspicious transactions to the FIAU in accordance with the provisions of Regulation 15(3) and the duty to inform the FIAU prior to

carrying out a transaction that is known or suspected to be related to ML/FT in accordance with Regulation 15(4), if such information is received or obtained in the course of ascertaining the legal position for their client or performing their responsibility of defending or representing that client in, or concerning judicial proceedings, including advice on instituting or avoiding proceedings, whether such information is received or obtained before, during or after such proceedings.

This principle was upheld in a judgement by the European Court of Justice in ***Ordre des barreaux francophones and germanophones & Others vs Conseil des Ministres C-305/05, (ECJ Grand Chamber) 26th June 2007***. The court held the following:

"The reporting obligations apply to lawyers only insofar as they advise a client in the preparation or execution of certain transactions – essentially those of a financial nature or concerning real estate – or when they act on behalf of and for a client in any financial or real estate transaction. As a rule, the nature of such activities is such that they generally take place in a context with no link to judicial proceedings and consequently, those activities fall outside the scope of the right to a fair trial. Moreover, as soon as lawyers acting in connection with a financial or real estate transaction are called upon for assistance in defending a client or in representing such a client before the courts, or for advice as to the manner of instituting or avoiding judicial proceedings, those lawyers are exempt from the reporting obligations, regardless of whether the information has been received or obtained before, during or after the proceedings. An exemption of that kind safeguards the right of the client to a fair trial".

Although the judgement only related to lawyers, Regulation 15(9) extends the same principle to other legal professions, notaries, auditors, accountants and tax advisors. This principle ensures that the trust placed by the client in the professional is not breached when these professionals are called upon to ascertain the legal position of a client, to defend a client or represent such a client before the courts, or for advice as to the manner of instituting or avoiding judicial proceedings.

Moreover, where the subject persons mentioned in this section are seeking to dissuade a client from engaging in an illegal activity, they shall not be in breach of their confidentiality obligations and any such disclosure shall not constitute tipping off.[80] Nevertheless, in any other circumstances where the professional privilege referred to under this section does not apply, the professional is under an obligation to file a STR with the FIAU ensuring also that all non-disclosure obligations under the PMLFTR and these Implementing Procedures are adhered to.

5.11 Prohibited and Permissible Disclosures

Regulation 16(1) prohibits a subject person, as well as any official or employee of a subject person, from disclosing to the person concerned or to a third party that:

(a) a STR has been made to the FIAU;
(b) the FIAU demanded information within the context of an ML/FT analysis;

[80] Regulation 16(3) of the PMLFTR.

(c) information has been or may be transmitted to the FIAU within the context of an ML/FT analysis; and
(d) a ML/FT analysis or investigation has been, is being carried out, or may be carried out by the FIAU or by a law enforcement agency respectively.

The term 'third party' includes any person who does not constitute part of the subject person and is thus considered to be an external person to the subject person. This would include any person to whom the subject person may have outsourced any of its functions, processes etc.

Although this prohibition does not extend to the disclosure of the above defined information within the subject person, it is recommended that subject persons adopt a careful stance when circulating such information internally to avoid risks of leakages and disclosures, which would place subject persons in breach of Regulation 16(1).

Breach of the above constitutes a criminal offence termed as "tipping-off" and, given the potential prejudice that any disclosure of the above mentioned information may have on an analysis or investigation, it arises even though no prejudice may actually result or the person disclosing the information did not know or suspect that the disclosure was likely to prejudice the analysis or investigation. Therefore, for this offence to subsist it is sufficient that the disclosure is made, irrespective of the effect that such disclosure has or is likely to have. The punishments applicable for the offence of tipping off are laid out in more detail in Section 8.3.6.

A subject person must, however, still retain the necessary contact with a customer and should enquire, in a tactful manner, regarding the background to one or more transactions or to activity that appears to be inconsistent with the normal pattern of activity of the customer, or in adverse media coverage that the subject person may have become aware of. This is prudent practice and forms an integral part of CDD measures. Such enquiries would not in themselves give rise to tipping off.

Although the PMLFTR outline the prohibition of disclosure for subject persons, there are certain circumstances established by the PMLFTR where disclosures made will not constitute an offence in terms of the PMLFTR.[81] Such circumstances include disclosures:

(a) to the supervisory authority relevant to that subject person or to law enforcement agencies in accordance with applicable law;

(b) between a subject person and another person who:
  (1) undertakes activities equivalent to relevant financial business;
  (2) is situated in a Member State or third country; and
  (3) forms part of the same group of companies and applies group-wide policies and procedures as provided for in Regulation 6;

(c) between a subject person who undertakes activities under paragraphs (a) or (c) of the definition of 'relevant activity' in terms of Regulation 2 of the PMLFTR and another person who:

[81] Regulation 16(2) of the PMLFTR.

(1) undertakes equivalent activities in a Member State or a third country imposing requirements similar to those laid down in the PMLFTR; and
(2) performs his professional activities, whether as employee or not within the same legal person or within a larger structure to which the subject person belongs and which shares common ownership, management or compliance control;

(d) between a subject person who undertakes relevant financial business or activities under paragraphs (a) or (c) of the definition of 'relevant activity' in terms of Regulation 2 of the PMLFTR and another person:
(1) from the same professional category situated in a Member State or a third country imposing requirements similar to those laid down in the PMLFTR; and
(2) in cases related to the same customer and the same transaction; and
(3) where such persons are subject to obligations of professional secrecy and personal data protection.

(e) disclosures by a subject person to a competent court, tribunal or other judicial authority in or outside Malta in the course of proceedings instituted against the subject person for or as a consequence of the failure or the delay in carrying out a transaction including disclosures made in any written pleadings or submissions.

Such disclosures would be permissible and would not constitute a breach of Regulation 16(1) of the PMLFTR only if all of the following conditions are met:
(1) the disclosure is made after the lapse of the one (1) working day period of suspension as stipulated in Article 28(1) of the PMLA; and
(2) where applicable, the disclosure is made after the lapse of any period of time during which the execution of the transaction is opposed by the FIAU in terms of Article 28 of the PMLA.

(f) disclosures by a subject person to a supervisory authority or professional body exercising supervision or regulatory oversight over the subject person making the disclosure, that the subject person delayed from carrying out a transaction in terms of Article 28(1) of the PMLA.

Such a disclosure would be permissible and would not constitute a breach of Regulation 16(1) of the PMLFTR only if all of the following conditions are met:
(1) the disclosure is made on the lapse of the one (1) working day period of suspension as stipulated in Article 28(1) of the PMLA has expired;
(2) where applicable, the disclosure is made after the lapse of any period of time during which the execution of the transaction is opposed by the FIAU in terms of Article 28 of the PMLA.

Subject persons forming part of a group have to bear in mind the obligations arising from Regulation 6 of the PMLFTR on the application of group-wide policies. These group policies are to include policies and procedures on data protection and the sharing of information within the said group, even where the subsidiaries or branches are established outside the EEA. This would include policies and procedures regulating the sharing of information to reflect Regulation 16 of

the PMLFTR. Where the laws of a third country do not allow a subsidiary or a branch to adhere to the group policies and procedures, including relative to sharing of information, the subject person is expected not to share information with the said subsidiaries and branches and refer the matter to the FIAU as provided for under Regulation 6(4) of the PMLFTR.

Furthermore, any *bona fide* communication or disclosure made by a subject person or by an employee or director of such subject person, in fulfilment of any requirement envisaged under the PMLFTR, does not constitute a breach of the duty of professional secrecy, or any other restriction (whether imposed by statute or otherwise) and such person will not be subject to liability of any kind.[82]

5.12 Reports for Compliance Purposes

Article 16(1)(c) of the PMLA charges the FIAU with the responsibility of monitoring compliance with AML/CFT obligations by subject persons. This responsibility is further elaborated under Article 26 of the PMLA which empowers the FIAU to carry out this responsibility on a risk- sensitive basis. To be able to do so, the FIAU has to collect data, information or documentation from subject persons. Regulation 19 of the PMLFTR empowers the FIAU to require from subject persons periodical reports on the internal policies and procedures they maintain and apply, as well as any other information the FIAU deems necessary for the fulfilment of its supervisory functions.

On the basis of the information gathered from these reports, the FIAU can get a clear picture of **where** is the risk, **what** is the risk and **how** best to manage that risk. These reports assist the FIAU in fulfilling another essential function, which is the compilation of statistics and records in order to coherently plan its compliance reviews as well as gauge the effectiveness of the AML/CFT regime in Malta. This function emanates from Article 16(1)(g) of the PMLA and is reflected in Regulation 14(2) of the PMLFTR.

Reports required from subject persons may take the form of a questionnaire having both closed-ended and open-ended questions. They will usually require the completion of general details on the subject persons, as well as other information which may, *inter alia*, include:

(a) Information and data relating to the risk exposure of the subject person;
(b) Information and data relating to the AML/CFT preventive and mitigating measures adopted by the subject person to tackle the identified risk exposure;
(c) Statistical data in relation to the subject person's business.

Whenever the FIAU requests subject persons to compile and transmit a report, the FIAU will provide subject persons specific instructions and details on the procedure to follow, including:

(a) instructions on how the report is to be compiled;
(b) instructions on how and in what manner the report is to be transmitted to the FIAU;
(c) the time-frames/deadlines within which such report is to be submitted to the FIAU;

[82] Regulation 15(10) of the PMLFTR.

(d) any applicable administrative fees (including late submission fees if and where applicable) in relation to the submission of the compliance report; and
(e) appropriate intimation notice/s warning subject persons of the consequences for non-observance with the instructions and information provided in the Explanatory Note.

5.13 Reporting under Regulation (EU) 2015/847

Subject persons who are payment service providers have additional reporting obligations in terms of the Regulation (EU) 2015/847. The said Regulation obliges payment service providers who are acting either as a payee's payment service provider or as an intermediary payment service provider to notify to the FIAU about payment service providers who repeatedly fail to accompany transfer of funds with the information required in terms of the said Regulation.

This reporting obligation is explained in more detail in the Guidance Note issued by the FIAU and entitled *Guidance Note on Information Accompanying Fund Transfers*. Any reporting under this section should be done using the form attached to the said Guidance Note which is to be submitted electronically on the following email address – compliance@fiumalta.org. Reporting should take place without undue delay, and no later than three months after identifying the repeatedly failing payment service provider.

5.14 The Protection of the Whistleblower Act

The FIAU has been designated as one of the authorities which in terms of the Protection of the Whistleblower Act[83] is to receive external disclosures of improper practices from the private sector. In the case of the FIAU, the external disclosures must relate to improper practices linked to the PMLA or the PMLFTR. These may include disclosures relative to actions:

(a) whereby a person has failed, is failing or is likely to fail to comply with any AML/CFT obligation arising from the PMLA, the PMLFTR, the FIAU Implementing Procedures and any other binding procedures issued by the FIAU; or

(b) which are tantamount to a money laundering or funding of terrorism offence whether this has been committed, is being committed or is likely to be committed.

Employees who makes any such disclosure are afforded the protection of the law against any discriminatory action that the employer may take against him. It should be noted that the identity of the employee making the external disclosure is protected and can only be disclosed in exceptional circumstances where that is necessary to take action on the external disclosure and only if the person's prior consent thereto is obtained. Any employee can make an external disclosure, including employees of subject persons.

However, it is important to note that:

[83] Cap 527 of the Laws of Malta.

(a) Employees making a disclosure will only be able to benefit from the safeguards provided by the Protection of the Whistleblowing Act if the said disclosure is made in good faith without any expectations of a personal gain and reasonably believing that the information provided is true; and

(b) An external disclosure may be received by the FIAU only once the improper practice has been reported through any internal whistleblowing procedures maintained by the employer, and no action was taken by the employer to redress the same. Where determinate conditions subsist, the employee may proceed with disclosing the improper practice externally to the FIAU even without attempting to make an internal disclosure. This is only possible where the employee has reasonable grounds to believe that:

i. The head of the organisation is or may be involved in the improper practice; or
ii. Immediate reference to the FIAU is justified by the urgency of the matter to which the disclosure relates or some other exceptional circumstance; or
iii. At the time he makes the disclosure, he will be subjected to occupational detriment if he makes an internal disclosure; or
iv. It is likely that evidence relating to the improper practice will be concealed or destroyed if he makes an internal disclosure.

In the case of subject persons' employees, prior to making an internal disclosure in terms of the Protection of the Whistleblower Act they should consider whether the information they are seeking to disclose should be reported internally to the MLRO by making use of the internal reporting procedures maintained by the subject person for the reporting of knowledge or suspicion of ML/FT.

External disclosures should ideally be submitted to the FIAU in writing and marked as strictly confidential. Submissions may be sent either via email on whistleblowing@fiumalta.org or in writing addressed to the FIAU's Whistleblowing Reports Unit. Upon receipt of an external disclosure, the Whistleblowing Reports Unit will carry out a first review of the report to determine whether:

(a) All the conditions for an external disclosure to be made are met. The said Unit is allowed forty-five (45) days from receipt of the external disclosure within which to make the said determination and inform the employee as to its conclusions. Where the Whistleblowing Reports Unit concludes that an internal disclosure should have been filed, it will desist from considering any further the alleged improper practice and will direct the employee to disclose the improper practice internally.

(b) Another authority referred to under the Protection of the Whistleblower Act or the Malta Police would be better placed to investigate the alleged improper practice disclosed by the employee. Where it so concludes, the Whistleblowing Reports Unit will transmit the relevant information to the said authority or to the police, and notify the employee in

writing of the action taken. This has to be done within thirty (30) days from receipt of the external disclosure. At no point will the employee's identity be disclosed and he will still be entitled to the protection offered by the Protection of the Whistleblower Act.

Any external disclosures that are deemed by the Whistleblowing Reports Unit to fall within its remit will be thoroughly investigated to determine whether there is any *prima facie* evidence of wrongdoing. To this end the Whistleblowing Reports Unit may request the employee to attend for meetings, request any witnesses indicated in the external disclosure to give statements, collect additional information on the organisation or individuals involved in the alleged improper practice and carry out any other checks that it may deem necessary.

Information disclosed to the Whistleblowing Reports Unit may be shared with other sections of the FIAU when such other sections request information in the course of conducting their own functions. Any information shared will not include any details as to the employee's identity.

The employee will be duly informed of the investigation's outcome and of any action taken where this may be warranted. Given the potential different nature of the improper practices that may be disclosed to it, the Whistleblowing Reports Unit is not in a position to set a determinate timeframe within which it will conclude its investigation. However, it will strive to do so within a reasonable time.

Action may include forwarding the information received to other sections within the FIAU for further analysis or action or, where the improper practice is considered to amount to a crime or contravention, referring the matter to the Malta Police. Any information so forwarded will not include any details as to the employee's identity.

An employee may opt to make an anonymous disclosure. While the Reports Unit will take into consideration even such disclosures, employees that make anonymous disclosure do not benefit from the protection provided for in the Protection of the Whistleblower Act.

CHAPTER 6 – OUTSOURCING

6.1 What is to be considered as Outsourcing?

Outsourcing is the engagement of a third party by a subject person to carry out an activity, process or service that would normally be carried out by the subject person itself. Outsourcing therefore means that the subject person would not implement certain measures and procedures itself but would delegate these to another person. For the avoidance of doubt the acquisition of software or access to commercial databases to assist in, or facilitate, the carrying out of AML/CFT obligations without any data or information belonging to the subject person being submitted to and processed by a third party is not to be considered as outsourcing.

Outsourcing is to be distinguished from the possibility allowed to subject persons to exercise reliance on the CDD measures carried out by another subject person in terms of Regulation 12 of the PMLFTR. In case of reliance, the subject person would typically rely upon another subject person or a third party who would have carried out CDD to meet its own AML/CFT obligations and the subject person or third party being relied upon grants the subject person placing reliance access to the information and documentation so collected. No reliance can be made in so far as risk assessment and ongoing monitoring obligations are concerned.

The situation in the case of outsourcing differs from the reliance arrangement in that rather than relying on the CDD measures undertaken by another subject person or third party, the subject person is delegating the implementation of certain AML/CFT obligations to another person(s). The below sections set out the requirements which are to be applied when a subject person outsources certain AML/CFT obligations to another person.

To the extent allowed by law, subject persons may also be able to appoint agents in order to extend their network to carry out their activities. This is not to be considered as outsourcing as the agent is deemed to form part of the subject person itself and has to abide by the controls, policies, measures and procedures established by the subject person.

6.2 Responsibility of the Subject Person

The PMLFTR are very clear in setting out what the general obligations of subject persons are when it comes to preventing ML/FT; it is the subject person's responsibility to ensure that it is at all times abiding by these obligations. Responsibility can never be delegated and as a consequence:

(a) Outsourcing is not to be extended to the adoption and application of policies and procedures necessary to ensure the subject person is at all times compliant with its AML/CFT obligations. While it is permissible for a subject person to engage consultants to assist it in carrying out any risk assessment or drawing up any policies and procedures, it is the subject person's ultimate responsibility that these address the ML/FT risks to which it is exposed, satisfy the requirements at law, and are implemented properly;

(b) The subject person must effectively monitor how the service provider is carrying out the outsourced AML/CFT measures and procedures to ensure that these are being carried out as required by law and in accordance with the subject person's own policies and procedures. By way of example, this can be done through periodical reports provided by the person to whom a function has been outsourced to the subject person, spot checks, and requests for CDD information on particular clients. Subject persons may implement other measures in order to ensure effective supervision;

(c) The subject person must ensure that it has a contingency plan in the eventuality of a sudden termination of the outsourcing arrangement which would ensure that it can resume without undue delay the implementation of the outsourced AML/CFT obligations.

The FIAU will at all times consider the subject person as responsible for compliance with its AML/CFT obligations.

6.3 Extent of Outsourcing

Outsourcing is to be allowed only in so far as the implementation of a subject person's policies and procedures are concerned. A subject person may, therefore, outsource certain AML/CFT obligations to another person. The obligations which may be outsourced, whether in whole or in part, relate to:

(i) the implementation of risk assessments procedures (Regulation 5 of the PMLFTR);
(ii) the implementation of CDD procedures (Regulation 7 to Regulation 11 of the PMLFTR);
(iii) the implementation of record keeping obligations (Regulation 13 of the PMLFTR).

(collectively referred to as the "**General Outsourced Activities**").

The subject person will at all times remain responsible for all other obligations in terms of the PMLFTR and these Implementing Procedures, including, without limitation, the acceptance or otherwise of a customer, the termination of a business relationship, the undertaking of an occasional transaction etc.

Unless otherwise specified in these Implementing Procedures or in any *ad hoc guidance* (such as set out in Section 5.1.2 of these Implementing Procedures) outsourcing does not extend to the appointment of the MLRO and of the officer in charge of the monitoring function referred to in Section 5.3. This means that these two functions cannot be outsourced to third parties as they have to carried out at all times by an officer or employee of the subject person who meets the conditions set out in Chapter 5 of Part I of the Implementing Procedures. The person/s assuming these functions is/are to continue to exercise the functions assigned to him /them under the said Chapter and is/are to be responsible for monitoring the activities of the third party.

In addition, unless otherwise specified in these Implementing Procedures or in *ad hoc guidance,* the outsourcing of the General Outsourced Activities does not extend to the determination as to whether a STR is to be filed with the FIAU. This is to remain within the discretion of the MLRO of the subject person and the subject person must ensure (through its internal reporting procedures) that even the third party (to whom certain functions are outsourced) can submit reports to the MLRO, for the MLRO to assess whether an STR should be filed with the FIAU. Nevertheless, a subject person may still outsource a third party to flag unusual transactions that may become the subject of an internal report to the MLRO or engage consultants to assist in the determination of whether a STR is to be filed or otherwise, in full respect of any non-disclosure obligations binding the subject person and in line with conditions set out in Section 5.4 above.

6.4 Conditions to which Outsourcing is subject

Given the risks to which the subject person may be exposed in situations where the outsourced third party fails to effectively carry out the outsourced function, the FIAU considers that outsourcing is not to be unconditional but that there must be specific requirements which must be met for outsourcing to be permissible. To this end, whenever a subject person is outsourcing the General Outsourced Activities the subject person must ensure that they are complying with the requirements set out in this section.

In this regard, prior to outsourcing the General Outsourced Activities to a third party, the subject person should:

(i) make an assessment of any potential ML/FT risk due to the proposed outsourcing,
(ii) maintain a written record of the assessment, and
(iii) monitor the perceived risk.

In order to ensure that proper arrangements are in place and in order to make sure that the outsourced entity has the necessary competence and resources to be able to undertake the General Outsourced Activities in an appropriate manner, the subject person is required to ensure that all of the following conditions are met:

(a) The outsourcing does not negatively prejudice the ability of the subject person to comply with its obligations at law and the effectiveness of the subject person's compliance and audit functions, nor will the outsourcing impede the effective supervision of the subject person by the FIAU or the compliance by the subject person with any obligation related to the analytical function of the FIAU;
(b) The third party has the necessary resources, qualifications, skills and authorisations (if required) at its disposal to effectively carry out the measures and procedures it is to perform on behalf of the subject person;
(c) The manner in which the third party proposes to implement the General Outsourced Activities on behalf of a subject person is in line with all applicable legal requirements and the subject person's own policies and procedures;
(d) The third party is in good standing, there being no adverse information in its regard, and it is located and operating from Malta, an EU Member State or another reputable jurisdiction; and

(e) The third party is not subject to any obligation which would lead to a breach of any data protection, professional secrecy, confidentiality or non-disclosure obligation to which the subject person has to adhere.

The subject person shall maintain a copy of the assessment undertaken prior to entering into an outsourcing arrangement and shall make it available to the FIAU upon request.

The outsourcing of the General Outsourced Activities to a third party must be regulated by a written agreement which clearly sets out:

(a) the exact parameters of the measure or procedure being outsourced to the third party;
(b) the precise requirements concerning the performance of the measure or procedure, taking account of the intended objective of the measure or procedure to be outsourced;
(c) the respective rights and obligations of the parties to the agreement , including:

- the obligation of the third party to immediately notify the subject person of any change in its circumstances which negatively affect its standing or its ability to meet its obligations under the agreement;
- the right of the subject person to monitor the third party's performance and the obligation of the third party to take such corrective measures as may be required by the subject person to ensure that the measure or procedure being outsourced is carried out effectively;
- unrestricted and immediate access at any time by the subject person to any data, documentation, information, reports or findings obtained subsequently to the implementation of the measure or procedure outsourced, including the ability to access and retrieve data, information and documentation for the purposes of submitting STRs or replying to requests for information from the FIAU, law enforcement and any other relevant supervisory authority without having to disclose the purpose why the said data, information or documentation is being accessed; and
- where the retention of data, information and documents collected in the course of implementing the outsourced measures or procedures also forms part of the outsourcing agreement, the segregation of said data, information and documents from that belonging to the third party or any other customer thereof.

(d) the circumstances under which the agreement can be terminated and the terms that would become applicable, including:

- a termination clause allowing either the proper and orderly transfer of the outsourced measure or procedure to another third party identified by the subject person or the proper and orderly reintegration of the said measure or procedure within the subject person, with the third party continuing to carry out the outsourced measure or procedure until such time as the transfer is complete;
- the possibility for the subject person to terminate the agreement where the FIAU so requires and where the third party is no longer in a position to meet its obligations under the agreement.

(e) the ownership of any data, information, reports or other documentation that may be produced, collated or collected in the course of carrying out the measure or procedure being outsourced, taking into consideration the record-keeping obligations of the subject person;

(f) that any processing of personal data has to take place in accordance with applicable data protection laws and any data, information, reports or other documentation are kept confidential and will not be disclosed to anyone other than in those circumstances where the law permits such disclosure;

(g) the communication lines to be followed, especially with regard to the transmission of data, information, documentation, reports or findings to the subject person by the third party related to the measures or procedures outsourced;

(h) that the third party is to allow the FIAU, including anyone duly authorised to act on its behalf, direct access to its premises and to any data, information, documentation reports or finding relative to the outsourced measures or procedures as may be required by the FIAU;

(i) the fact that sub-contracting by the third party is not to be allowed without the prior agreement of the subject person, which consent can only be granted once the subject person has ascertained that the sub-contractor meets the conditions set out in this section and that the sub-contracting will not impact negatively the arrangement entered into between the subject person and the third party;

(j) the subject person must regularly evaluate the performance of the third party using mechanisms such as service delivery reports, self-certification, independent reviews or the subject person's own audit function.

Subject persons are to note that the above does not exempt subject persons from any additional regulatory requirements to which they may be subject.

6.5 Outsourcing within a Group Context

Where the subject person forms part of a group of companies and it contemplates outsourcing the General Outsourced Activities to another group entity, the subject person will still have to ensure that the conditions set out herein are met.

CHAPTER 7 – AWARENESS, TRAINING AND VETTING OF EMPLOYEES

7.1 Awareness and training: the obligation and purpose behind it

Every subject person is required to take appropriate and proportionate measures from time to time to:

- ensure that employees are aware of relevant AML/CFT legislation and data protection requirements, as well as of the subject person's AML/CFT measures, policies, controls and procedures; and
- provide training in relation to the recognition and handling of operations and transactions which may be related to proceeds of criminal activity, money laundering or the funding of terrorism.[84]

The emphasis in the PMLFTR is on the words "appropriate" and "proportionate": therefore there is no place for a 'one size fits all' or a haphazard approach towards training. Training needs to be well thought out and planned, targeted, but also proportionate depending on the nature of the subject person's activities, the risks it is exposed to, as well as the size of the subject person's business or operation.

The PMLFTR also emphasises that such measures need to be taken from time to time, meaning that such training and awareness raising initiatives are taken on a regular basis. A subject person should set its training programme, including the content and frequency of any training or awareness raising sessions, on the basis of the risks identified through the subject person's business risk assessment, the specific roles of the employees being trained, and any relevant developments including legislative changes, development of new products or services, new markets targeted by the subject person etc. In all cases, new employees should be made aware of their responsibilities and those of the subject person upon their employment or engagement.

Awareness of the AML/CFT procedures of the subject person and training in relation to identification of unusual activities or suspicious transactions are key elements in the detection and deterrence of ML/FT activities. It is therefore critical that every subject person allocates adequate resources to train its employees. Even though a subject person may have the best designed AML/CFT policies and procedures, the effectiveness of these procedures ultimately depends on its employees being fully aware of them and sufficiently knowledgeable to implement them. The content and effectiveness of the training provided will therefore be critical to the success or failure of a subject person's AML-CFT strategy. Proper training to staff, so as to ensure that they are fully alert to the very risks of money laundering and the funding of terrorism and in the identification of unusual transactions and to riskier situations that may turn out to be suspicious, is critical to the success and effectiveness of a subject person's efforts at combatting ML/FT.

In terms of applicable law, individual members of staff (and particularly directors or similar officers responsible for the management of a body or association of persons,[85] as well as

[84] Regulation 5(5)(b) and (e) of the PMLFTR.
[85] Regulation 21(7) of the PMLFTR.

employees in certain instances[86]) may actually face administrative sanctions for contraventions of AML/CFT obligations or lawful requirements, orders or directives issued by the FIAU committed by the body or association of persons, or criminal penalties if they are involved in money laundering or the funding of terrorism, or if they breach their non-disclosure obligations under the PMLFTR. It is important, therefore, that staff is made aware of these obligations, and are given appropriate training.

It should also be borne in mind that Regulation 5(5)(c) of the PMLFTR obliges subject persons to "***appoint, where appropriate with regard to the nature and size of the business, an officer at management level whose duties shall include the monitoring of the day-to-day implementation of the measures, policies, controls and procedures adopted under this regulation***" which also includes the implementation of a training programme.

7.2 Employees to be Provided with Training

It should be noted that awareness and training should be provided to employees whose duties include the handling of either relevant financial business or relevant activity[87], irrespective of their level of seniority. This includes:

(a) directors,
(b) senior management,
(c) the MLRO and designated employee(s),
(d) compliance staff; and
(e) All members of staff involved in the activities of the subject person which fall within the definition of relevant financial business and relevant activity.

It is important to emphasise that when referring to employees in an AML/CFT context, the term should not be interpreted in a restrictive manner, meaning that it should not only refer to individuals who have a contract of employment with the subject person in the strict legal sense of the term, but should be interpreted so as to also include individuals who are engaged by the subject person to carry out aspects of its business involving relevant activity or relevant financial business (such as temporary or contract staff).

The training should be relevant to the specific responsibilities and functions of the respective employees within that subject person. Thus it is expected that front-office employees, for instance, would be provided with training that is different from that required by back-office employees. Effective training measures should ideally make reference to real-life scenarios that are or will be encountered by the employees, such as, for instance, the steps to be followed when on-boarding customers, the handling of high-risk customers and the behaviour to be adopted when faced with transactions that appear to be suspicious.

In order to be in a position to recognise and handle suspicious transactions, employees should be trained on how the products and services of the subject person may be misused for ML/FT purposes. Of relevance to this is strong awareness of ML/FT typologies and of red flags and risk

[86] Regulation 16(1) of the PMLFTR.
[87] Regulation 5(7) of the PMLFTR.

indicators applicable to the particular subject person. Knowledge on relevant typologies plays an important role in the recognition of ML/FT, and employees should be kept aware of the ever-changing behaviour and practises used by money launderers and terrorists. Similarly, employees should be provided with a relevant list of red flags and risk indicators, as these are a useful tool towards recognizing possible ML/FT activity.

Employees located outside Malta

Where activities relating to the operations of a Maltese subject person are undertaken by staff outside Malta, those employees must be made aware of and trained to follow the AML/CFT policies and procedures applicable to the Maltese operations. Where relevant, there may also be certain local training and awareness obligations in the host state that may also need to be met.

7.3 Content of Training

Through training measures, the subject person should seek to ensure that relevant employees are knowledgeable of the subject person's:

(a) Customer due diligence measures;
(b) Record-keeping procedures;
(c) Internal reporting procedures;
(d) The role of the MLRO in filing STRs with the FIAU (external reporting);
(e) Risk management measures, including:
    - Customer acceptance policies;
    - Customer risk assessment procedures;
    - Internal controls;
    - Compliance management;
    - Communications;
    - Employee screening policies and procedures;
    - Any other relevant policies and procedures concerning AML/CFT
(f) The ML/FT risks posed by the business and/or activities of the subject person (i.e. the outcomes of its business risk assessment).

All employees should know who their MLRO, any designated employee(s) and the officer carrying out the monitoring function referred to in Section 5 are, as well as the functions and responsibilities of these key persons.

Employees should also be made aware of the following legislative instruments and other binding guidance:

(a) The provisions of the PMLA;
(b) The provisions of the PMLFTR;
(c) The provisions of the Criminal Code concerning the funding of terrorism;
(d) Relevant data protection laws, rules and guidance;
(e) The FIAU Implementing Procedures, other guidance and/or interpretative notes issued by the FIAU; and

(f) The applicable offences and penalties resulting from breaches of all of the above.

Furthermore, employees should be made aware of the potential effect of any breach of applicable law and regulations on the subject person, the employees personally and the customers of the subject person.

The lists provided for under this Section are not exhaustive, and any policies and procedures related to AML/CFT implemented by the subject person would need to be incorporated into the training measures. Moreover, all policies and procedures should be made readily available to all employees to enable them to refer to such information whenever required.

7.4 Method of delivery of training

The FIAU does not seek to impose any particular methods of training and hence subject persons may determine what would work best in accordance with the size and nature of their activities and taking into consideration training methods used for other aspects of their operations. Training may, for instance, be comprised of a mix of online learning systems with focused classroom training for higher risk activities, video and other digital media, external training, procedures manuals or any other medium that is able to deliver effective training.

Regardless of the medium used, any training provided should ideally include or be supplemented with material that employees may refer to from time to time as may be necessary in the course of carrying out their duties.

Furthermore, subject persons are to maintain records of the training provided in order to monitor which employees have received training, how frequently, and the nature of training provided. In line with record keeping requirements, training records are to include:

a) The date on which training was delivered;
b) The nature of the training;
c) The names of the employees who received training; and
d) A copy of any training materials provided.

7.5 Screening of new employees

Subject persons shall have in place appropriate procedures for due diligence when hiring employees who would be handling relevant financial business or relevant activity for the subject person, which is to include obtaining a Police conduct certificate or equivalent documentation [88]. Such screening should allow subject persons to assess the conduct and integrity of the individual. It is also relevant to note that various laws, regulations and guidelines applicable to regulated entities require the licensee to employ staff that is 'fit and proper' and in possession of the necessary skills and expertise, knowledge and experience, sufficient to enable them to discharge

[88] Regulation 5(5)(a)(ii) of the PMLFTR

the obligations entrusted to them. This should also be borne in mind by all subject persons whenever engaging employees to handle relevant financial business or relevant activity, especially when engaging a MLRO, designated employee or an on officer to carry out the monitoring function referred to in Chapter 5 above.

Screening of individuals should be carried out prior to their engagement or, if they are already employed with the subject person, whenever they are entrusted with new roles or responsibilities concerning relevant duties. Moreover, screening must be an ongoing process and thus subject persons should ensure that they carry out employee screening from time to time.

Finally, subject persons must take into consideration the relevant provisions concerning the retention of records, which includes personal data, and which are outlined in more detail under Chapter 9 of these Implementing Procedures Part I.

CHAPTER 8 – JURISDICTIONS, GROUPS AND PENALTIES

8.1 Non-Reputable Third Countries

A number of obligations under the PMLFTR require subject persons to assess the level of ML/FT risk emanating from a particular jurisdiction and to determine whether a jurisdiction is deemed to be a non-reputable one as defined under Regulation 2(1) of the PMLFTR. This section is intended to assist subject persons in the application of these obligations in the light of the Financial Action Task Force (FATF) public documents on high-risk and non-cooperative jurisdictions as well as the EU legal acts identifying high risk third countries.

The FATF Public Documents

The FATF issues two public documents which provide a list of jurisdictions that are considered to pose a higher risk of ML/FT in view of a number of identified strategic deficiencies within their AML/CFT regime. The ML/FT risks posed by the jurisdictions listed in the FATF documents vary depending on the seriousness of the deficiencies and the level of commitment made by each jurisdiction to address those deficiencies. It is to be noted that the FATF documents are issued three times a year and as a result the list changes depending on the level of progress achieved (or the lack of) by each jurisdiction in addressing the deficiencies identified in their respect.[89]

The first public document issued by the FATF is the **Public Statement** which classifies jurisdictions into the following two categories:

(a) jurisdictions subject to a FATF call on its members and other jurisdictions to apply counter-measures to protect the international financial system from the ongoing and substantial ML/FT risks emanating from the jurisdictions;

(b) jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies and are subject to a FATF call on its members to consider the risks arising from the deficiencies associated with each jurisdiction.

The FATF also issues a second document entitled "***Improving Global AML/CFT Compliance: On-going Process***" ("On-going Process document"). This document contains a list of jurisdictions that have been identified by the FATF as having strategic AML/CFT deficiencies but that have provided a high-level political commitment to address the deficiencies through implementation of an action plan developed in conjunction with the FATF. The situation differs in each jurisdiction and therefore every country on the list presents different degrees of ML/FT risks.

Three different categories of non-reputable / high risk jurisdictions are therefore identified in the FATF public documents:

[89] The latest issued FATF Statements, may be accessed through the FIAU website, on the following link www.fiumalta.org/Statements.

Table 6 – Categories identified by FATF

Categories identified by FATF	
Category 1	Jurisdictions that have strategic AML/CFT deficiencies and to which counter-measures apply
Category 2	Jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies
Category 3	Jurisdictions with strategic AML/CFT deficiencies that have developed an action plan with the FATF and have made a high-level political commitment to address their AML/CFT deficiencies

EU legal acts identifying high-risk third countries

Article 9 of the 4th AML Directive, empowers the European Commission to adopt delegated acts (**EU legal acts**) **identifying** and therefore listing **high risk third countries with strategic deficiencies** in their AML/CFT regimes that pose significant threats to the financial system of the Union in order to protect the proper functioning of the internal market.

The relevant EU legal acts should, where appropriate, be aligned with FATF standards with a view to reinforcing the efficacy of the fight against money laundering and terrorist financing at a global level, albeit the Commission's assessment in identifying high-risk third countries is deemed to be an autonomous process based on specific criteria, while taking into account evaluations made by FATF and other international organisations. This therefore means that the European Commission remains free to differ from the FATF list.

Assessing and managing the ML/FT risk posed by high risk jurisdictions/high risk third countries identified in the FATF public documents and/or identified in the EU legal acts

Regulation 5(5) of the PMLFTR requires subject persons to have in place procedures to manage the ML/FT risks posed by their customers, products and services, transactions and delivery channels as well as countries and geographical areas. These procedures are mandatorily required in order for subject persons to be able to determine, *inter alia*, whether a customer or a beneficial owner is likely to pose a higher risk of ML/FT. Among other things, the customer risk assessment should include the identification of risks posed by a business relationship or an occasional transaction established or carried out with a natural or legal person from a particular jurisdiction, particularly those considered to pose a higher risk of ML/FT.

The FATF Risk-Based Approach Guidance[90], lists a number of factors that should be assessed in determining whether a jurisdiction poses a higher risk of ML/FT. This includes the situation where a jurisdiction is identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures. Therefore, all the jurisdictions that are identified by the FATF or EU Commission as having strategic AML/CFT deficiencies are to be considered as posing varying degrees of higher risk of ML/FT and subject persons are required to include the risks posed by such jurisdictions when conducting the customer risk assessment. For further guidance on the carrying out of customer risk assessments and the factors to be considered reference should be made to Section 3.5.

On the basis of Regulation 11(1)(c) of the PMLFTR, when dealing with natural or legal persons established or linked with a non-reputable jurisdiction, subject persons are required to apply commensurate EDD measures accordingly. Hence, whenever a subject person is faced with a business relationship or an occasional transaction connected to a non-reputable, the subject person should, in accordance with the above mentioned regulation, apply appropriate EDD measures[91]. A connection to a jurisdiction listed by the FATF or the EU Commission under the lists mentioned above may take various forms. By way of example, a business relationship or an occasional transaction shall be considered to be connected to a non-reputable jurisdiction falling within Categories 1, 2 and 3 if the customer, the beneficial owner, the source of funds/wealth or the business/economic activity are situated in or originate from such a jurisdiction. On the other hand however, not every form of connection to a non-reputable jurisdiction shall give rise to the requirement to apply EDD. By way of example, where a business relationship or an occasional transaction involves a customer who is a citizen of a non-reputable jurisdiction but does not reside in such jurisdiction and the business/economic activity and/or the source of wealth/funds involved are not in any way connected to such jurisdiction, the requirement to apply EDD does not arise.

Subject persons should also apply the risk based approach when it comes to the application of EDD measures in this regard. By way of example, EDD measures in relation to a business relationship or an occasional transaction connected to a jurisdiction falling within FATF Category 1 should be more stringent than those applied in relation to a business relationship or an occasional transaction connected to a jurisdiction falling within FATF Category 2, since the ML/FT risks posed by the former category 1 are considered to be higher.

Subject persons may, with respect to business relationships or occasional transactions involving non-reputable jurisdictions consider applying the following EDD measure:

(a) Obtain additional information on the customer and on the beneficial owner(s);
(b) Obtain additional information on the intended nature of the business relationship;
(c) Obtain information on the source of funds and source of wealth of the customer and of the beneficial owner(s);
(d) Obtain information on the reasons for the intended or performed transactions;

[90] FATF RBA Guidance, p. 23, paragraph 3.5

[91] It should be noted that the PMLFTR do not prohibit the establishment of a business relationship or the carrying out of an occasional transaction with/ for a natural or legal person established or linked with a non-reputable jurisdiction but rather, requires subject persons to apply commensurate EDD measures targeted to mitigate and if possible neutralise ML/FT risks associated with that particular jurisdiction.

(e) Obtain the approval of senior management for establishing or continuing the business relationship;
(f) Conduct enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;
(g) Introduce enhanced relevant reporting mechanism or systematic reporting of financial transactions;
(h) Limit business relationships or transactions with natural persons or legal entities from non-reputable jurisdictions.

Subject persons are prohibited from applying simplified due diligence (SDD) measures set out under Regulation 10 of the PMLFTR, as well as the reliance provisions set out under Regulation 12 of the PMLFTR in relation to a business relationship or occasional transactions connected to non-reputable jurisdictions.

In terms of Regulation 11(2) of the PMLFTR, when undertaking occasional transactions for, or establishing business relationships, or acting in the course of a business relationship with a natural or legal person established in a non-reputable jurisdiction, in respect of which there has been an international call for counter-measures (i.e. FATF Category 1 jurisdictions) subject persons are obliged to notify the FIAU of this occurrence. The FIAU may (in collaboration with the relevant supervisory authority), require a business relationship not to continue or a transaction not to be undertaken, or apply any other counter-measure as the FIAU may deem adequate under the respective circumstances. For all intents and purposes of this obligation emanating from the proviso under Regulation 11(2) of the PMLFTR, subject persons are to deem all listed under the FATF statements or by the EU Commission legal acts referred to above as non-reputable jurisdictions.

8.2 Group-Wide Policies and Procedures

8.2.1 Parents, Majority-Owned Subsidiaries and Branches

Regulation 6 of the PMLFTR requires subject persons that form part of a group to implement effective group-wide AML/CFT policies and procedures. What this implies for subject persons that are included within a group will vary according to whether they fall to be considered as a parent undertaking on the one hand or as a majority-owned subsidiary or branch on the other.

8.2.1.1 Subject Person as the Parent Undertaking

Where the subject person is a parent undertaking it has to ensure that it adopts a set of group-wide policies and procedures which address effectively the risks that each individual component of the group subject to AML/CFT requirements faces as well as the risks which the group as a whole is exposed to. Thus, apart from an individual business risk assessment, it may also be necessary to carry out a group-wide business risk assessment. Moreover, in drafting the said policies and procedures, the subject person has to consider the respective AML/CFT obligations to which its majority-owned subsidiaries or branches are subject to and ensure that the group-wide policies and procedures do not impede its subsidiaries and branches from meeting the same.

8.2.1.2 Subject Person as a Majority-Owned Subsidiary or Branch

Where the subject person is a majority-owned subsidiary or a branch, the subject person will have to ensure that any group-wide policies and procedures that it is required to apply allow it to meet its AML/CFT obligations. In situations where the said policies and procedures impede as much, the subject person is still required to abide by its obligations at law and should inform its parent that the group-wide policies and procedures being applied are not in line with Maltese law. Shortcomings in the group-wide policies and procedures cannot justify non-compliance with the PMLA, the PMLFTR, any Implementing Procedures or any other order, directive or guidance given by the FIAU.

8.2.2 Sharing of Information

The group-wide policies and procedures have to include policies and procedures on the sharing of information within the group for AML/CFT purposes. Thus, in so far as any information is collected by a subject person to meet its obligations under the PMLA, the PMLFTR or any FIAU Implementing Procedures, said information has to be used only for AML/CFT purposes and not for example for commercial purposes. Exception being made for any entities delegated with the implementation of AML/CFT measures, policies, controls and procedures, there would therefore be no grounds to justify the sharing of any such information with entities within the group which do not have any AML/CFT obligations.

Moreover, when sharing information within a group for AML/CFT purposes, subject persons have to consider whether so doing would run counter to the non-disclosure obligation arising from Regulation 16 of the PMLFTR. As already explained in Section 5.11, a subject person is precluded from disclosing to third parties that information has been demanded by the FIAU or that information has been or may be transmitted to the FIAU. This restriction applies also within a group context unless it is possible for the entities within the group to rely on the exceptions provided for under Regulation 16(2)(b) and (c). Subject to what has already been stated hereabove, any AML/CFT information which does not fall within the ambit of the non-disclosure requirement can still be shared within a group without any restriction thereon.

8.2.3 Reporting of Suspicious Transactions

Reporting of suspicious transactions is another aspect which needs to be considered carefully. In so far as all the subject persons within a group are subject to the PMLFTR and they have appointed a group-wide MLRO, it is possible for reporting to be centralised within the group. Where either of these conditions are not met, then each subject person would have to report any suspicious transactions individually and on its own account. In particular, it is to be noted that where a group comprises entities which are subject to reporting obligations in jurisdictions other than Malta, these entities have to comply with the reporting obligations set out in the local laws applicable to them.

8.2.4 Impediments to the Application of Group-Wide Policies and Procedures

Subject persons with majority-owned subsidiaries or branches in a jurisdiction other than a Member State which do not impose AML/CFT obligations of an equivalent level as those arising from 4th AML Directive have to ensure that these subsidiaries and branches still apply the same group-wide policies and procedures as any other entity within the group subject to AML/CFT obligations.

Where there may be impediments to do so, the subject person has to consider whether this impossibility gives rise to ML/FT risks and take measures to address the same. In this regard, it is to be noted that the ESAs have been mandated to issue regulatory technical standards on the measures to be so taken[92]. Given that these standards are issued by means of a regulation, they need not be transposed into Maltese law and are directly applicable to the subject persons they are addressed to. This notwithstanding, other subject persons are to consider whether the measures laid down therein can also be applied in their particular circumstances and, should this be the case, apply the same.

Where a subject person has to take any such measures, it is to inform the FIAU accordingly of the particular circumstances encountered, the risks identified, and, to the extent that this was possible, the measures taken to counter these risks and why it was deemed that these were sufficiently effective. In addition, subject persons are to note that in these circumstances it would not be able to exercise reliance on any such entities and, in so far as they are located in high risk jurisdictions, any transactions or activities involving the same is to be considered as presenting a high risk of ML/FT and as requiring the application of EDD measures.

It is important to note that the PMLFTR empower the FIAU, together with the relevant supervisory authority, to take additional action where it considers that the measures implemented by the subject person were not enough. These measures may include one or more of the following:

(a) Not to establish or even terminate business relationships that involve any such subsidiary or branch;
(b) Not to undertake any transactions through or involving the said subsidiaries or branches;
(c) Closing down the operations of any such subsidiary or branch.

8.3 Penalties for Breaches of AML/CFT Obligations

The PMLA and the PMLFTR contemplate a number of criminal offences and administrative breaches. Criminal offences carry with them pecuniary fines and/or imprisonment, and are subject to proceedings before the criminal courts of Malta as regulated by the Criminal Code

[92] 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

(Chapter 9 of the Laws of Malta). The criminal offences under the PMLA and the PMLFTR are listed under Section 8.3.5.

The following subsections deal with breaches of an administrative nature.

8.3.1 Administrative Sanctions under PMLFTR

Regulation 21 of the PMLFTR states that the failure to comply with any lawful requirement, order or directive issued by the FIAU under the PMLFTR and the PMLA, as well as any contravention of the PMLFTR or of any procedures (including these Implementing Procedures) or guidance issued in terms of Regulation 17 may render subject persons liable to an administrative sanction.

Administrative sanctions are pecuniary in nature, although the FIAU may issue reprimands in writing under certain circumstances. Sanctions may also be accompanied by other measures, including publication on the FIAU website or notification to relevant authorities or bodies, depending on the nature of the breach.

Penalties may either be imposed as a one-time fixed penalty or else on a daily cumulative basis. In the latter case, the minimum daily penalty that may be levied is of €250 per day.

Pecuniary Sanctions

The value of the sanctions that may be imposed for every separate contravention or failure to comply ranges from €1,000 to €46,500.

Serious, repeated or systematic contraventions

Notwithstanding the above, in cases of serious, repeated or systematic contraventions of the provisions of the PMLFTR or of any procedures or guidance issued in terms of Regulation 17 of the PMLFTR (including these Implementing Procedures), the maximum sanction that may be imposed shall vary depending on the activity carried out by the subject person, as follows:

Where the subject person carries out **relevant activity**, the maximum penalty shall be of €1,000,000, or of the equivalent of twice the value of the benefit derived from the contravention in question, where such value can be quantified.

Where the subject person carries out **relevant financial business**, the maximum penalty shall be of €5,000,000, or of the equivalent of 10% of the total annual turnover of the subject person, according to the latest available approved financial statements.

Minor contraventions

Where, on the other hand, the contraventions are deemed to be minor in nature, and the circumstances so warrant, the FIAU may impose a penalty below the aforementioned minimum threshold of €1,000, but of no less than €250. The FIAU may alternatively issue a reprimand in writing. As with all sanctions imposed, the issuance of a reprimand upon a subject person shall be taken into consideration in determining any future sanctions.

Table 7 below illustrates the penalties that may be imposed for breaches of the PMLFTR.

Table 7 – Penalties

Relevant Activity		
	Minimum	**Maximum**
Penalty for each contravention	€1,000	€46,500
Minor contraventions	€250 / Reprimand	€1,000
Serious, Repeated or Systematic Breaches	€1,000	€1,000,000 or 2x value of the benefit derived
Relevant Financial Business		
	Minimum	**Maximum**
Penalty for each contravention	€1,000	€46,500
Minor contraventions	€250 / Reprimand	€1,000
Serious, Repeated or Systematic Breaches	€1,000	€5,000,000 or 10% of annual turnover

Penalties imposed on directors of a legal person

In cases where a contravention has been committed by a legal person, the FIAU may deem it more appropriate to impose the penalty upon that natural person who at the time of the contravention was a director or officer tasked with the responsibility for the management of the legal person, or was purporting to act in such capacity, unless that person can prove that the contravention was committed without his or her knowledge and that all due diligence had been exercised in order to prevent the commission of that contravention.

In such instances, the FIAU may additionally communicate with the relevant authority or body responsible for the authorisation, licensing, registration or regulation of the subject person in question in order to recommend that action be taken to preclude that natural person from exercising any managerial functions within the subject person, as may be appropriate.

8.3.2 Procedure for imposition of sanctions

Where the FIAU becomes aware that a subject person may potentially be in breach of its obligations at law, it shall follow the procedure outlined hereunder in order to determine whether the circumstances warrant the imposition of a sanction:

1) The subject person is notified in writing of the potential breach or breaches detected by the FIAU, and is furthermore advised of the possibility that such breaches may lead to a penalty;
2) Subject persons are given the opportunity to make representations, and are requested to substantiate their representations with material information. Such information will allow

the Compliance Monitoring Committee of the FIAU to determine whether or not the sanction is to be imposed; [93]

3) The Compliance Monitoring Committee of the FIAU will evaluate the submissions and any other relevant circumstances, and will determine whether the finding amounts to a breach, as well as the sanction to be imposed or any other measure to be taken.

Where a sanction is imposed, the subject person shall be notified of the decision by means of a sanction letter. This letter will include the reasons for the decision, and instructions on payment. Subject persons shall have twenty (20) days from date of notification to settle the payment of the penalty. Subject persons may also appeal decisions where the penalty exceeds five thousand euro (€5000). The procedure for appealing penalties is further explained under Section 8.3.3. On the lapse of the aforementioned 20 days, should the subject person not have settled payment or filed an appeal, the penalty shall be deemed to be final and due.

The Committee may also determine that the breach does not subsist, or that the circumstances do not warrant the issue of a pecuniary penalty. In such cases, the Committee may still decide that a warning is appropriate or that particular measures are to be undertaken by the subject person.

8.3.3 Appeals from Administrative Penalties

Article 13A of the PMLA introduces the possibility of appealing an administrative penalty exceeding five thousand euro (€5,000), whether this amount is in respect of one or more contraventions covered by the same administrative act.

Subject persons may appeal from the entire penalty or from part thereof, as long as the part(s) appealed from exceed €5,000, in which case the subject person is to clearly state which parts of the penalty are being appealed from. The outcome of an appeal shall either confirm, vary or reverse the administrative penalty in question.

Subject persons must file an appeal application within **twenty (20) days** of notification of the sanction letter. The application must be filed in the Court of Appeal (Inferior Jurisdiction) and the relevant provisions of the Code of Organisation and Civil Procedure shall apply.

Subject persons are to note that the information and documents that form part of the appeal proceedings, including the appeal application and reply, remain confidential in nature and while subject persons have every right to consult a lawyer to represent them in court, the appeal will be held behind closed doors. The judgment will not be published through the usual means, save for those provisions relating to publication of penalties under the following sections.

8.3.4. Publication of Administrative Penalties and other Measures

[93] The Compliance Monitoring Committee is an internal committee of the FIAU which is responsible for determining whether a subject person has breached or otherwise its AML/CFT obligations.

8.3.4.1 Publication

Article 13C of the PMLA requires the FIAU to publish those administrative penalties which exceed €10,000 and which have become final and due.

A sanction is deemed to have become final and due:

- Upon the lapse of twenty days from the date of notification of the sanction letter and no appeal has been filed;
- Upon the termination of appeal proceedings filed by the subject person, if such appeal is decided against the subject person or is withdrawn or deserted;

Such publication shall be carried out in accordance with the policies and procedures established by the Board of Governors of the FIAU which are available on the FIAU's website.

8.3.4.2 Notification

Notification to ESA (Article 13(4) PMLA)

The FIAU is obliged to notify the relevant European Supervisory Authority (ESA) of any sanction or measure imposed upon a subject person carrying out relevant financial business. In such cases, the FIAU shall notify the relevant ESA of the action taken, and shall also notify it of any appeal proceedings lodged by the subject person, and the outcome of such appeal.

The European Supervisory Authorities responsible for the supervision of entities carrying out relevant financial business are the following:

- European Banking Authority (EBA);
- European Insurance and Occupational Pensions Authority (EIOPA);
- European Securities and Markets Authority (ESMA);

Notification to relevant governing authority (Article 21(6) PMLFTR)

Whenever the FIAU imposes an administrative penalty on any subject person, it shall be informing the supervisory authority, body or entity responsible for the authorisation, licensing, registration or regulation of, or the granting of a warrant to, the subject person in question. In doing so, the FIAU will be providing all the necessary information and documentation concerning the contravention.

8.3.5 CRIMINAL OFFENCES

Criminal Offences under the PMLA

Article	3(1)
Offence	Money laundering.

Penalty	A fine *(multa)* not exceeding €2,500,000, or imprisonment for a period not exceeding 18 years, or both such fine and imprisonment .

Article	4(2) / 4B(2)
Offence	Disclosure that an investigation is taking place, or other disclosures likely to prejudice an investigation.
Penalty	A fine *(multa)* not exceeding €11,646.87, or imprisonment for a period not exceeding twelve months, or both such fine and imprisonment.

Article	4(6A)
Offence	Disclosure likely to prejudice an attachment order or a connected investigation.
Penalty	A fine *(multa)* not exceeding €11,646.87, or imprisonment for a period not exceeding twelve months, or both such fine and imprisonment.

Article	4(5) / 4(10)
Offence	Acting in contravention of an investigation order or an attachment order.
Penalty	A fine *(multa)* not exceeding €11,646.87, or imprisonment for a period not exceeding twelve months, or both such fine and imprisonment.

Article	6
Offence	Acting in contravention of a freezing order.
Penalty	A fine *(multa)* not exceeding €11,646.87, or imprisonment for a period not exceeding twelve months, or both such fine and imprisonment.

Criminal Offences under the PMLFTR

Regulation	7(11)
Offence	False declaration, false representation or the production of false documentation by a customer or person purporting to act on the customer's behalf
Penalty	A fine *(multa)* not exceeding €50,000, or imprisonment for a period not exceeding two years, or both such fine and imprisonment.

Regulation	16(1)
Offence	Prohibited disclosures (tipping off)
Penalty	A fine *(multa)* not exceeding €115,000, or imprisonment for a period not exceeding two years, or both such fine and imprisonment.

CHAPTER 9 – RECORD KEEPING PROCEDURES

9.1 Purpose of keeping records

Subject persons have to retain records of any business relationship they enter into and of any transaction they carry out, be it an occasional transaction or a transaction that takes place within the context of a business relationship. These records are to include any documentation and information produced or obtained in complying with their obligations under the PMLA, the PMLFTR and any Implementing Procedures issued thereunder.

These records are not only intended to show that a subject person complied with its obligations at law but are also essential for a subject person to effectively discharge certain aspects of its AML/CFT obligations like the carrying out, or revision, of its business risk assessment and the carrying out of ongoing monitoring.

In addition, the records maintained by subject persons are intended to assist the FIAU, relevant supervisory authorities and law enforcement agencies in the prevention, detection, analysis or investigation of possible ML/FT. Hence, these bodies have the authority at law to request such information.[94] Moreover, subject persons should be aware that other authorities may, in terms of applicable law, demand access to certain records maintained in terms of this section for purposes other than the prevention, detection, analysis or investigation of possible ML/FT.

9.2 Records to be retained

Subject persons must have procedures in place to ensure that the following records are maintained:

(a) records of the actions taken to adopt and implement the risk-based approach which are to include the following:
   (i) a copy of the Business Risk Assessment referred to in Section 3.3, changes thereto as well as a record of any decision taken with respect to the said assessment;
   (ii) a copy of the subject person's most recent controls, policies, measures and procedures; and
   (iii) a copy of each Customer Risk Assessment carried out by the subject person with respect to customers as is referred to in Section 3.5 and of any revision thereof.

(b) the CDD information and documents obtained for identification and verification of identity purposes. The records to be maintained are to include the following:

   (i) where subject persons view the original CDD documents listed in Section 4.3.1.1(i) and (ii), the original documents themselves (where it is possible to retain originals) or a true copy of such original documents, signed and dated by an officer of the subject person or a scanned copy retained by making use of the electronic system set out under Section 4.3.1.1(iii);

[94] Regulation 13(1) of the PMLFTR.

(ii) where subject persons receive a copy of the CDD documents listed in Section 4.3.1.2(i), such copy should be maintained;
(iii) where subject persons use commercial electronic data providers in accordance with Section 4.3.1.2(ii) to verify the identity of any individual, the results of the search should be maintained;
(iv) where subject persons use video conferencing tools, identity verification software, or E-Ids as envisaged under Section 4.3.1.2 (i) and (ii) to verify the identity of any individual, the records listed in those sub-sections should be retained;
(v) where the verification of the residential address of any individual is carried out by visiting the same individual at such address, a record of the visit should be maintained;
(vi) where verification of the residential address of any individual is carried out by sending correspondence or codes via registered mail or other mail courier service in accordance with the procedure set out under Section 4.3.1.2 (i), the records listed in that section should be retained;
(vii) the documentation and other information obtained in fulfilment of the obligations set out in Sections 4.3.2.1 to 4.3.2.5, Section 4.8 and Sections 4.9 should be retained; and
(viii) any document obtained to ensure that the agent is duly authorised in writing to act on behalf of the customer (in fulfilment of the obligation set out in Section 4.3.3) should also be retained;

(c) records containing details relating to the business relationship that is formed and all transactions carried out in the course of a business relationship or occasional transaction. These records are to include the following:

(i) information gathered on the purpose and intended nature of the business relationship and information gathered to establish the business and risk profile as required under Section 4.4;
(ii) files related to accounts held by the subject person, where applicable, and all business correspondence of the subject person exchanged in the course of a business relationship or in the carrying out of an occasional transaction;
(iii) details on all transactions, whether international or domestic, carried out by the customers. The details should include:
    (a) the customer's and beneficiary's:
        - name,
        - address or
        - other identifying information that is usually used by the subject person to identify parties to a transaction,
    (b) the nature and date of the transaction;
    (c) the type and amount of currency involved;
    (d) the type and identifying number of any account involved in the transaction;
    (e) the volume of funds flowing through the account;

(f) the origin of the funds, where necessary, and the form in which the funds were placed or withdrawn[95]; and

(iv) any supporting evidence and records necessary to reconstruct all transactions carried out or facilitated by that subject person in the course of a business relationship or any occasional transaction.

Such records should either consist of original documents or else copies which are admissible in court proceedings.

Subject persons should also retain the following records required as evidence of compliance with the PMLFTR and for statistical purposes:

(a) internal reports made to the MLRO as referred to in Section 5.4;
(b) a record of any written determinations made by the MLRO and the designated employee, including the reasons for not filing a STR with the FIAU;
(c) STRs made by the subject person to the FIAU and of any follow-up submissions made in connection thereto;
(d) a record of AML/CFT training provided as indicated in Section 7.3;
(e) records of conduct certificates or other documentation obtained in the carrying out of employee screening as referred to in Section 7.5;
(f) records of any outsourcing agreements entered into and other documentation which evidences the subject person's adherence to its obligations under Chapter 6 of these Implementing Procedures;
(g) records of any reliance agreements entered into and of any related assessments undertaken on the other subject person or third party in terms of Section 4.10; and
(h) other important records, including:

- any reports by the MLRO or by the officer entrusted with the monitoring function under Section 5.3 above to senior management made for the purposes of complying with the obligations under the PMLFTR, such as recommendations on internal procedures, correspondent banking relationships, PEPs, etc;
- records of consideration of those reports and of any action taken as a consequence thereof;
- records of any internal audit reports or assessments dealing with AML/CFT issues;
- any other records that are necessary to demonstrate compliance with the obligations under the PMLA, the PMLFTR and any Implementing Procedures issued thereunder.

9.3 Period of retention of records

[95] These requirements only apply to those subject persons who carry out transactions in the course of their business.

Subject persons shall maintain the records, referred to in Section 9.2, for a period of **five (5) years**. However, subject persons are to note that the FIAU, relevant supervisory authorities or law enforcement agencies are entitled to demand that records, including personal data, be retained for longer periods, where such extension is considered necessary for the purposes of the prevention, detection, analysis and investigation of ML/FT activities by the FIAU, relevant supervisory authorities or law enforcement agencies.[96] This does not mean that subject persons can be directed to hold any records indefinitely, as the retention period as extended can never exceed **ten (10) years** in total.

Where a subject person ceases to conduct 'relevant financial business' or 'relevant activity' and the retention period has not yet elapsed, the record retention period shall continue to run until it lapses in full and irrespective of this cessation. Thus, individuals and/or entities that used to carry out 'relevant financial business' or 'relevant activity' are still obliged to retain records in accordance with this Chapter of the Implementing Procedures even after they cease to be considered as subject persons.

Although upon the expiry of the five (5) year period or any extension thereof, the necessity of retaining personal data in terms of the PMLFTR would cease, subject persons should consider whether they are subject to any other record retention obligations under any other applicable laws which set a longer retention period for the same data.

The date of commencement of this time period depends on the type of records to be retained as set out in Section 9.3.1 to Section 9.3.8 below.

9.3.1 CDD documentation

With respect to CDD documentation referred to in Section 9.2(b), the time period of five (5) years shall commence from the date on which the business relationship is terminated or the occasional transaction is carried out. In the case of a series of occasional transactions, the five (5) year period shall start to run on the date of the carrying out of the last transaction in that series of transactions.

Where the formalities necessary to end a business relationship could not be observed, the five (5) year period commences on the date on which the last transaction in the course of that business relationship was carried out.

The above-stated do not apply only with respect to CDD documentation, but also to the customer risk assessment and any revisions thereof applicable to the particular business relationship or occasional transaction.

9.3.2. Documentation on the business relationship and on the transactions carried out in the course of a business relationship or in relation to an occasional transaction

[96] Second proviso to Regulation 13(2) of the PMLFTR.

The time period for the retention of documentation referred to in Section 9.2(c) commences from the date on which all dealings taking place in the course of the transaction in question were completed. In relation to an occasional transaction or a series of occasional transactions, the time period commences on the date on which the occasional transaction or the last of a series of occasional transactions took place.

In so far as any other records which relate to the business relationship itself rather than to the transactions carried out in the course of the same are concerned, the retention period shall commence to run from the date on which the business relationship is terminated. Where the formalities necessary to end a business relationship could not be observed, the five (5) year period commences on the date on which the last transaction in the course of that business relationship was carried out.

9.3.3 Internal Reports made to the MLRO and STRs

An internal report made to the MLRO which has not given rise to a disclosure to the FIAU under Regulation 15(3) of the PMLFTR shall be maintained by the subject person for a period of five (5) years, as may be extended, together with a record of the reasons for not forwarding the report to the FIAU. This period shall commence to run on the date when the MLRO reaches the determination not to make a disclosure to the FIAU.

Copies of STR shall also be retained by the subject person for five (5) years, as may be extended, which period shall start to run on the date when the report was submitted.

9.3.4 Records submitted together with a STR

Notwithstanding what has been stated in Section 9.3.1 and Section 9.3.2 above, the retention period for any records referred to in those sections which are submitted as part of, or together with, a STR shall commence on the later date between either the date when the STR was submitted to the FIAU or the date when the business relationship ends or the transaction, be it an occasional transaction or otherwise, is carried out.

The above is applicable also in those cases where a STR is submitted following termination of a business relationship.

9.3.5 AML/CFT training

The time period of five (5) years for the retention of AML/CFT training records referred to in Section 9.2 shall commence to run from the date when the training was conducted.

9.3.6 Employee Screening Records

Employee screening records are to be retained until the employment relationship comes to an end or the employee is no longer entrusted with carrying out relevant financial business or relevant activity on behalf of the subject person.

9.3.7 Outsourcing Records

Records related to outsourcing and reliance arrangements are to be retained for five (5) years from the termination of any such arrangement.

9.3.8 Other Records

With respect to any other records referred to in Section 9.2 above, the retention period for the records referred to in Section 9.2(a)(i) and (ii) shall commence to run upon cessation of activities by the subject person. Any reports, assessments or action plans referred to in Section 9.2 and not already covered in the previous sections are to be retained for five (5) years, or for such longer period as the subject person may be directed, which commence when the same are adopted or approved by the subject person.

Further guidance on the retention period applicable to other categories of records may be provided by the FIAU in guidance or procedures requiring the retention of the same.

9.4 Form of records

Subject persons may maintain their records in any one of the following forms:

- in physical files; or
- in any electronic form.

Notwithstanding the above, whenever subject persons obtain documents certified by third parties (i.e. not being officers or employees of the subject person) in fulfilment of their obligations under these Implementing Procedures, subject persons should retain on file the physical document certified by the third party and not a copy thereof.

Records kept must be of good quality and clearly legible. Any photographic evidence of identity is to be sufficiently clear as to allow the individual concerned to be identified from the same. Subject persons should use a standardised approach to record keeping and must ensure that the approach used enables the quick retrieval of records for the purposes laid out in Section 9.5 below.

9.5 Retrieval of records

Subject persons are required to maintain efficient record-keeping procedures that enable them to retrieve information in a timely manner when so requested by the relevant authorities acting in accordance with the applicable laws.

9.5.1 General Requirements

Subject persons are required to provide the FIAU, relevant supervisory authorities and law enforcement agencies, for the purposes of the prevention, detection, analysis and investigation of ML/FT with information as might be required from time to time related to:

(a) whether they maintain or have maintained a business relationship with, or carried out an occasional transaction for, or involving, a specified natural or legal person/s during the previous five (5) years; and
(b) the nature of that relationship or transaction.

To this effect, subject persons are required to establish effective systems which are commensurate with the size and nature of their business and that enable them to respond efficiently, adequately, promptly and comprehensively to such enquires made to them by the FIAU or by supervisory authorities or law enforcement agencies in accordance with applicable law. The provision of this information is of particular importance in the context of procedures leading to measures such as freezing or seizing of assets – including terrorist assets.

When requests for information are made by the FIAU, subject persons should ensure that they are able to reply to these enquiries in a timely manner, but not later than five (5) working days from when the demand is made.[97] It should be noted that the FIAU may impose a shorter response time for replies to requests for information.[98] In all cases, the subject person can make representations justifying why the requested information cannot be submitted within the response time imposed by the PMLFTR, or as shortened by the FIAU.[99] In such cases the FIAU may, at its discretion and after having considered such representations, extend such time period as may be reasonably necessary to obtain the information, whereupon the subject person shall submit the information requested within the time period as extended.

9.5.2 Organisation and Categorisation of Records

To facilitate the retrieval of records and to assist in any compliance monitoring activity conducted by the FIAU or other relevant supervisory authorities, subject persons are to maintain a list of their current business relationships setting out:

(a) The name of the customer and/or customer reference number;
(b) The risk categorization of the business relationship (risk rating or risk score);
(c) The type of service being provided or product being offered;
(d) Whether the customer is a natural person, legal person, a trust or other legal arrangements;
(e) The date of commencement of the business relationship and, where applicable, the date on which it ceased;
(f) A list of all the jurisdictions that the customer deals with, including the jurisdictions where:

[97] Regulation 15(8) of the PMLFTR.
[98] First proviso to Regulation 15(8) of the PMLFTR.
[99] Second proviso to Regulation 15(8) of the PMLFTR.

- The customer and, where applicable, the ultimate beneficial owner/s reside;
- The legal person, trust or other legal arrangement is registered or incorporated, as may be applicable;
- The business or economic activity of customer is carried out;

(g) Whether the customer or ultimate beneficial owner is a PEP, or an immediate family member or a close associate of a PEP; and

(h) Whether reliance has been exercised with respect to the particular business relationship.

A similar list should also be maintained for any occasional transactions carried out over the previous five (5) years and any business relationships that were terminated over the same period of time.

9.6 Record Keeping Obligations and Data Protection

The records which a subject person is required to retain will inevitably contain personal data. At times, this may give rise to questions as to how a subject person is to reconcile its obligations in terms of the PMLA, the PMLFTR and any Implementing Procedures issued thereunder, and data protection obligations which it has to abide by. To this end, the FIAU is providing some guidance on this aspect. Subject persons are to note that:

(a) A subject person has to inform a customer that the collection of personal data is necessary to comply with its obligations under the PMLA, the PMLFTR or any applicable Implementing Procedures issued thereunder, and that any such personal data will be used only for AML/CFT purposes (other than where the subject person is subject to additional obligations which require it to process the same data). It is therefore important that subject persons ensure that any such data is actually used only for the said purposes and should restrict access thereto accordingly.

(b) The PMLFTR do not impose restrictions on the right of access that a data subject can exercise in terms of the applicable laws other than to ensure that any analysis or investigation into possible cases of ML/FT is not prejudiced. Thus, in line with what is provided in Regulation 16(1) of the PMLFTR, in replying to a data subject who is exercising his right of access a subject person cannot disclose that it has received and replied to a request for information from the FIAU in his regard, or that it has generated an internal report or submitted a STR which concerns the data subject. In this regard subject persons are to keep in mind the provisions of the Restriction of the Data Protection (Obligations and Rights) Regulations issued under the Data Protection Act, which provide for restrictions to certain obligations and rights emanating from Article 23 of the GDPR. In particular, subject persons should be aware that Regulation 4(b) permits restrictions to such rights to be made where such restrictions are a necessary measure required 'for the prevention, detection, investigation and prosecution of criminal offences, including measures to combat any money laundering activity, and the execution of criminal penalties'

(c) Once the five (5) year retention period expires, subject persons have to assess the necessity of retaining personal data held in terms of the PMLA, the PMLFTR and any Implementing Procedures for longer periods. Subject persons should therefore consider

any data protection requirements to which they are subject and whether there exists a justification to hold onto the said records (e.g. an additional requirement at law to retain all or part of these records for a period in excess of the five (5) years imposed by the PMLFTR).

(d) The risk-based approach allows subject persons to understand which information may be required in order to carry out CDD measures that are commensurate and appropriate according to the level and kind of risks identified. When requesting information and documents from the customer, such as for identification and verification purpose, or for assessing the source of wealth, subject persons should consider the necessity and proportionality of the specific requests made in light of the risk posed by a given business relationship or occasional transaction. This may be done by assessing:

i) Whether the information or document that is requested or provided helps the subject person to fulfil the purpose or the requirement for which it is being requested or retained;
ii) Whether other information or documents which are less instrusive or hold less personal data may be obtained to achieve the same purpose;

Examples of unnecessary processing:

a) Requesting a bank statement to verify the residential address when a government issued identification document has already been provided containing such information;
b) Requesting detailed source of wealth information on a PEP for the purposes of opening a a bank account for that PEP's son/daughter when that bank account is being opened primarily to receive monthly university stipend payments.

In the event that a subject person is directed by the FIAU, a relevant supervisory authority or a law enforcement agency to retain records for a period in excess of five (5) years as described in Section 9.3, the subject person would have to carry out this assessment once the longer retention period expires.