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

PART I

Issued: **20th May 2011**
Last amended: **26th February 2015**

TABLE OF CONTENTS

ABBREVIATIONS

3rd AML Directive	European Union Directive 2005/60/EC
AML/CFT	Anti-money laundering/combating funding of terrorism
CDD	Customer due diligence
EDD	Enhanced customer due diligence
EU	European Union
FATF	Financial Action Task Force
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
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
PMLFTR	Prevention of Money Laundering and Funding of Terrorism Regulations
RBA	Risk-Based Approach
SDD	Simplified customer due diligence
STR	Suspicious transaction report
UN	United Nations

CHAPTER 1 – INTRODUCTION

1.1 To whom do the Implementing Procedures apply?

The Procedures Implementing the Provisions of the Prevention of Money Laundering and Funding of Terrorism Regulations, hereinafter referred to as 'Implementing Procedures', are intended for those persons, whether natural or legal, referred to in the PMLA[1] and the PMLFTR[2] as 'subject persons'.[3]

The PMLFTR define subject persons as those persons carrying out relevant activity or relevant financial business.

'Relevant activity'[4] 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 execution 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 trusts, companies or similar structures, or when acting as a trust or company service provider;
(d) trust and company service providers not already covered under paragraphs (a), (c), (e) and (f);
(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) any person providing trustee or any other fiduciary service, whether authorised or otherwise, in terms of the Trusts and Trustees Act;
(g) casino licensee;

[1] Act XIX of 1994 as amended, Cap. 373 of the Laws of Malta.
[2] Legal Notice 180 of 2008 as amended, issued on 31st July 2008.
[3] Article 14 of the PMLA and Regulation 2 of the PMLFTR respectively.
[4] Regulation 2 of the PMLFTR.

(h) other natural or legal persons trading in goods whenever payment is made in cash in an amount equal to fifteen thousand euro (€15,000) or more whether the transaction is carried out in a single operation or in several operations which appear to be linked; and
(i) any activity which is associated with an activity falling within paragraphs (a) to (h)".

'Relevant financial business'[5] is defined in the PMLFTR as:

"(a) any business of banking or any business of an electronic money institution carried on by a person or institution who is for the time being authorised, or required to be authorised, 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 authorised, or required to be authorised, under the provisions of the Financial Institutions Act;
(c) long term insurance business 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 or enrolled or required to be enrolled under the provisions of the Insurance Intermediaries Act, any affiliated insurance business carried on by a person in accordance with the Insurance Business (Companies Carrying on Business of Affiliated Insurance) Regulations, and any business of insurance carried on by a cell company in accordance with the provisions of the Companies Act (Cell Companies Carrying on Business of Insurance) Regulations;
(d) investment services carried on by a person or institution licensed or required to be licensed under the provisions of the Investment Services Act;
(e) 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;
(f) a collective investment scheme, marketing its units or shares, licensed or recognised, or required to be licensed or recognised, under the provisions of the Investment Services Act;
(g) any activity other than that of a scheme or a retirement fund, carried on in relation to a scheme, by a person or institution registered or required to be registered under the provisions of the Special Funds (Regulation) Act and for the purpose of this paragraph, ''scheme'' and ''retirement fund'' shall have the same meaning as is assigned to them in the said Act;
(h) 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;
(i) any activity under paragraphs (a) to (h) carried out by branches established in Malta and whose head offices are located inside or outside the Community;[6]
(j) any activity which is associated with a business falling within paragraphs (a) to (i)".

[5] Regulation 2 of the PMLFTR.
[6] In accordance with Regulation 2 of the PMLFTR, 'Community' shall mean the European Community and, for the purposes of the PMLFTR, shall include EEA States. Reference in these Implementing Procedures to 'Community' shall be construed in accordance with the definition provided in the PMLFTR.

1.2 Purpose of the Implementing Procedures

The purpose of these 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.

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

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

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 Financial Action Task Force.[7] Subject persons should therefore ensure that when reference is made to the Implementing Procedures such reference is made to the most recent version.

1.3 How should the Implementing Procedures be used?

The Implementing Procedures recognise the principle of proportionality in their application. Consequently, subject persons are allowed a degree of flexibility in the application of certain AML/CFT measures in relation to their individual size and business activity. The manner in which this flexibility is to be exercised is explained in detail in different parts of these Implementing Procedures.

The primary consideration in applying AML/CFT measures should be the ML/FT risks to which the subject person may be vulnerable. As a general rule subject persons are required to manage their ML/FT risks in the most appropriate and proportionate manner in accordance with the risks

[7] The FATF was established by the G7 Summit that was held in Paris in 1989 in response to mounting concern over the money laundering phenomenon. It is an inter-governmental body, consisting of thirty-five members, whose purpose is the development and promotion of policies and to monitor members' progress in implementing necessary measures to combat ML/FT. The FATF issued the Forty Recommendations in April 1990 to provide a comprehensive set of standards to be followed in a plan for a coordinated global fight against money laundering. These recommendations were revised in 1996 and 2003. A new set of special recommendations, known as the Nine Special Recommendations, were issued in 2001 in response to the emerging threat of financing of terrorism. The Forty Recommendations, together with the Nine Special Recommendations, are intended to be of universal application and are widely accepted as the blue print for most national legislation in this area. Further information may be obtained on the FATF website at the following link: http://www.fatf-gafi.org/pages/0,2987,en_32250379_32235720_1_1_1_1_1,00.html.

identified pursuant to the carrying out of a risk assessment. The Implementing Procedures assist subject persons in achieving this objective within the parameters of the law.

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, which applies to each sector specifically, is incomplete on its own and must be read in conjunction with Part I of the Implementing Procedures. The Implementing Procedures shall be binding on subject persons as from the date on which they are issued.

A reading of the Implementing Procedures should not be construed as a substitute for a reading of the PMLFTR. Moreover, this document should not be used as an internal procedures manual or as a checklist of steps to be taken when complying with AML/CFT obligations.

1.4 Status of the Implementing Procedures

These Implementing Procedures are being issued under Regulation 17 of the PMLFTR, which empowers the FIAU to issue such Implementing Procedures for the carrying into effect of the provisions of the PMLFTR. In accordance with this Regulation, these Implementing Procedures **are binding on all subject persons** and failure to comply with such procedures shall render subject persons liable to an administrative penalty of not less than two hundred and fifty euro (€250) and not more than two thousand five hundred euro (€2,500).[8] Penalties imposed under Regulation 17 shall be imposed by the FIAU without recourse to a court hearing and may be imposed either as a one time penalty or a daily cumulative basis until compliance, provided that in the latter case the accumulated penalty shall not exceed twelve thousand five hundred euro (€12,500).[9]

In view of the fact that the Implementing Procedures provide an interpretation of the provisions of the PMLFTR and measures as to how the PMLFTR are to be effectively implemented in practice, in a vast majority of cases a breach of the Implementing Procedures will also constitute a breach of the PMLFTR. In such cases the FIAU will impose the penalty contemplated under the relevant provision of the PMLFTR which has been breached. Any other breach of the Implementing Procedures shall warrant an administrative penalty in terms of Regulation 17(2). The FIAU shall not impose a penalty for a breach of the Implementing Procedures where a subject person has already been sanctioned for the same act or omission in terms of the PMLFTR.

It should also be noted that Regulation 4(6)(a) of the PMLFTR states that a court shall take into consideration these Implementing Procedures in determining whether a subject person has complied with the obligations emanating from the PMLFTR.

[8] Regulation 15(15) of the PMLFTR.
[9] Regulation 15(16) of the PMLFTR.

CHAPTER 2 – OVERVIEW

2.1 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 lend a legitimate appearance to such proceeds. This process is of crucial importance for criminals as it enables the perpetrators to make 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.

Traditionally, three stages were identified for the process of money laundering – the placement stage, the layering stage and the integration stage. In the placement stage money derived from illegal activities is often initially introduced into the financial system by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments that are then collected and deposited into accounts at another location. This is the point at which the proceeds of crime are most apparent and most easily detected. 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. For instance the launderer may transfer the funds to a series of bank accounts situated in different jurisdictions. The launderer would then integrate the funds by investing such funds into, for instance, real estate, luxury goods, or business ventures thereby enabling the funds to enter the economy in a legitimate manner.

It should be noted that the three-stage model is rather simplistic and does not accurately reflect every type of money laundering operation. In fact, a modern explanation of money laundering moves away from the traditional three-stage concept and focuses more on the concealment or disguise of the origin of the illicit money.

The definition of money laundering[10] in the PMLA goes beyond generically expounding the notion of money laundering and 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;

[10] The definition provided in Article 2 of the PMLA transposes Article 1(2) of the EU Third Money Laundering Directive (2005/60/EC). This definition also reflects the definition of money laundering provided in Article 9 of the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198) to which Malta is a party.

(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)".

2.2 What is funding of terrorism?

Funding of terrorism is the process by which terrorist organisations or individual terrorists are funded in order to be able to carry out acts of terrorism.[11] This process is defined in Article 328F of the Criminal Code (Cap. 9 of the Laws of Malta) as the process by which a person "receives, provides or invites another person to provide, money or other property intending it to be used, or which he has reasonable cause to suspect that it may be used, for the purposes 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. Another difference is that while the money launderer generates income by obscuring the link between the crime and the generated funds, the terrorist's ultimate aim is not to generate income from the fund-raising mechanisms but to obtain resources to support terrorist operations.[12]

Although it would seem logical that funding from legitimate sources would not need to be laundered, there is nevertheless often a need for terrorists to obscure or disguise links between the organisation or the individual terrorist and its or his 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.[13]

Some of the specific methods detected with respect to various terrorist organisations include cash smuggling, structured deposits to or withdrawals from bank accounts, purchases of various types of monetary instruments, use of credit or debit cards and wire transfers.[14]

[11] Article 328A of the Criminal Code (Cap. 9 of the Laws of Malta) provides a definition of acts of terrorism.
[12] FATF, *Guidance for Financial Institutions in Detecting Terrorist Financing*, April 2002, pp. 4-5, paragraph 12, 13 and 16.
[13] *Ibid*, p.5, paragraph 15.
[14] *Ibid*, p.5, paragraph 15.

2.3 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 (Cap. 101 of the Laws of Malta) was amended to introduce the offence of money laundering in relation to the proceeds of certain drug-related offences. 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 (Cap. 31 of the Laws of Malta) 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 were consequently repealed and replaced by the PMLFTR, which now 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.

2.3.1 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.

The first part of the PMLA provides a definition of money laundering (refer to Section 2.1) and criminalises the act of money laundering.[15] The maximum penalty for the offence of money laundering is a fine amounting to two million, three hundred twenty nine thousand, three hundred seventy three euro and forty euro cents (€2,329,373.40) or to imprisonment for a period not exceeding fourteen years, or to both such fine and imprisonment.[16] 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 unincorporated.[17] The PMLA also provides a definition of criminal activity[18]

[15] Article 3(1) of the PMLA.

[16] Article 3(1) of the PMLA. The amount of two million, three hundred twenty nine thousand, and three hundred seventy three euro and forty euro cents (€2,329,373.40) corresponds to the sum of one million Maltese liri (Lm 1,000,000) at the fixed Maltese lira/Euro exchange rate of 0.4293.

[17] Article 3(2) of the PMLA.

[18] Article 2(1) of the PMLA.

and property.[19] Originally, the PMLA only applied to a limited list of predicate offences,[20] 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.[21]

The PMLA lays down the procedures for the prosecution of a money laundering offence[22] as well as the measures for the confiscation of property upon a conviction of money laundering,[23] measures for the freezing of assets when a person is charged with an offence of money laundering[24] and measures for the issuance of an investigation and/or attachment order when a person is suspected of having committed an offence of money laundering.[25] Additionally, by virtue of article 435AA of the Criminal Code, which is applicable to the PMLA, the Criminal Court may now order a bank to monitor the banking operations being carried out through one or more accounts of a person suspected of having committed an offence of 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 an offence 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 2.4.

2.3.2 The Prevention of Money Laundering and Funding of Terrorism Regulations

The PMLFTR, which were issued by virtue of Legal Notice 180 of 2008, have repealed and replaced the 2003 Regulations. The various amendments to the Regulations since 1994 reflect the corresponding international developments and legislative developments within the European Union. In fact the PMLFTR transpose the 3rd AML Directive which, in turn, is modelled on the FATF Forty Recommendations and the Nine Special Recommendations.[26]

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

[19] Article 2(1) of the PMLA.
[20] The predicate offence is the underlying criminal activity from which the illegal funds originate.
[21] Article 2(1) of the PMLA.
[22] Article 3(2A), (3), (4), (6) and (7) of the PMLA.
[23] Article 3(5) of the PMLA.
[24] Article 5 of the PMLA.
[25] Article 4 of the PMLA.
[26] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing – *OJ L 309, 25.11.2005, page 15*. The transposition into Maltese law include the Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC as regards the definition of 'politically exposed person' and the technical criteria for simplified due diligence procedures and for exemptions on grounds of a financial activity conducted on an occasional or very limited basis – also referred to as the Implementation Directive – *OJ L 214, 04.08.2006, page 29.*

- customer due diligence;
- record keeping;
- internal reporting;
- training; and
- procedures on internal control, risk assessment, risk management, compliance management and communications.

2.4 The Financial Intelligence Analysis Unit

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 defines its powers and functions. The FIAU is a government agency having a distinct legal personality which is responsible for the implementation of the AML/CFT regime in Malta. The model adopted by the Maltese legislator is an administrative model, meaning that the investigative and law enforcement powers are vested in the Police.

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 financial reports made by subject persons on transactions suspected of involving ML/FT. The FIAU is given additional powers for co-operating and exchanging information with local and foreign supervisory authorities and foreign FIUs. Another core function of the FIAU, discussed in more detail in Section 2.4.1 below, is its responsibility to monitor and ensure compliance by subject persons with their obligations under the PMLFTR.

The Unit has a wide-ranging power to demand information. 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 penalties on subject persons in cases of failure to comply with the provisions of the PMLFTR and may require the closure of branches of subject persons in certain particular circumstances.

The PMLA specifically mentions two main organs of the Unit: 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, and which is 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.

2.4.1 The FIAU's compliance monitoring function

The FIAU is responsible for monitoring compliance by subject persons with the obligations set out under the PMLFTR. In the fulfilment of such responsibility the FIAU conducts both off-site and on-site monitoring as explained below.

Off-site monitoring is carried out on the basis of a desk-review of information received from the subject person. Such information would include the procedures manual of the subject person, as well as any other documentation held by the subject person that would be deemed relevant by the FIAU in carrying out its compliance assessment. Additionally, in order to further assist the FIAU in carrying out its off-site compliance monitoring function, subject persons are required to submit an annual compliance report containing information and data on the activities of the subject person (for further details refer to Section 6.11).

After carrying out a degree of off-site monitoring, the FIAU may also carry out on-site examinations at the premises of the subject persons to determine the extent to which the provisions of the PMLFTR are being implemented in practice. In the course of on-site examinations the MLRO is expected to provide a detailed explanation of the internal procedures of the subject person and to produce a number of customer files for inspection, selected randomly in advance by the officers carrying out the examination. 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, to carry out on-site examinations on behalf of the FIAU. In fact, the MFSA conducts AML/CFT on-site examinations on behalf of the FIAU in relation to subject persons carrying out relevant financial business and authorised trustees. Notwithstanding the fact that the FIAU may request the MFSA to carry out on-site examinations on its behalf, the officers of the FIAU often participate in such on-site examinations. In all cases where on-site examinations are conducted by the MFSA the findings of the examination are reported to the FIAU and the FIAU determines whether any action is necessary to rectify breaches of the PMLFTR which are detected during the on-site examinations.

CHAPTER 3 – CUSTOMER DUE DILIGENCE

This chapter provides implementing procedures in relation to Regulations 7, 8, 10, 11 and 12 of the PMLFTR, which set out measures related to customer due diligence.

The purpose of the requirement of CDD measures is to ensure that subject persons have adequate mechanisms in place in order to be in a position to determine who the applicant for business, the customer or any beneficial owner is, to verify whether such person is the person he purports to be, to determine whether such person is acting on behalf of another person, to establish the purpose and intended nature of the business relationship and to monitor such business relationship on an ongoing basis.

CDD measures assist subject persons in determining whether a customer falls within their risk parameters and to understand the business profile of the customer with sufficient clarity in order to identify those transactions that fall outside this profile and thus to be able to form an opinion on ML/FT suspicions when necessary. Additionally, CDD measures enable subject persons to assist the FIAU by providing timely and precise information on customers and/or their activities when a request is made according to law.

The PMLFTR also provide for the application of simplified and enhanced CDD measures in certain specific circumstances, as well as reliance by subject persons on the CDD measures carried out by other subject persons or third parties.

3. 1 Application of CDD measures

The CDD measures that subject persons are required to carry out are the following:

- identification and verification of the applicant for business (refer to Section 3.1.1);
- identification and verification of the beneficial owner, where applicable (refer to Section 3.1.2);
- identification and verification when the applicant for business does not act as principal (refer to Section 3.1.3);
- obtaining information on the purpose and intended nature of the business relationship (refer to Section 3.1.4);
- conducting ongoing monitoring of the business relationship (refer to Section 3.1.5);
- establishing the source of wealth and source of funds (refer to Section 3.1.6);
- setting up of a customer acceptance policy and ensuring that the applicant for business meets the requirements set out in such policy (refer to Section 4.1.1.1).

It is to be noted that the PMLFTR prohibit subject persons from keeping anonymous accounts or accounts in fictitious names.[27]

For the purposes of fulfilling the obligation imposed on subject persons to combat the funding of terrorism, subject persons should, *inter alia*, have a system in place which detects whether an

[27] Regulation 7(4) of the PMLFTR.

applicant for business is subject to any financial sanctions issued by the UN Security Council or the EU in relation to persons known to be involved in terrorism. Such system should be sufficiently adequate for subject persons to keep themselves updated with all sanctions that might have an impact on their business operations. A useful source in this regard is the 'Sanctions Implementation' section on the website of the MFSA[28] which is however neither authoritative nor complete. In fact, the use of such source should not be considered to be a substitute for the subject person's own independent research for such purposes.

3.1.1 Identification and verification of the applicant for business

Subject persons are required to establish systematic procedures for identifying an applicant for business and ensuring that such identity is verified on the basis of documents, data or information obtained from a reliable and independent source.

3.1.1.1 Who is the applicant for business?

The PMLFTR define an applicant for business as a legal or natural person, whether acting as principal or agent, who seeks to form a business relationship, or carry out an occasional transaction with a subject person.[29]

The applicant for business may either be a legal or a natural person. This notion is important as the application of CDD measures varies to some extent when applied to legal entities and other arrangements and natural persons. It is also important to distinguish between the situation where an applicant for business is acting as principal and where the applicant for business is acting as agent. The latter situation entails the subject person to carry out additional measures as set out in Sections 3.1.3.2 to 3.1.3.6.

Two types of prospective customers emerge from the definition of applicant for business:

The first is the applicant for business who seeks to form a **business relationship**. A business relationship, in accordance with the definition contained in the PMLFTR,[30] must comprise three important cumulative elements, which are the following:

(a) the relationship must be of a business, professional or commercial nature;
(b) the relationship must subsist for a period of time; and
(c) one of the persons involved in the relationship must be a subject person.

The second type of applicant for business is the prospective customer who carries out an **occasional transaction** with a subject person. The PMLFTR define an occasional transaction as any transaction other than a transaction carried out in the exercise of an established business relationship. An established business relationship is defined as a relationship which is formed once the subject person carries out customer due diligence measures in accordance with the provisions of the PMLFTR in relation to the applicant for business.[31]

[28] http://www.mfsa.com.mt/pages/viewcontent.aspx?id=105.
[29] Regulation 2 of the PMLFTR.
[30] *Ibid.*
[31] *Ibid.*

However, it should be noted that not every transaction that a customer carries out with a subject person outside an established business relationship automatically necessitates the application of CDD measures. In fact, CDD measures shall only be applied when an occasional transaction involves:

- a payment of fifteen thousand euro (€15,000) or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- a transaction which involves a money transfer or remittance, within the meaning of Regulation (EC) No 1781/2006, amounting to one thousand euro (€1,000) or more; and
- a transaction amounting to two thousand euro (€2,000) or more referred to in Regulation 9 of the PMLFTR.[32]

It is worth noting that the PMLFTR do not define 'customer'. The meaning of this word, therefore, has to be inferred from the context in which it is used in the PMLFTR and its ordinary dictionary meaning.

3.1.1.2 The nature of identification and verification of a natural person

The subject person must first identify the applicant for business and then verify such identity, which are two separate and distinct procedures.

(i) Identification

Identification takes place by obtaining the personal details and other relevant information in relation to that person.

With respect to a **natural person** the following information should be obtained:

(a) official full name;
(b) place and date of birth;
(c) permanent residential address;
(d) identity reference number, where available; and
(e) nationality.

This procedure should apply in the same manner with respect to both a resident and a non-resident applicant for business.

(ii) Verification

Verification takes place by making reference to documents, data or information obtained by the applicant for business from a reliable and independent source. For the purposes of this obligation, a reliable and independent source includes, *inter alia,* a government authority, department or agency, a regulated utility company or a subject person carrying out relevant financial business in Malta, in a Member State of the EU[33] or in a reputable jurisdiction, since these entities would have already checked the existence and characteristics of the persons concerned.

[32] This obligation only applies to casino licensees.
[33] For the purpose of this document, references to an EU Member State include reference to an EEA State.

(a) Where the applicant for business is present for verification purposes:

(1) the verification of the details provided by the person on his identity shall be carried out by making reference to a government-issued document containing photographic evidence of identity such as:

- a valid unexpired passport;
- a valid unexpired national or other government-issued identity card; or
- a valid unexpired driving licence.

(2) the verification of the residential address shall be carried out by making reference to any one of the following documents:

- a recent statement from a recognised credit institution;
- a recent utility bill;
- correspondence from a central or local government authority, department or agency;
- a record of a visit to the address by a senior official of the subject person;
- any government-issued document listed in paragraph (1) above, where a clear indication of residential address is provided; or
- any other document as may be specified in sectoral implementing procedures issued by the FIAU.

Documents, other than official government issued documents, must not be more than six months old.

Subject persons are required to view the above documents and keep a true copy of the original document on file. Such copy should be signed and dated by the officers of the subject person. Particular care should be taken to ensure that the documents obtained have not been forged or tampered with. Additionally, any documentation which is in a language not understood by the subject person should be translated. The translation should be dated, signed and certified by an independent person of proven competence confirming that it is a faithful translation of the original.

Where the applicant for business is a minor the above procedures should still be followed to the fullest extent possible. Where it is impossible to refer to an identification document of the minor because this does not exist, subject persons are required to identify and verify the identity of the parents or legal guardians in accordance with the procedures set out above and obtain proof of parenthood or legal guardianship.

(b) Where the applicant for business is not present for verification purposes:

Where the applicant for business is not present subject persons would only be in a position to obtain a copy of the original documents listed under paragraph (a)(1) above. Therefore, apart from obtaining a copy of such original documents, subject persons are also required to apply one of the enhanced due diligence measures set out in Section 3.5.1. With respect to the

documents listed under paragraph (a)(2) above subject persons should either obtain the original document or a certified copy.

Alternatively, subject persons may wish to verify the identification details and residential address of the applicant for business **by electronic means**. This is possible where the verification of the identity of a person is done electronically through recognised commercial electronic data providers set up specifically for that purpose.

Since there are no commercial electronic data providers in Malta, this method of verification may not be used for the verification of the identity of persons resident in Malta, unless such persons are registered with a foreign electronic data provider. In the event that a subject person is required to verify the identity of a person resident in a country where such electronic data providers may be legally set up, the subject person may make use of such electronic data providers for the purposes of verification of identity.

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;
- it uses a range of 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; 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 the level of certainty they provide as to the identity of the subject.

It is important to note that when conducting electronic verification, the standard level of confirmation should at least comprise the following:

(a) one match on an individual's full name and current permanent residential address; **and**
(b) a second match on an individual's full name and **either** his current permanent residential address **or** his date of birth.

Where the identity of an applicant for business is verified by electronic means, subject persons are also required to apply one of the enhanced due diligence measures set out in Section 3.5.1.

3.1.1.3 The nature of identification and verification of a legal person

For the application of CDD measures in relation to a legal person, subject persons should refer to Sections 3.1.3.2 to 3.1.3.5 further below.

3.1.2 Identification and verification of the beneficial owner

Subject persons are required to identify the beneficial owner, where applicable,[34] taking reasonable measures to verify the identity such that the subject person is satisfied of knowing who the beneficial owner is and, in the case of a body corporate, trust or similar legal arrangement, reasonable measures are to be taken to understand its ownership and control structure.[35] The requirements set out in sub-section (i) of Section 3.1.1.2 shall apply to the identification of a beneficial owner.

3.1.2.1 Who is the beneficial owner?

Regulation 2 defines a beneficial owner as a:

- **natural** person who ultimately owns or controls the customer; and/or
- **natural** person on whose behalf or for the benefit of whom a transaction is being conducted.

The key element in this definition is the notion of a 'natural person'. A beneficial owner is the ultimate owner of the assets subject to a business relationship or an occasional transaction.[36] The definition in Regulation 2 further clarifies who shall be considered a beneficial owner in certain determinate situations. This is illustrated in Table 1 below.

(a) Body corporate or body of persons	(i) A natural person/s that has: • Direct ownership of more than 25% (including bearer shares); or • Direct ownership of more than 25% voting rights; or • Direct control of more than 25% (including bearer shares); or • Direct control of more than 25% voting rights; or • Indirect ownership of more than 25% shares (including bearer shares) ; or • Indirect ownership of more than 25% voting rights; or • Indirect control of more than 25% shares (including bearer shares); or • Indirect control of more than 25% voting rights. (ii) A natural person who otherwise exercises control over the management of that body corporate or body of persons.
(b) Legal entity or legal arrangement which administers and distributes funds	(i) Determined beneficiaries – natural persons who are the beneficiaries of at least 25% of the property (ii) Non-determined beneficiaries – the class of persons in whose main interest the legal entity or arrangement is set up or operates (iii) A natural person who controls at least 25% of the property of the legal entity or arrangements

[34] The phrase 'where applicable' is being used in view of the fact that business relationships or occasional transactions do not always involve a beneficial owner.
[35] Regulation 7(1)(b) of the PMLFTR.
[36] This does not apply in the context of trusts.

(c) Long term insurance business	The beneficial owner shall be construed to be the beneficiary under the policy.

Table 1 – Definition of a beneficial owner

The contents of Table 1 are explained in further detail below.

(a) (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 or control, including, where applicable, through bearer shareholdings, more than 25% of the shares or voting rights in that body corporate or body of persons.

NOTE: *Natural persons who ultimately own or control a* ***company that is listed on a regulated market*** *which is subject to disclosure requirements consistent with Community legislation or equivalent international standards* ***shall not be considered to be beneficial owners*** *for the purposes of the PMLFTR and therefore the obligation under Regulation 7 does not apply.*

In order to determine who ultimately owns or controls more than 25% of the shares or voting rights in the body corporate or body of persons, reference may be made to the examples in Figure 1 and Figure 2 below.

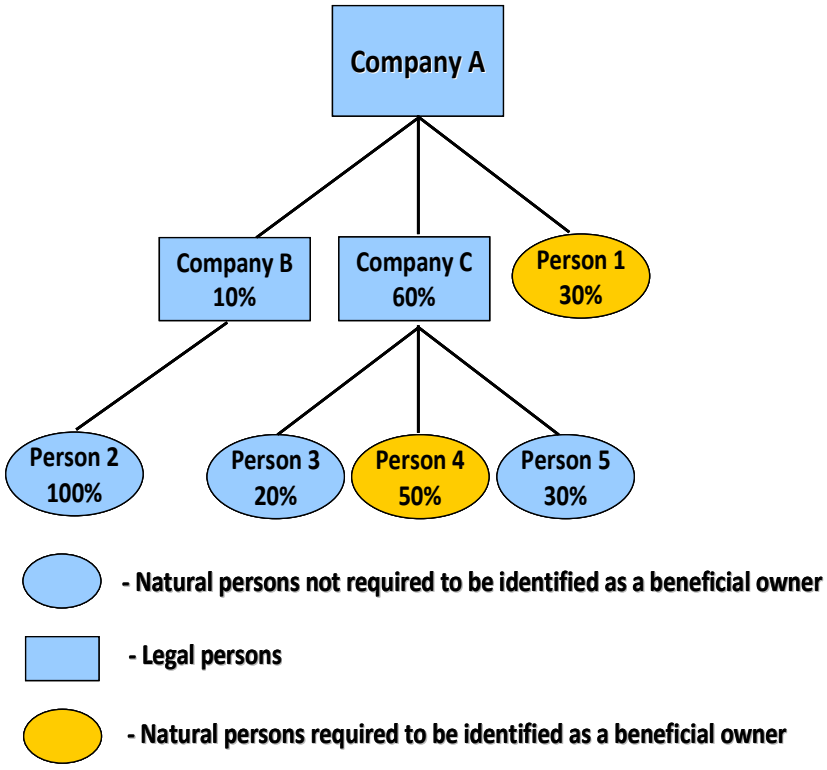

Figure 1 – Illustration I of beneficial owner

In Figure 1 subject persons are required to determine the natural persons who ultimately own more than 25% of the shares in Company A. 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, only natural person 4 qualifies as a beneficial owner for the purposes of the PMLFTR as he 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. Natural persons 2, 3 and 5 ultimately hold 10%, 12% and 18% of the shares in Company A respectively and therefore do not qualify as a beneficial owner for the purposes of the PMLFTR.

In Figure 2 subject persons are required to identify the natural persons who ultimately own more than 25% of the shares in Company V. 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 qualifies as a beneficial owner for the purposes of the PMLFTR as he ultimately holds 26% of the shares in Company V through Company X. Natural person 2 ultimately holds 10.4% of the shares in Company V and therefore does not qualify as a beneficial owner for the purposes of the PMLFTR. 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 Company Y and Company W and 15.6% of the shares in Company V through Company Z and Company X.

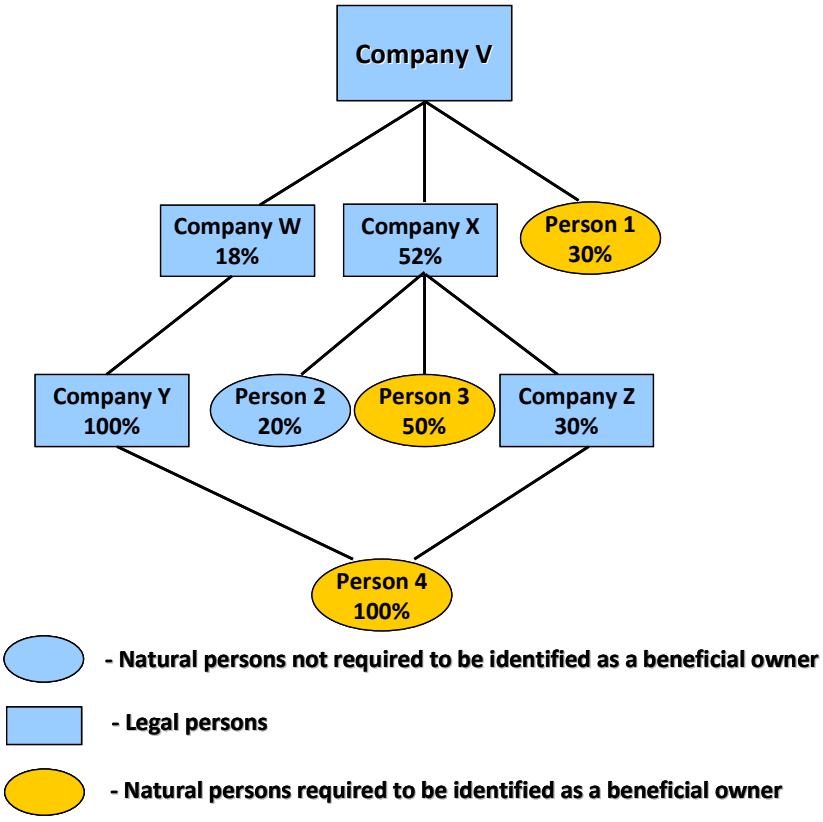

Figure 2 – Illustration II of beneficial owner

(ii) A natural person who otherwise exercises control over the management of that body corporate or body of persons.

This provision refers to those natural persons who, notwithstanding the fact that they own or control 25% or less of the shares or voting rights in the body corporate or body of persons, still exercise control over the management of that body corporate or body of persons. Since it is impossible to provide an exhaustive list of persons who fall within this category, 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. For instance, reference may be made to the Companies Act (Cap. 386 of the Laws of Malta) which refers to the notion of shadow directors. Article 316(5) of the Companies Act defines shadow directors as "person[s] in accordance with whose directions the directors of the company are accustomed to act". Such persons would therefore also be considered to be exercising control over the management of a company and would qualify as beneficial owners for the purposes of the PMLFTR.

In practice, it may prove to be difficult for subject persons to determine whether a person who is not officially appointed to act as a director is exercising control over the management of a company. In those cases where a subject person is aware or has reason to believe that a person is exercising control without holding any official appointment, such subject person should request more information directly from the applicant for business, and where the applicant for business confirms that such person exists, a written declaration signed by the applicant for business and the person exercising control over the management of the company must be provided to the subject person.

(b) *the beneficial owner of any other legal entity or legal arrangement which administers and distributes funds includes:*

(In this case the term 'legal entity' refers to entities such as foundations and associations,[37] while the term 'legal arrangement' refers to trusts and other similar arrangements)

(i) where the beneficiaries have been determined, a natural person(s) who is the beneficiary of at least 25% of the property of the legal entity or arrangement;

For instance, in order to determine who the beneficiary of at least 25% of the property of a trust is, subject persons are required to request the trustee of the trust to produce the trust deed, an extract thereof or a signed declaration by the trustee clearly showing the extent of the beneficial interest in the trust property that each beneficiary holds.

The same would apply in the case where it is necessary to determine who the beneficiary of at least 25% of the property of a foundation is. Subject persons are required to request the administrator of the foundation to produce the deed of foundation, an extract thereof or any other written document drawn up in accordance with the law which clearly states the extent of the rights that each beneficiary holds with respect to the property endowed in the foundation.

[37] In certain jurisdictions a trust is considered by law to have a legal personality separate from that of the trustee.

(ii) where the beneficiaries have not yet been determined, the class of persons in whose main interest the legal entity or arrangement is set up or operates;

In order to determine the class of persons in whose main interest the legal entity or legal arrangement, such as a trust, is set up or operates, subject persons are required to request the trustee of the trust in question to produce the trust deed, an extract thereof or a signed declaration by the trustee clearly setting out such information.

(iii) a natural person(s) who controls at least 25% of the property of the legal entity or arrangement.

In this case reference is being made to those instances where a person controls at least 25% of the property of the legal entity or arrangement, notwithstanding the fact that such person does not appear to be a beneficiary in an official manner. For instance, a person may not appear on the trust deed as a beneficiary of a trust but may still be exercising control over the property settled on trust and would therefore be the beneficial owner for the purposes of this sub-regulation.

It is difficult for subject persons to determine whether a beneficiary is actually exercising control or whether this control is being exercised by another person on whose behalf he is acting. Therefore, where the subject person is a trustee, the trustee shall require the beneficiary to sign a declaration stating that control over the property of the trust is not being exercised by a person other than the beneficiary appearing on the trust deed. In those cases where the beneficiary informs the trustee of the existence of a person exercising control over the property settled on trust other than the beneficiary appearing on the trust deed, the trustee shall require the beneficiary to identify the person exercising such control.

Where the subject person is a person or entity other than a trustee, the subject person shall require the trustee to sign a declaration confirming that he is not aware of the existence of a person exercising control over the property settled on trust other than the beneficiary appearing in the trust deed. In those cases where the trustee has been informed by the beneficiary of the existence of a person exercising control over the property settled on trust other than the beneficiary appearing on the trust deed, the subject person shall request the trustee to confirm the identity of such person.

(c) in the case of long-term insurance business, the beneficial owner shall be construed to be the beneficiary under the policy.

The PMLFTR are clear in specifying who the beneficial owner is in the circumstances under this sub-paragraph.

Without prejudice to the provisions of Regulation 8(5) of the PMLFTR, in those cases where it is not possible for the subject person to determine **with certainty** who the beneficial owner is on the basis of documentation available to him, subject persons should consider requesting the applicant for business to provide a written statement or declaration of beneficial ownership signed by the applicant for business and the beneficial owner.

3.1.2.2 Verification of the identity of the beneficial owner

The verification of identity of the beneficial owner, where applicable, should be carried out in accordance with the relevant sub-Sections of Section 3.1.3.

3.1.3 Applicant for business not acting as principal

Subject persons must determine whether the applicant for business is acting on behalf of somebody else by requesting such information directly from the applicant for business. Where the applicant for business is acting on behalf of someone else, subject persons must not only identify and verify the applicant for business but they are also required to apply additional measures.

The type of additional measures to be applied will depend on whether the person on whose behalf the applicant for business is acting is a natural person or a body corporate, a body of persons, or any other form of legal entity or arrangement. The additional measures to be applied with respect to a natural person are dealt with in Section 3.1.3.1, whereas the additional 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 3.1.3.2 to 3.1.3.6.[38] **In either case, the subject person must ensure that the applicant for business is duly authorised in writing to act on behalf of such other person.**

In the event that the applicant for business qualifies for the application of simplified due diligence, as laid out in Section 3.4, then such additional measures need not be applied.

3.1.3.1 When the principal is a natural person

Where the applicant for business is not acting as the principal and the principal is a natural person, subject persons should, in addition to identifying and verifying the identity of the applicant for business, identify and verify the identity of the principal. The identification and verification procedures to be applied with respect to the principal are those laid out in Section 3.1.1.2.

3.1.3.2 When the principal is a public company

Public companies may be listed or unlisted on a regulated exchange. In the case of public listed companies, subject persons may apply simplified CDD measures in accordance with Section 3.4 in view of the fact that these companies are subject to market regulation and a high level of public disclosure in relation to their ownership and business activities.

Where the public company is not listed, however, simplified CDD shall not be applied. In this case the subject person must first identify the public company by gathering the following information:

(a) official full name;
(b) registration number;
(c) date of incorporation or registration; and

[38] The list provided in Sections 3.1.3.2 to 3.1.3.6 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.

(d) registered address or principal place of business.

The subject person must then verify the above information as well as the legal status of the company by viewing one or more of the following documents, as the case may be:

- the certificate of incorporation;
- a company registry search, including confirmation that the public company has not been, and is not in the process of being dissolved, struck off, wound up or terminated;
- the most recent version of the Memorandum and Articles of Association or other statutory document.

In relation to the documents above, subject persons are required to view the original document, a certified copy of the original or a downloaded copy from the official registry website. Certification should be carried out by the company secretary, a director or an officer occupying an equivalent position or by the Registrar of Companies or a person occupying an equivalent position in a foreign jurisdiction. Alternatively, certification may be carried out by any of the persons referred to under Section 3.5.1(b). Where an original document is viewed, subject persons are required to keep a true copy of the document on file, which should be signed and dated by an officer of the subject person. Where a downloaded version is obtained by the subject person, documentary evidence of the download should be maintained clearly indicating the date when such document was obtained.

Once the verification is complete, the subject person must identify all the directors. In the case of directors who are natural persons, identification should be carried out by referring to the list of directors contained in the most recent version of the Memorandum and Articles of Association, by performing a company registry search provided that the officers of the company are listed therein or by obtaining a copy of the directors' register of the company. In the case of corporate directors, subject persons are required to obtain details of the corporate director's official full name, registration number, date of incorporation or registration and 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 merely to identify them.

Another requirement under the PMLFTR is the establishment of the ownership and control structure of the company. In order to comply with such obligation subject persons should obtain and maintain on file an explanation of the ownership and control structure of the company from the applicant for business, 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. 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 to under Section 3.5.1(b).

In order for the subject person to undertake any business or provide any services to the applicant for business it must ensure that the applicant for business discloses the identity of the beneficial owners and produces the relevant authenticated identification documentation in respect of the beneficial owners (refer to Section 3.1.2.1). The subject person must also take all reasonable measures to ensure that the applicant for business keeps the subject person informed of any changes in the beneficial ownership.

The procedure outlined above should apply in the same manner with respect to legal persons registered or established in Malta or in any other jurisdiction. However, subject persons should be aware that the type of documentation issued by company registries may vary between different countries. Therefore attention should be paid to the jurisdiction the documents originate from.

It is also important for subject persons to keep 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. In such situations, additional measures such as those listed in the following paragraph may be considered.

Where appropriate, subject persons should obtain further documentation on a risk-sensitive basis in accordance with the framework adopted by the subject person. Such additional information may include the following:

- a copy of the Shareholders' Register;
- information from independent sources such as, for instance, business information services; and
- a copy of the latest audited financial statements, where applicable.

It should also be pointed out that any documentation which is in a language not understood by the subject person should be translated. The translation should be dated, signed and certified by an independent person of proven competence, confirming that it is a faithful translation of the original.

3.1.3.3 When the principal is a private company

The subject person is required to first identify the private 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.

The subject person must then verify the above information as well as the legal status of the company by viewing one or more of the following documents, as the case may be:

- the certificate of incorporation;
- a company registry search, including confirmation that the private company has not been, and is not in the process of being dissolved, struck off, wound up or terminated;
- the most recent version of the Memorandum and Articles of Association or other statutory document.

In relation to the documents above, subject persons are required to view the original document, a certified copy of the original or a downloaded copy from the official registry website. Certification should be carried out by the company secretary, a director or an officer occupying an equivalent position or by the Registrar of Companies or a person occupying an equivalent position in a foreign

jurisdiction. Alternatively, certification may be carried out by any of the persons referred to under Section 3.5.1(b). Where an original document is viewed, subject persons are required to keep a true copy of the document on file, which should be signed and dated by an officer of the subject person. Where a downloaded version is obtained by the subject person, documentary evidence of the download should be maintained clearly indicating the date when such document was obtained.

Once the verification is complete, the subject person must identify all the directors. In the case of directors who are natural persons identification should be carried out by referring to the list of directors contained in the most recent version of the Memorandum and Articles of Association, by performing a company registry search provided that the officers of the company are listed therein or by obtaining a copy of the directors' register of the company. In the case of corporate directors, subject persons are required to obtain details of the corporate director's official full name, registration number, date of incorporation or registration and 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 merely to identify them.

Another requirement under the PMLFTR is the establishment of the ownership and control structure of the company. In order to comply with such obligation subject persons should obtain and maintain on file an explanation of the ownership and control structure of the company from the applicant for business, 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. 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 3.5.1(b).

In order for the subject person to undertake any business or provide any services to the applicant for business it must ensure that the applicant for business discloses the identity of the beneficial owners and produces the relevant authenticated identification documentation in respect of the beneficial owners (refer to Section 3.1.2.1). The subject person must also take all reasonable measures to ensure that the applicant for business keeps the subject person informed of any changes in the beneficial ownership.

The procedure outlined above should apply in the same manner with respect to legal persons registered or established in Malta or in any other jurisdiction. However, subject persons should be aware that the type of documentation issued by company registries may vary between different countries. Therefore attention should be paid to the jurisdiction the documents originate from.

It is also important for subject persons to keep 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. In such situations, additional measures such as those listed in the following paragraph may be considered.

Where appropriate, subject persons should obtain further documentation on a risk-sensitive basis in accordance with the framework adopted by the subject person. Such additional information may include the following:

- a copy of the Shareholders' Register;
- information from independent sources such as, for instance, business information services; and
- a copy of the latest audited financial statements, where applicable.

It should also be pointed out that any documentation obtained by the subject person which is in a language not understood by the subject person should be translated. The translation should be translated, dated, signed and certified by an independent person of proven competence, confirming that it is a faithful translation of the original.

3.1.3.4 When the principal is a commercial partnership

The same procedure applicable to a private 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.

The subject person must then verify the above information as well as the legal status of the partnership by viewing one or more of the following documents, as the case may be:

- the certificate of incorporation;
- a registry search, including confirmation that the partnership has not been, and is not in the process of being, dissolved, struck off, wound up or terminated;
- the most recent version of the partnership agreement or other statutory document.

In relation to the documents above, subject persons are required to view the original document, a certified copy of the original or a downloaded copy from the official registry website. Certification should be carried out by one of the general partners or an officer occupying an equivalent position or by the Registrar of Companies or a person occupying an equivalent position in a foreign jurisdiction. Alternatively, certification may be carried out by any of the persons referred to under Section 3.5.1(b). Where an original document is viewed, subject persons are required to keep a true copy of the document on file which should be signed and dated by an officer of the subject person. Where a downloaded version is obtained by the subject person, documentary evidence of the download should be maintained clearly indicating the date when such document was obtained.

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 should be carried out by either referring to the list of partners contained in the most recent version of the partnership agreement or by performing a registry search provided that the partners are listed therein. In the case of corporate partners, subject persons are required to obtain details of the corporate partner's official full name, registration number, date of incorporation or registration and 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 merely to identify them.

Another requirement under the PMLFTR is the establishment of the ownership and control structure of the partnership. In order to comply with such obligation subject persons should obtain and maintain on file an explanation of the ownership and control structure of the partnership from the applicant for business, 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. 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 to under Section 3.5.1(b).

In order for the subject person to undertake any business or provide any services to the applicant for business it must ensure that the applicant for business discloses the identity of the beneficial owners and produces the relevant authenticated identification documentation in respect of the beneficial owners (refer to Section 3.1.2.1). The subject person must also take all reasonable measures to ensure that the applicant for business keeps the subject person informed of any changes in the beneficial ownership.

The procedure outlined above should apply in the same manner with respect to partnerships registered or established in Malta or in any other jurisdiction. However, subject persons should be aware that the type of documentation issued by company registries may vary between different countries. Therefore attention should be paid to the jurisdiction the documents originate from.

It is also important for subject persons to keep 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. In such situations additional measures such as those listed in the following paragraph may be considered.

Where appropriate, subject persons should obtain further documentation on a risk-sensitive basis in accordance with the framework adopted by the subject person. Such additional information may include the following:

- information from independent sources such as, for instance, business information services; and
- a copy of the latest audited financial statements, where applicable.

It should also be pointed out that any documentation obtained by the subject person which is in a language not understood by the subject person should be translated. The translation should be dated, signed and certified by an independent person of proven competence, confirming that it is a faithful translation of the original.

3.1.3.5 When the principal is 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; and
(d) the foundation or association's registered address.

The subject person must then verify the above information as well as the legal status of the foundation or association by viewing one or more of the following documents, as the case may be:

- the certificate of registration;
- the most recent version of the constitutive document.

In relation to the documents above, subject persons are required to view either the original document or a certified copy of the original. Certification should be carried out by one of the founders or associates. Alternatively, certification may be carried out by any of the persons referred to under Section 3.5.1(b). Where an original document is viewed, subject persons are required to keep a true copy of the document on file. Such copy should be signed and dated by an officer of the subject person.

Once the verification is complete, the subject person must identify all the persons vested with the administration and representation of the foundation or association. This should be done by referring to the constitutive document. It is important to note that the PMLFTR do not require subject persons to verify the identity of the administrators but merely to identify them.

Another requirement under the PMLFTR is the establishment of the ownership and control structure of the foundation or association. In order to comply with such obligation subject persons should obtain and maintain on file an explanation of the ownership and control structure of the foundation or association from the applicant for business and verify such information by requesting the appropriate documentation. In the case of a foundation, subject persons are required to identify the founder, a person (other than the founder of the foundation) who has endowed the foundation, and, if any rights a founder of the foundation had in respect of the foundation and its assets have been assigned to some other person, that person.

In order for the subject person to undertake any business or provide any services to the applicant for business it must identify the class of persons in whose main interest the foundation or association is set up or operates (refer to Section 3.1.2.1). The subject person must also take all reasonable measures to ensure that the applicant for business keeps the subject person informed of any changes.

The procedure outlined above should apply in the same manner with respect to foundations or associations registered or established in Malta or in any other jurisdiction. However, subject persons should be aware that the type of documentation issued by the appropriate authorities may

vary between different countries. Therefore attention should be paid to the jurisdiction the documents originate from.

It is also important for subject persons to keep in mind that the systems in certain jurisdictions may be less transparent than in others and the documentation emanating from public authorities situated in such jurisdictions may not be sufficient to fulfil the identification and verification requirements laid out in the PMLFTR. Therefore subject persons should consider alternative ways of conducting their identification and verification procedures.

It should also be pointed out that any documentation obtained by the subject person which is in a language not understood by the subject person, should be translated. The translation should be dated, signed and certified by an independent person of proven competence, confirming that it is a faithful translation of the original.

3.1.3.6 When the principal is a trustee of a trust

Where the applicant for business is a trustee acting in the interest or for the benefit of a beneficiary of a trust, the subject person must apply a number of measures to verify and identify all the persons involved in the trust.

First, the subject person is required to identify and verify the identity of the trustee and the protector, where applicable, in accordance with Section 3.1.1.2. The subject person must then verify the existence of the trust and ascertain that the trustee/protector is acting for the trust.
In respect of trusts the subject person should obtain the following information:

(a) the full name of the trust;
(b) the nature and purpose of the trust; and
(c) the country of establishment.

This information should be obtained by requesting a copy of the trust deed from the trustee. In the event that the trustee is not able to provide the full copy of the trust deed, an authenticated relevant extract of the trust deed or a signed declaration by the trustee containing the information listed in (a) to (c) above would suffice.

The subject person may also consider obtaining a copy of the authorisation issued by the relevant authority for that person to act as a trustee. Alternatively, the subject person may obtain information from the website of the relevant authority and keep a record of such information.

In addition to the above procedures, the subject person shall not undertake any business with or provide any service to the trustee unless the trustee discloses the identity of the beneficial owners (refer to Section 3.1.2.1) and the identity of the trust settlor as well as producing the authenticated identification documentation of such persons. The subject person must take all reasonable measures to ensure that the trustee keeps the subject person informed of any changes in the beneficial ownership.

In the case where the beneficiaries of the trust have not yet been determined, the PMLFTR stipulate that the beneficial owners shall be the class of persons in whose main interest the trust is set up or

operates. In such a case, subject persons are merely required to verify that such class of persons is known (refer to Section 3.1.2.1(b)(ii)).

3.1.4 Information on the purpose and intended nature of the business relationship

Once the applicant for business and the beneficial owner(s), where applicable, have been identified and their identity verified, subject persons shall obtain information on the purpose and intended nature of the business relationship in order to be in a position to establish the business and risk profile of the applicant for business. This obligation does not apply in the context where the applicant for business seeks to carry out an occasional transaction.

Information that is relevant for this purpose should at least include the following:

(a) the nature and details of the business/occupation/employment of the applicant for business;
(b) the source(s) of wealth (refer to Section 3.1.6);
(c) the expected source and origin of the funds to be used in the business relationship (refer to Section 3.1.6); and
(d) the anticipated level and nature of the activity that is to be undertaken through the relationship.

Where the services of the subject person are being provided in relation to a business activity, the subject person should consider reviewing copies of recent and current financial statements, where applicable and on a risk-sensitive basis.

3.1.5 Ongoing monitoring of the business relationship

Subject persons are required to monitor the business relationships with their customers on an ongoing basis. Once the business profile of a customer has been established, ongoing monitoring enables subject persons to identify any unusual transactions which may involve ML/FT. This gives greater assurance that the activities of the subject person are not being misused for the purposes of ML/FT.

Ongoing monitoring of a business relationship includes:[39]

(a) the scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being undertaken are consistent with the subject person's knowledge of the customer, his business and risk profile, including where necessary, the source of funds; and
(b) ensuring that the documents, data or information held by the subject person are kept up to date.

Paragraph (a) above requires subject persons to collect the necessary information to ensure that the customer's business corresponds to the information disclosed by the customer at the beginning of the business relationship and that the business patterns of the customer are consistent with the risk profile established by the subject person. Where it is revealed that the customer's business and

[39] Regulation 7(2) of the PMLFTR.

risk profiles have significantly diverged from the established patterns or for no apparent economic or lawful purpose, action should be taken in accordance with the internal procedures of the subject person. This should be conducive to reviewing the risk profile of the customer and considering whether reporting is necessary in accordance with the procedures set out in Section 6.4.

Thus, as a result of the introduction of systems and procedures to ensure ongoing monitoring, activities which do not conform with the established business and risk profiles of the customer are immediately brought to the attention of the MLRO. The MLRO would then be in a position to assess whether there is a suspicion of ML/FT and whether that suspicion warrants a report to the FIAU in terms of Regulation 15 of the PMLFTR (refer to Section 6.4).

In order to fulfil the obligation set out in paragraph (b) above, subject persons are required to have a system in place to keep up-to-date documents, data or information held in the fulfilment of their CDD obligations, including information and documents obtained by the subject persons in order to fulfil the obligation set out under Regulation 7(1)(a)(b) and (c). This should include the updating of expired documentation mentioned under Section 3.1.1.2(ii)(a)(1). This ensures that in the event of an analysis or investigation of ML/FT the subject person is in a position to provide accurate and updated information to the FIAU or the Police.

The PMLTFR further require that in monitoring a business relationship subject persons should pay special attention to any large or complex transactions, including unusual patterns of transactions which have no apparent or visible economic or lawful purpose and business relationships and transactions with persons from a non-reputable jurisdiction (refer to Section 3.1.5.1 and Section 3.1.5.2 respectively).

3.1.5.1 Complex or large transactions

Regulation 15(1) requires subject persons to examine with special attention, and to the largest extent possible, the background and purpose of any complex or large transactions, including unusual patterns of transactions, which have no apparent economic or visible lawful purpose, and any other transactions which are particularly likely, by their nature, to be related to ML/FT.

This obligation requires subject persons to pay special attention to the following transactions:

(a) complex transactions that have no apparent economic or visible lawful purpose;
(b) large transactions that have no apparent economic or visible lawful purpose;
(c) unusual patterns of transactions that have no apparent economic or visible lawful purpose; and
(d) transactions which are particularly likely, by their nature, to be related to ML/FT.

Subject persons shall examine as far as possible the background and purpose of such transactions and establish their findings in writing. This requirement goes beyond the normal ongoing monitoring or the identification procedures of suspicious transactions. Subject persons are therefore required to also implement specific procedures for this purpose. The findings from the assessment of these transactions should serve as an additional element to be taken into consideration in assessing the customer's risk profile. The findings established by subject persons should not be automatically reported to the FIAU but should be made available to the FIAU and the

relevant supervisory authority if and when the subject person is requested to do so. However, in the event that the findings of the subject person indicate a suspicion or knowledge of ML/FT, a report should be filed with the FIAU in accordance with Section 6.4.

3.1.5.2 Business relationships and transactions with persons from a non-reputable jurisdiction

Subject persons shall pay special attention to business relationships and transactions with persons, companies and undertakings, including those carrying out relevant financial business or a relevant activity, from a jurisdiction that does not meet the criteria of a reputable jurisdiction (refer to Section 8.1). If those transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible, be examined, and written findings should be made available to the FIAU and to the relevant supervisory authority to the extent required by Section 3.1.5.1.

3.1.6 Source of wealth and source of funds

The **source of funds** is the activity, event, business, occupation or employment from which the funds used in a particular transaction are generated. On the other hand, **source of wealth** refers to the economic activity which generates the total net worth of the customer. 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 where 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 above.

Within the context of the ongoing monitoring of a business relationship subject persons are required to obtain information on the source of funds both at the establishment of the business relationship and on an ongoing basis thereafter. The subject person should not be satisfied with a generic description when questioning the customer about the origin of the funds used in the context of a business relationship. For instance, an explanation by the customer stating that the funds consist of the proceeds generated by a business would not be sufficient and the subject person is required to request the customer to provide more detailed information on the business concerned as well as producing documents, such as copies of invoices or contracts, to substantiate such explanation.

Depending on circumstances surrounding that transaction, the scrutiny of transactions may take place either in real time as the transaction is being carried out or after the event, through a review of the transactions or activities that the customer has carried out. Monitoring may be carried out in response to specific types of transactions, on the basis of the profile of the customer, through a comparison of the activities or the profile of the customer with that of a similar peer group of customers, or through a combination of these approaches.

It should be noted that notwithstanding the fact that the PMLFTR require subject persons to identify the source of funds within the context of a business relationship, subject persons should also consider ensuring that the source of funds utilised by the applicant for business to carry out an occasional transaction are also identified.

Irrespective of whether the transaction is carried out within an established business relationship or as an occasional transaction and regardless of any exemption or threshold, subject persons should invariably identify the source of funds when there is knowledge or suspicion that the applicant for business, or a person on whose behalf the applicant of business is acting, may have been, is, or may be engaged in ML/FT.

3.2 Timing of CDD procedures

This part of the Implementing Procedures deals with the various scenarios where the subject person is required to carry out CDD and specifies the moment in time when the CDD is to be carried out.

The PMLFTR require CDD measures to be applied in the following cases:[40]

- to all applicants for business when seeking to establish a business relationship;
- to existing customers when appropriate or when the subject person becomes aware that changes have occurred in the circumstances surrounding the established business relationship;
- to all applicants for business when seeking to carry out an occasional transaction;
- when the subject person suspects that a transaction may involve ML/FT; or
- when the subject person doubts the veracity or adequacy of previously obtained customer identification information, for the purpose of identification or verification.

3.2.1 Timing of CDD when establishing a business relationship

When an applicant for business seeks to establish a business relationship, subject persons are required to apply CDD procedures when contact is first made, as stated in Regulation 7(5) of the PMLFTR. In practice, requiring the applicant for business 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 instance, it would still be premature for the requirement of verification procedures to apply in the case of a preliminary business meeting or telephone call with a prospective customer for the purposes of exploring the legal position in Malta with a view of establishing a business relationship. However, the moment the prospective customer takes active steps that show that he intends to establish a business relationship, that subject person is required to complete the identification and verification procedures. In fact, during a preliminary meeting it may be advisable to inform prospective customers that in the event that a decision is taken to establish a business relationship, the prospective customer would be expected to provide the necessary CDD documentation immediately, prior to the establishment of that business relationship.

[40] Regulation 7(5) to (7) of the PMLFTR.

3.2.1.1 Exceptions when CDD may be carried out <u>after</u> 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 **during** the establishment of a business relationship where it is necessary for the continued normal conduct of business provided that:

(a) the risk of ML/FT is low; and provided further that
(b) the verification procedures be completed as soon as is reasonably practicable after the initial contact.[41]

This derogation from the general principle envisages those situations where it is impossible to require the completion of verification procedures before establishing a business relationship. In the event that CDD measures are applied after the establishment of a business relationship, subject persons should record the reasons for deferring the application of CDD measures. A determination on whether the risk of ML/FT is low should be based on the mandatory risk procedures described in Section 4.1.

(ii) Specific exceptions applicable in relation to life insurance business

Notwithstanding the general principle and the exception under paragraph (i) above, in relation to life insurance, subject persons carrying out any activity under paragraph (c) of the definition of 'relevant financial business' in the PMLFTR may complete the verification of the identity of the beneficiary under the policy after the establishment of a business relationship. Verification must however take place:

- at or before the time of payout; or
- at or before the time the beneficiary intends to exercise any of his rights vested under the policy.

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

Notwithstanding the general principle and the exception under paragraph (i) above, subject persons carrying on the business of banking or the business of electronic money institutions under the provisions of the Banking Act may open a bank account prior to the completion of the verification process. This exception is subject to the condition that adequate measures are put in place such that no transactions, apart from the initial transfer of funds to open the account, are to be carried out through the account until the verification procedures have been satisfactorily completed.

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

(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 and similar legal arrangements, where it is not possible to identify and verify the identity of the beneficiary at the time that contact is first made since such persons have not yet been named as a beneficiary or otherwise informed of the existence of the trust. In these cases, the PMLFTR provide that subject persons have to identify the class of persons in whose main interest the legal entity or arrangement is set up or operates. However, subject persons are required to identify and verify the identity of the beneficiaries as soon as they are named or otherwise informed of the existence of the trust.

3.2.2 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 and when the subject person becomes aware that changes have occurred in the circumstances surrounding the established business relationship.

Regulation 7(6) of the PMLFTR sets out an obligation on subject persons to review all customer files on a risk-sensitive basis upon the entry into force of the PMLFTR. Subject persons are allowed to do so "at appropriate times", meaning that the PMLFTR do not impose an obligation on subject persons to update all CDD documentation of all existing customers prior to 31st July 2008 when the PMLFTR came into force. However, since the PMLFTR require subject persons to update documentation of existing clients at appropriate times on a risk-sensitive basis, subject persons are required to update the documentation of customers posing a higher risk, determined on the basis of the subject persons' procedures for risk-assessment and risk-management referred to in Section 4.1, as soon as reasonably practicable. With respect to other customers, subject persons should update CDD documentation when certain trigger events occur, such as when an existing customer applies to open a new bank account or to establish a new relationship, or where an existing relationship changes. Moreover, it should be noted that ongoing monitoring obligations should assist subject persons in identifying the instances where additional or updated CDD documentation is needed.

Furthermore, if a lower risk customer wishes to acquire a high-risk product, his risk-profile will change accordingly. In such circumstances, the subject person would be required to obtain additional documentation or to update the CDD documentation maintained in relation to that customer to cater for the higher risk posed by the acquisition of a high-risk product.

3.2.3 Timing of CDD when an occasional transaction is carried out

As already stated in Section 3.2.1, the PMLFTR require the application of CDD measures when contact is first made between the subject person and the applicant for business. This time-frame also applies in the case of occasional transactions.

However, occasional transactions may vary in nature. For instance, in the case of an occasional transaction where the service is to be provided immediately, CDD documentation must be provided when contact is first made. This would apply for example in a case involving the transfer of money

through a money remittance provider. On the other hand, where an applicant for business merely seeks to obtain information from the subject person, such as for instance general information on the legal position in Malta with respect to a particular occasional transaction, the subject person would not be required to verify the identity of the applicant for business at that stage. Such obligation would only arise when the applicant for business actually takes active steps to engage the subject person to carry out the occasional transaction.

Subject persons are required to carry out CDD measures when a person knows or suspects that the applicant for business may have been, is, or may be engaged in ML/FT, or that the transaction is carried out on behalf of another person who may have been, is, or may be engaged in ML/FT, regardless of any exemption or threshold.

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

Subject persons must repeat CDD measures immediately when doubts have arisen regarding the veracity or adequacy of previously obtained customer identification information.

3.2.5 Acquisition of the business of one subject person by another

Where a subject person acquires the business of another subject person, in whole or in part, it is not necessary for all existing customers to be re-identified, 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 were in line with the provisions of the PMLFTR and the Implementing Procedures. In the event that the records of the customers are not all obtained or the procedures adopted by the previous subject person 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.

3.3 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), 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; or
(c) terminate the business relationship with the customer.

In addition to the action taken under paragraphs (a), (b) or (c) above the subject person shall consider filing a STR with the FIAU.

When a subject person is unable to complete the identification and verification procedures, before opting to apply one of the measures above, it should first consider whether the inability to complete such procedures is due to a deliberate avoidance or reluctance by the applicant for business to provide the necessary documents, data or information or simply because the required information does not exist, such as for instance in the case where a person does not have either an identity card, a passport or a driving licence. In the latter circumstances, subject persons should

obtain alternative documents which are sufficient for the applicant for business or the beneficial owner to be identified and for their identity to be verified in accordance with the PMLFTR. Such alternative documents may include documents obtained from a government or other official source, such as a public registry, which is vested with the powers to provide official information on the details of the identity of a person.

Moreover, in deciding whether to opt for one of the measures under paragraphs (a), (b) and (c) indicated above, the subject person should consider whether such action may frustrate efforts of an investigation of a suspected operation of ML/FT. In that event the subject person should carry on with the business and immediately inform the FIAU of the circumstances.

Where the subject person receives funds prior to the completion of verification measures in accordance with Section 3.2.1 and the subject person is unable to complete such verification measures or decides not to establish a business relationship with an applicant for business, the funds in question should only be released to the original remitter of the funds using the same financial channels through which the funds were delivered.

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 members of the accountancy profession, auditors, tax consultants, 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.

3.4 Simplified Due Diligence

Regulation 10 of the PMLFTR provides for the application of simplified due diligence. This Regulation states that CDD measures shall not be applied in certain specific circumstances mentioned in the Regulation itself. This means that in these specific circumstances, subject persons need not identify or verify the applicant for business or beneficial owner, need not obtain information relating to the purpose or intended nature of the business relationship and need not carry out ongoing monitoring of that relationship. Subject persons are only required to maintain a minimal amount of information about the applicant for business or the beneficial owner as explained hereunder.

3.4.1 Categories of applicants for business qualifying for SDD

In applying SDD in accordance with Regulation 10, subject persons are required to gather sufficient information to determine that the applicant for business falls within one of the following categories:

(a) Applicants for business, which are authorised to undertake relevant financial business, including regulated entities in the financial sector such as credit institutions, companies carrying on long-term insurance business, investment firms, etc. The rationale behind this provision is that such persons are subject to mandatory licensing and supervision and would have therefore gone through the 'fit and proper' test. This provision also

applies to applicants for business which are licensed or authorised to carry out activities equivalent to relevant financial business in another Member State of the European Community or in a reputable jurisdiction;

(b) Legal persons listed on a regulated market and which are subject to public disclosure requirements. These entities may either be authorised under the Financial Markets Act,[42] an equivalent regulated market within the Community, or in a reputable jurisdiction. Legal entities which are listed on a regulated market undergo a very rigorous listing procedure and are subject to public disclosure requirements;

(c) Beneficial owners of pooled accounts held by notaries or independent legal professionals. Since notaries and independent legal professionals are subject to AML/CFT measures they would have already carried out CDD measures in respect of the beneficial owners. Notaries and independent legal professionals falling within the scope of this provision are those members of these professions who are situated in Malta, in the Community or in a reputable jurisdiction. The notaries and independent legal professionals shall ensure that supporting identification documentation is available, or may be made available on request, to the credit institution that is acting as the depository of the pooled accounts;

(d) Certain domestic and foreign public authorities or bodies which fulfil all of the criteria set out in Regulation 10(1)(d)(i) to (iv);

(e) Legal persons who present a low risk of ML/FT, which fulfil the criteria set out in Regulation 10(2).

It should be noted that SDD may also be applied in those situations where the applicant for business is fully owned by a legal person falling within paragraphs (a) and (b) above and in such cases the subject person shall only gather sufficient information to determine that such legal person fully owns the applicant for business and that it qualifies under paragraphs (a) and (b).

The PMLFTR also provide an exhaustive list of products or transactions in respect of which SDD may be applied. The list includes certain insurance policies with one instalment premium or periodic payable premiums which do not exceed certain amounts; certain insurance policies in respect of pension schemes; pensions or similar retirement schemes to employees where contributions are made by way of deductions from an employee's wages and where the scheme prohibits members from assigning their interest under the scheme; electronic money products; and certain other product or transaction that represents a low risk of ML/FT which are specified in Regulation 10(3) and (4) of the PMLFTR.

3.4.2 Circumstances where SDD shall not apply

The PMLFTR prohibit the application of SDD where the subject person knows or suspects that the applicant for business may have been, is, or may be engaged in ML/FT, or that the transactions carried out on behalf of another person who may have been, is, or may be related to ML/FT. In such circumstances, even though the applicant for business or the product qualifies for SDD, the simplified procedure would not be able to be applied.

[42] Cap. 345 of the Laws of Malta.

Additionally, the PMLFTR state that notwithstanding the fact that an applicant for business or a product or transaction falls within one of the categories listed in Section 3.4.1, the subject person shall in any case pay special attention to the activities of that applicant for business or to any type of product or transaction that, by its nature, may be used or abused for ML/FT, and where there is information that suggests that this risk may not be low, the applicant for business or that product or related transactions shall not be considered as representing a low risk of ML/FT and SDD shall not be applied. In order to be able to adhere to the provisions of Regulation 10(6), subject persons should conduct periodic monitoring of the business relationship.

It should also be noted that the PMLFTR empower the FIAU, in collaboration with the relevant supervisory authorities, to determine that a particular jurisdiction does not meet the criteria of a reputable jurisdiction (refer to Section 8.1), where the circumstances so necessitate. In the event that such a determination is reached subject persons may be prohibited from applying the provisions dealing with SDD. Indeed, the FIAU has determined, by means of a guidance note which is contained within Appendix III, that certain categories of jurisdictions referred to in FATF public statements shall not be considered to be reputable thereby prohibiting subject persons from applying the provisions dealing with SDD in relation to the jurisdictions within these categories.

3.5 Enhanced Due Diligence

Subject persons must apply enhanced due diligence on a risk-sensitive basis in situations, which by their nature, represent a higher risk of ML/FT (refer to Section 4.1.1.2). 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 or transactions are better monitored and managed to avoid even inadvertent involvement in ML/FT. Whereas the PMLFTR provides for SDD measures to be applied on an optional basis, it is mandatory for EDD measures to be applied whenever there is a higher risk of ML/FT.

The PMLFTR refer to three specific types of relationships in respect of which EDD measures must necessarily be applied:

- where the applicant for business has not been physically present for identification purposes;
- in relation to cross-border correspondent banking relationships;
- in relation to a business relationship or occasional transaction with a PEP.

In addition to the three specific instances mentioned above, subject persons shall conduct EDD in relation to a business relationship or a transaction connected to a jurisdiction listed under the public documents issued by the FATF as required in the guidance note on high-risk and non-cooperative jurisdictions issued by the FIAU, which is contained within Appendix III. It should be noted that in the guidance note reference is also made to Regulation 15(3) of the PMLFTR which requires subject persons to inform the FIAU of any business relationships or transactions with persons, companies and undertakings, including those carrying out relevant financial business or a relevant activity from a non-reputable jurisdiction which continues not to apply measures equivalent to those laid down in the PMLFTR. In such cases the FIAU may, in collaboration with the relevant supervisory authority, require the subject person not to continue such business

relationship, not to undertake a transaction or to apply any other counter-measures as may be adequate under the circumstances. The guidance note links this requirement to those jurisdictions listed in the FATF public statement which have strategic AML/CFT deficiencies and to which counter-measures apply.

While the enhanced due diligence measures to be carried out in the three relationships mentioned above are specifically set out, the PMLFTR does not specify which enhanced due diligence measures are to be applied in other situations which, by their nature, can present a higher risk of ML/FT. Subject persons are therefore required to use their discretion in applying enhanced due diligence measures in such situations. However, it should be noted that such measures must be applied on a risk-sensitive basis and should be appropriate in view of the higher risk of ML/FT.

3.5.1 Non face-to-face applicants for business

Where the applicant for business has not been physically present for identification purposes, the subject person is not in a position to establish that the applicant for business is actually the person he purports to be without resorting to adequate measures to compensate for the higher risk. Therefore, in addition to the identification and verification of identity measures to be carried out in accordance with Section 3.1.1.2, subject persons are required to apply **one or more** of the following measures:

(a) *establish the identity of the applicant for business by using additional documentation and information*;

The applicant for business must provide the subject person with additional documentation containing identification details which would have been obtained by the applicant for business in the jurisdiction where he holds citizenship after producing an identification document containing a photograph. Alternatively, a bank reference may also be provided which confirms the identity details of the applicant for business. Where such additional documentation does not contain reference to the residential address of the applicant for business, a utility bill or a bank statement containing the residential address of the applicant for business should also be produced.

(b) *verify or certify the documentation supplied using supplementary measures;*

This measure consists in the certification of the documentation used for the purposes of the verification of identity by a legal professional, accountancy professional, a notary, a person undertaking relevant financial business or a person undertaking an activity equivalent to relevant financial business carried out in another jurisdiction.

Such certification should be evidenced by a written statement stating that:

- the document is a true copy of the original document;
- the document has been seen and verified by the certifier; and
- the photo is a true likeness of the applicant for business or the beneficial owner, as the case may be.

The certifier must sign and date the copy document (indicating his name clearly beneath the signature) and clearly indicate his profession, designation or capacity on it and provide his contact details. Where doubts have arisen about the existence of the certifier, subject persons should make independent checks to verify the existence of such certifier and document such checks.

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.

(c) *require certified confirmation of the documentation supplied by a person carrying out relevant financial business;*

Subject persons may consider alternative ways, other than the measures set out under paragraph (b) above, for the purposes of obtaining certification of the documentation provided by the applicant for business. In fact, under this paragraph the PMLFTR provide for the possibility of obtaining certified confirmation of the documentation by any entity carrying out relevant financial business.

Such certification should be evidenced by a written statement stating that:

- the document is a true copy of the original document;
- the document has been seen and verified by the certifier; and
- the photo is a true likeness of the applicant for business or the beneficial owner, as the case may be.

(d) *ensure that the first payment or transaction into the account is carried out through an account held by the applicant for business in his name with a credit institution authorised under the Banking Act*[43] *or otherwise authorised in another Member State of the Community or in a reputable jurisdiction*.

This is an important measure in the EDD process as it will entail a bank-to-bank transfer from an existing account through which the customer would have already been identified.

3.5.2 Correspondent banking relationships

The second instance specified in the PMLFTR where EDD should be applied refers to those circumstances where credit institutions seek to establish a cross-border correspondent banking, or other similar relationship, with respondent institutions situated in a country other than a Member State of the Community.[44]

Where a credit institution seeks to establish such correspondent banking relationship, in addition to the obligations set out under Regulation 7, it has to ensure that:

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

[44] For further guidance on the establishment and maintenance of correspondent banking relationships credit institutions may refer to the *Wolfsberg AML Principles for Correspondent Banking*.(http://www.wolfsberg-principles.com/corresp-banking.html).

(a) *it fully understands and documents the nature of the business activities of its respondent institution, including from publicly available information:*
   (1) the reputation of the institution;
   (2) the quality of supervision of that institution; and
   (3) whether that institution has been subject to a ML/FT investigation or regulatory measure.

Subject persons are not required to obtain information from private commercial sources but may make use of publicly available information to understand the nature of the business of the respondent institution.

(b) *it assesses the adequacy and effectiveness of the internal controls of the institution for the prevention of ML/FT;*

There are various measures which can be carried out to fulfil this requirement. These measures, which can either be applied independently of each other or cumulatively, are the following:

(1) The credit institution obtains a copy of the procedures manual of the respondent institution and assesses the adequacy and effectiveness of the respondent institution's internal controls on the basis of the measures set out in the PMLFTR; or
(2) The credit 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 credit 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;*

In accordance with preamble 26 of the 3rd AML Directive, the approval of senior management means approval by a person occupying the immediate higher level of the hierarchy of the person seeking such approval. The approval, therefore, need not necessarily be obtained from the board of directors, where applicable. However, it should be ensured that a request for approval is always made by a person occupying a managerial position within the structure of the subject person. The approval of senior management should be in writing and available for inspection.

(d) *it documents the respective responsibilities for the prevention of ML/FT;*

The credit institution seeking to establish the correspondent relationship 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 credit institution has verified the identity of and performed ongoing due diligence of the customers having direct access to the accounts of the respondent institution and that it is able to provide relevant CDD data upon request.*

Where accounts of a respondent institution can be used by third parties, credit institutions should either refuse to open such accounts due to the higher ML/FT risks posed or, if accepted, obtain written confirmation from the respondent institution that it will assume responsibilities for CDD on such persons. One way of ensuring that the measures required to be carried out in accordance with this obligation are being fulfilled by the respondent institution, is for the credit institution to carry out random and spontaneous checks.

Credit institutions are also prohibited from entering into, or continuing, correspondent banking relationships with shell banks. The PMLFTR require credit institutions to take appropriate measures to ensure that they do not enter into, or continue, a correspondent banking relationship with banks which are known to permit shell banks to use their accounts. In this regard, it is pertinent to keep in mind that credit institutions need to make adequate checks to assess the extent to which credit institutions with which a correspondent banking relationship is entered into, permit shell banks to use their account and maintain a record of such verifications.

3.5.3 Politically Exposed Persons

Subject persons are required to apply EDD measures to PEPs as defined in the PMLFTR.

3.5.3.1 Who qualifies as a PEP?

Regulation 2 defines a PEP as a natural person who is or has been entrusted with prominent public functions and includes his immediate family members or persons known to be close associates of such persons, but shall not include middle ranking or more junior officials. For the purposes of their customer acceptance process, subject persons are required to apply EDD in relation to PEPs residing in another Member State of the Community or in any other jurisdiction. Although the PMLFTR are clear regarding the application of EDD to PEPs, domestic persons who are or have been entrusted with prominent public functions may still pose a higher risk of ML/FT and subject persons should therefore consider applying EDD likewise to PEPs residing in Malta, even though this is not a mandatory requirement.

The term 'politically exposed persons' is broad and generally includes all persons who fulfil a prominent public function. In fact Regulation 11(7) states that a natural person who is or has been entrusted with a prominent public function shall include:

(a) Heads of State, Heads of Government, Ministers and Deputy and Assistant Ministers and Parliamentary Secretaries;
(b) Members of Parliament;

(c) Members of the Courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
(d) Members of courts of auditors, Audit Committees or of the boards of central banks;
(e) Ambassadors, *charge d'affaires* and other high ranking officers in the armed forces;
(f) Members of the administration, management or boards of State-owned corporations;

and where applicable, for the purposes of (a) to (e), shall include positions held at the Community or international level.

With respect to the term 'immediate family members' of PEPs, the PMLFTR provide that the term shall include:

(a) the spouse, or any partner recognised by national law as equivalent to the spouse;
(b) the children and their spouses or partners; and
(c) the parents.

With respect to the term 'persons known to be close associates', the PMLFTR provide that the term shall include:

(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 determining whether the applicant for business or a beneficial owner is a PEP, subject persons are required to obtain such information directly from the applicant for business. This information may be obtained from the applicant for business' response to a question posed in the application 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 and which would be required to be completed accordingly by the applicant for business and the beneficial owner, where applicable. This questionnaire should be signed by the applicant for business and the beneficial owner, where applicable. On the basis of the mandatory risk procedures referred to in Section 4.1, subject persons should determine whether the use of commercial databases to confirm the information provided by the applicant for business is necessary.

3.5.3.2 EDD measures to be applied in relation to PEPs

Subject persons are required to apply the following additional measures in relation to PEPs:

(a) *obtaining senior management approval;*

In accordance with preamble 26 of the 3rd AML Directive, the approval of senior management means approval by a person occupying the immediate higher level of the hierarchy of the person seeking such approval. The approval, therefore, need not necessarily be obtained from the board of directors, where applicable. However, it should be ensured that a request

for approval is always made by a person occupying a managerial position within the structure of the subject person. The approval of senior management should be in writing and available for inspection.

(b) *taking adequate measures to establish the source of wealth and funds involved:*

For further information reference should be made to Section 3.1.6.

(c) *conducting enhanced ongoing monitoring*.

Such monitoring should be conducted more regularly and more thoroughly, and a closer analysis should be undertaken on the transactions and their origin. For further information on ongoing monitoring reference should be made to Section 3.1.5.

3.5.4 New or developing technologies and products and transactions that might favour anonymity

Subject persons should pay special attention to any threat of ML/FT that may arise from new or developing technologies or from products or transactions that might favour anonymity, and take measures, if needed, to prevent their use in ML/FT. To this effect the mandatory risk procedures referred to in Section 4.1 should assist subject persons in identifying and establishing the extent of risk of ML/FT presented through technological innovations and products or transactions that might favour anonymity and to document findings and adopt measures to mitigate and contain such risk.

3.6 Reliance on other subject persons or third parties

The PMLFTR permit subject persons to rely on the CDD measures carried out by other subject persons or third parties, subject to a number of conditions.

3.6.1 CDD measures that may be relied on

Subject persons may only rely on CDD measures undertaken by other subject persons or third parties in relation to:

(a) the identification and verification of an applicant for business;
(b) the identification and verification of a beneficial owner, where applicable; and
(c) information on the purpose and intended nature of the business relationship.

It is very important to note that subject persons may not rely on the ongoing monitoring measures carried out by another subject person or third party.

The subject persons placing reliance should immediately obtain from the entity being relied on the information required under Regulation 7(1)(a) to (c). Therefore, notwithstanding the fact that the subject person is placing reliance on another entity, that subject person must obtain the details of the identity of the applicant for business, the identity of the beneficial owner, where applicable, and information on the purposes and intended nature of the business relationship.

Where reliance in accordance with Regulation 12 is being made, it is not necessary for the subject person placing reliance to receive copies of the identification and verification data and other relevant documentation obtained by the entity being relied on for the above-mentioned purposes, unless the subject person requests the entity being relied on to do so. Should the subject person require such documentation it must be forwarded by the entity being relied on immediately upon request.

In order to ensure that such documentation is available upon request, the subject person placing reliance and the entity being relied on should have a written agreement in place which regulates the procedure to be followed in such circumstances. Such an agreement should not necessarily be reduced into a detailed formal agreement but an exchange of letters would suffice. Subject persons should consider making occasional tests of the system to ensure that the entity being relied upon would provide the necessary documentation if a request is made and that it would adhere to the requirement of the immediacy stipulated in the PMLFTR.

The provisions under Regulation 12 dealing with reliance do not apply where the applicant for business involved falls within any one of the categories which qualify for the application of SDD.

3.6.2 Who qualifies as a third party?

The PMLFTR define a third party as a person:

(a) carrying out activities which are equivalent to 'relevant financial business' or 'relevant activity' in a Member State of the Community other than Malta or in a reputable jurisdiction (refer to Section 8.1); and

(b) subject to authorisation or to mandatory professional registration recognised by law.

The two criteria mentioned above are cumulative and therefore in order for reliance to be allowed it is necessary for both criteria to be satisfied.

3.6.3 Responsibility for compliance with CDD measures

Notwithstanding the fact that it is possible for a subject person to rely on another subject person or a third party, the subject person placing reliance remains responsible for compliance with CDD requirements referred to in Section 3.6.1.

Additionally, the subject person relying on another subject person or a third party is still required to carry out a risk-assessment (refer to Section 4.1.1) of the applicant for business or the beneficial owner, whenever applicable. In fact, the subject person must be in a position to determine whether the applicant for business or the beneficial owner falls within the risk appetite of the subject person and whether the application of customer EDD is necessary in accordance with Section 3.5.

3.6.4 Reliance on persons carrying on relevant financial business or equivalent activities

All subject persons may rely on other subject persons carrying on activities falling under the definition of relevant financial business.

Additionally, all 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 in Section 3.6.2, carrying on activities equivalent to those falling within the scope of 'relevant financial business', even if the documentation or data upon which these requirements have been based are different to those under domestic requirements.

3.6.4.1 Exception

Financial institutions whose main business is currency exchange or money transmission or remittance services or their equivalent, may only be relied upon in limited circumstances in accordance with Section 3.6.5 below.

3.6.5 Reliance on third parties carrying out currency exchange and money transmission/remittance services

Subject persons whose main business is currency exchange or money transmission or remittance services may recognise and accept the outcome of the relevant CDD measures carried out in accordance with provisions equivalent to the PMLFTR by third parties who undertake currency exchange or money transmission or remittance services, even if the documentation or data upon which these requirements have been based are different to those under domestic requirements.

3.6.6 Reliance on auditors, external accountants, tax advisors, notaries, independent legal professionals, trustees and other fiduciaries

All subject persons may rely on auditors, external accountants, tax advisors, notaries, independent legal professionals, trustees and other fiduciaries, when these are subject to the PMLFTR.

3.6.7 Reliance on third parties carrying out activities equivalent to those referred to in Section 3.6.6

Only auditors, external accountants, tax advisors, notaries, independent legal professionals, trustees and other fiduciaries when these are subject to the PMLFTR, may recognise and accept the outcome of the requirements referred to in Section 3.6.1, when such requirements are carried out by third parties who undertake activities equivalent to those referred to in Section 3.6.6 in accordance with provisions equivalent to the PMLFTR even if the documentation or data upon which these requirements have been based are different to those under domestic requirements. This means that only these categories of subject persons, in terms of the PMLFTR, may rely on their counterparts situated in third countries.

3.6.8 When reliance is not applicable

The provisions of reliance in the PMLFTR shall not apply:

(i) 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, such as

for instance agents of financial institutions as defined under the Financial Institutions Act.[45] This provision does not refer to outsourcing of CDD measures but to the outsourcing of certain operational activities of the subject person. In such a case, for the purposes of CDD, the outsourced entity would be regarded as part of the subject person and would not be required to carry out CDD measures separately. Therefore, the provisions of reliance would not apply in any case;

(ii) to reliance on subject persons under paragraph (i) in the definition of 'relevant activity' and subject persons under paragraph (j) in the definition of 'relevant financial business' in Regulation 2(1). These two paragraphs refer to any activity which is associated with an activity falling within the definition of relevant activity and relevant financial business.

3.6.9 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 'reputable jurisdiction' subject persons should refer to Section 8.1. Additionally, it is to be noted that the FIAU has determined, by means of a guidance note which is contained within Appendix III, that certain categories of jurisdictions referred to in FATF public statements shall not be considered to be reputable thereby prohibiting subject persons from relying on persons or institutions from the jurisdictions within these categories.

[45] Cap, 376 of the Laws of Malta.

CHAPTER 4 – MANDATORY RISK PROCEDURES AND THE RISK-BASED APPROACH

4.1 Mandatory risk procedures

Subject persons are required to have in place procedures to manage the ML/FT risks posed by their customers,[46] products and services. This requirement is found under Regulation 4(1)(c) which stipulates that subject persons are to establish procedures on, *inter alia*, **risk assessment** and **risk management** that are adequate and appropriate to prevent the carrying out of operations that may be related to ML/FT.

The risk-assessment and risk-management procedures should be contained in the procedures manual of the subject person referred to in Section 8.3.

4.1.1 Risk-assessment procedures

Risk-assessment procedures which are adequate and appropriate to prevent ML/FT should at least include identification and assessment of customer risk, product/service risk, interface risk and geographical risk, in accordance with Section 4.1.1.2 below, in relation to every business relationship or occasional transaction.

4.1.1.1 Purpose of risk-assessment procedures

The purpose of the risk-assessment procedures is to enable the subject person to be in a position to identify and assess the ML/FT risks that the subject person is or may become exposed to and thereby determine:

(a) whether the application of EDD in accordance with Section 3.5 is necessary;
(b) the point in time when the application of CDD in accordance with the PMLFTR to existing customers is to be carried out (for further details refer to Section 3.2.2); and
(c) whether a customer presents a low risk of ML/FT for the purposes of Section 3.2.1.1.(i), where applicable.

With respect to paragraph (a) above, Regulation 7(9) specifically requires subject persons to develop and establish effective customer acceptance policies to determine whether an applicant for business or a beneficial owner is a politically exposed person or is likely to pose a higher risk of ML/FT. A customer acceptance policy therefore, as a minimum, should include:

(a) a description of the type of customer that is likely to pose higher than average risk;
(b) the identification of risk indicators such as the customer background, country of origin, business activities, products, linked accounts or activities and public or other high profile positions, which should be carried out in accordance with Section 4.1.1.2 below; and

[46] For the purposes of Chapter 4 the term 'customer' shall be construed to include both the applicant for business and the beneficial owner, whenever applicable.

(c) the requirement for the application of EDD measures for higher risk customers and in the case of PEPs the measures set out in Section 3.5.3.

4.1.1.2 Identifying and assessing the risks

Notwithstanding the fact that there is no established set of risk categories, it is suggested that the four main risk areas which the subject person should take into consideration when identifying and assessing its ML/FT risks, should be:

(i) customer risk;
(ii) product/service risk;
(iii) interface risk;
(iv) geographical risk.

(i) Customer risk

The risk of ML/FT may vary in accordance with the type of customer. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. For instance, the risks posed by a pensioner, whose only source of income is his monthly pension, are much lower than the risks posed by a person whose transactions are mainly cash-based with no discernable source of his activity or a person whose commercial operations comprise complex business structures.

With respect to legal entities, subject persons should be aware that corporate structures, trusts, foundations, associations and commercial partnerships may be used as a vehicle to obscure the link between a criminal activity and the persons benefitting from the proceeds of such criminal activity.

The FATF[47] provides a list of categories of customers whose activities may pose a higher risk. This list includes:

- Customers conducting their business relationship or transactions in unusual circumstances, such as:
  - significant or unexplained geographical distance between the entity and the location of the customer.
  - frequent and unexplained movement of accounts to different entities.
  - frequent and unexplained movement of funds between entities in various geographical locations.
- Customers where the structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interests.
- Cash (and cash equivalent) intensive business.
- Charities and other 'not for profit' organisations which are not subject to monitoring or supervision (especially those operating on a 'cross-border' basis).
- Use of intermediaries within the relationship who are not subject to adequate AML/CFT laws and measures and who are not adequately supervised.
- Customers that are politically exposed persons.

[47] FATF, *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing – High Level Principles and Procedures*, June 2007 (hereinafter referred to as 'FATF RBA Guidance'), pp. 23-24, paragraph 3.6.

In determining the risk that a customer poses, subject persons should also be aware of the customer's behaviour. The following situations should be taken into consideration:

- Situations where there is no commercial rationale for the customer buying the product he seeks;
- Requests for a complex or unusually large transaction which has no apparent economic or lawful purpose;
- Requests to associate undue levels of secrecy with a transaction;
- Situations where the origin of wealth and/or source of funds cannot be easily verified or where the audit trail has been deliberately broken and/or unnecessarily layered; and
- The unwillingness of customers who are not private individuals to give the names of their real owners and controllers.[48]

Irrespective of all the above considerations, a customer should automatically be classified as a high-risk customer if he is subject to sanctions or other economic measures. In this case subject persons should exercise caution in providing certain services depending on the measures that the person is subject to, especially where the risk of ML/FT is higher. In this respect subject persons should consult a number of open sources, including the sources listed in Appendix I and any commercial databases to which the subject person may choose to subscribe.

(ii) Product/service risk

Some products/services are inherently more risky than others and are therefore more attractive to criminals. The FATF[49] lists a number of factors which should be taken into consideration when determining the risks of products and services:

- Services identified by competent authorities or other credible sources, such as the FATF itself, FSRBs, the International Monetary Fund, the World Bank and the Egmont Group,[50] as being potentially higher risk, including the following examples:
  - International correspondent banking services involving transactions such as commercial payments for non-customers (for example, acting as an intermediary bank) and pouch activities.
  - International private banking services.
- Services involving banknote and precious metal trading and delivery.
- Services that inherently provide more anonymity or can readily cross international borders, such as online banking (where the client is not present for identification and verification purposes), stored value cards, international wire transfers, private investment companies and trusts.

(iii) Interface risk

The channels through which a subject person establishes a business relationship and through which transactions are carried out may also have a bearing on the risk profile of a business relationship or

[48] This part of the Implementing Procedures is based on Chapter 4 of JMLSG Guidance.
[49] FATF RBA Guidance, p. 24, paragraph 3.7.
[50] The information provided by these entities does not have the effect of law and should not be viewed as an automatic determination that a particular factor on its own poses a higher risk of ML/FT.

a transaction. It is recognised that the use of internet for the provision of services may exacerbate the risk of ML/FT, in view of the rapidity with which online transactions may be conducted and the level of anonymity that such transactions may offer.

(iv) Geographical risk

The geographical risk is the risk posed to the subject person by the geographical location of the business/economic activity and the source of wealth/funds of the business relationship.

The FATF[51] lists a number of factors that should be assessed in determining when a country poses a higher risk. These include:

- Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations Security Council.[52] In addition, in some circumstances, countries subject to sanctions or measures which may not be universally recognised may be given credence by the subject person because of the standing of the issuer and the nature of the measures.
- Countries identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures.
- Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them.
- Countries identified by credible sources as having significant levels of corruption, or other criminal activity.

In this context reference should be made to the notion of 'reputable jurisdictions' explained in Section 8.1.

4.1.2 Risk-management procedures

Risk-management procedures should be introduced to control and mitigate higher risk situations. These procedures should, as a minimum, provide for the following measures:

(a) the implementation of a programme which sets out the additional measures to be applied by the subject person in higher risk situations;
(b) requiring a higher standard in relation to the quality of documents obtained; and
(c) monitoring transactions/activities to a higher degree where the risk warrants such additional measures.

4.2 The Risk-Based Approach

While the risk-assessment and risk-management procedures specified in Section 4.1 above are mandatory, the application of a RBA is optional. The possibility for the application of the RBA is laid out in Regulation 7(8) of the PMLFTR which stipulates that subject persons may determine the extent of the application of CDD requirements on a risk-sensitive basis, depending on the type of

[51] FATF RBA Guidance, p. 23, paragraph 3.5.
[52] Reference should also be made to sanctions, embargoes or similar measures issued by the EU.

customer, business relationship, product or transaction. The possibility to apply different measures on the basis of the particular ML/FT risks is a novel concept within the ambit of AML/CFT which was introduced by virtue of the 3rd AML Directive.

4.2.1 The purpose of the RBA

The principle behind the RBA is that resources should be directed proportionately in accordance with the extent of the ML/FT risks posed, so that the business, products and customers posing the highest risks receive the highest attention. Prior to the introduction of the RBA, subject persons were required to manage and control their risks solely on the basis of a rules-based approach. Such an approach meant that subject persons applied their resources evenly, so that all customers, products, etc, received equal attention. Such an approach may still be applied, in view of the fact that the RBA is not mandatory. However, while the application of the rules-based approach may lead to a 'tick box' approach with the focus being placed on meeting regulatory needs rather than on effectively combating ML/FT, the application of a risk-based approach ensures that measures to prevent or mitigate ML/FT are commensurate with the risks identified and that resources are allocated in the most efficient ways.[53]

Subject persons should be aware that where a decision to apply the RBA is taken, a framework should be implemented. The model[54] to be adopted to implement such framework may be simple or sophisticated depending on the size and nature of the business and services offered, the customer base and the geographical area of operation of the subject person. The implementation of the RBA, therefore, need not involve a complex set of procedures, provided that the procedures in place are based on a set of objective criteria.

An effective RBA involves the identification, recognition, assessment, categorisation and ranking of ML/FT risks and the establishment of reasonable controls for the prevention and management of such risks. The subject person should be able to show that reasonable business judgement has been exercised with respect to its customers and the determinations reached in the application of the RBA are justified in the light of the ML/FT risks identified. In fact, Regulation 7(8) states that subject persons may apply a RBA provided that they are **able to demonstrate that the extent of the application on a risk-sensitive basis is appropriate in view of the risks of ML/FT**.

The identification and assessment of risks is an ongoing procedure, since risks change over time depending on how circumstances develop and how threats evolve. Once the subject person has a clear understanding of the ML/FT risks that are a threat to the organisation, the subject person should then develop strategies to manage and mitigate those risks.

[53] FATF RBA Guidance, p. 2, paragraph 1.7.

[54] The term "model" when used in this paragraph should in no way be construed to mean that a sophisticated approach, such as the building of a matrix, is necessary in all circumstances. At times, where the size and nature of the business so warrant, a simple procedure commensurate to that business, capable of, as a minimum, enabling the identification of higher risk customers, would suffice.

Before going into a detailed explanation on the application of a risk-based approach, it is important to point out that the rationale behind the RBA is not to exempt subject persons from CDD measures where the risk of ML/FT is low, but rather to provide subject persons with the possibility to vary the extent of the application of CDD measures depending on the level of risks identified. The CDD process comprises a number of steps that need to be taken in all cases – identification and verification of identity of customers and beneficial owners, obtaining information on the purposes and intended nature of the business relationships and conducting ongoing monitoring. All of these steps which make up the CDD process must be completed regardless of the RBA. However, within the conduct of each and every one of these steps, the implementation of the RBA may allow for a determination of the extent and quantity of information required and the mechanisms to be used to meet the minimum standards set out in the PMLFTR.

Finally, it should be clear that the manner in which the RBA is applied by subject persons should not be designed in a way that it simply prohibits subject persons from undertaking certain transactions or establishing certain business relationships with potential customers, but it is expected to assist subject persons in managing potential ML/FT risks in an effective manner. Nevertheless, it is recognised that regardless of the strength and effectiveness of AML/CFT controls, criminals will continue to attempt to move illicit funds through the financial sector undetected and will, from time to time, succeed. This factor will be taken into account by the FIAU when assessing subject persons' compliance with the PMLFTR.[55]

4.2.2 The application of the RBA

As mentioned earlier, the application of the RBA entails the implementation of a framework. This framework consists of a number of steps:

(a) identifying and assessing risks;
(b) managing and controlling risks;
(c) monitoring controls; and
(d) recording the actions taken.

The manner in which these steps are to be applied shall depend on the circumstances of each individual subject person.

4.2.2.1 Identifying and assessing the risks

The first step in the application of the RBA is the identification and assessment of ML/FT risks, which is a mandatory procedure required by the PMLFTR. Reference should be made to Section 4.1.1.2 above for detailed information on the manner in which such procedure should be implemented.

[55] FATF RBA Guidance, p. 2-3, paragraph 1.12 and 1.13.

In the RBA, the four risk elements in Section 4.1.1.2 should be combined to produce a risk profile of the applicant for business or the beneficial owner. It is the result of the risk profile and the subject person's risk appetite that will determine the extent and the intensity of the documentation and other processes that will need to be fulfilled at the commencement of a business relationship or as an ongoing requirement.

While a risk assessment should always be performed at the inception of a business relationship, a comprehensive risk profile may only become evident once the customer has begun his planned operations or has begun transacting through an account, depending on the type of business, making monitoring of customer transactions and ongoing reviews of the activities of the customer a fundamental component of a risk-based approach.[56]

4.2.2.2 Obtaining a risk profile

Once the subject person has identified and assessed the particular risks of a prospective business relationship, such information should be collated so as to obtain a risk profile which will determine whether the prospective business relationship falls within the risk appetite of the subject person. There is no one single accepted methodology that should be applied to the risk categories discussed above. The following is an example of a methodology that may be used in practice. This methodology is merely being provided as a guide, it is not exhaustive and consequently should not be considered to be mandatory.

The methodology that is being provided is based on a scoring system. The different risk variables within each of the four risk categories outlined above 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.

[56] FATF RBA Guidance p. 22, paragraph 3.2.

Table 2 below illustrates how this system might work in practice.

	Scoring	Type of Customer	Product/ Service	Interface	Geographical
EXTREME	**9 – 10**	• PEPs • Sanctioned individuals or entities	• Services intended to render the customer anonymous	• Internet transactions	• Country subject to sanctions, embargoes
HIGH	**6 – 8**	• Non face-to-face • NPOs • Correspondent bank • Fiduciary arrangements	• Internet-based product • Services identified by FATF	• Internet transactions	• Non-reputable jurisdiction
MEDIUM	**3 – 5**	• Employees • Public figures • General public	• Normal products	• Non face-to-face	• Reputable jurisdiction • Equivalent country • Domestic
LOW	**1 – 2**	• Other individuals (e.g. pensioners)	• None	• Face-to-face	• EU Member State • Domestic

Table 2 – Risk scoring grid

Once the subject person establishes the risk scoring, the subject person should determine the extent of risk which the organisation is ready to take on in relation to every risk element. These four risk elements could then be combined to obtain a graphic representation of the risk appetite of the organisation, as in Figure 3 below. ***It should be noted that subject persons should have on record evidence to substantiate the criteria adopted to determine the risk appetite. This would be assessed by the FIAU in fulfilment of its compliance monitoring function.***

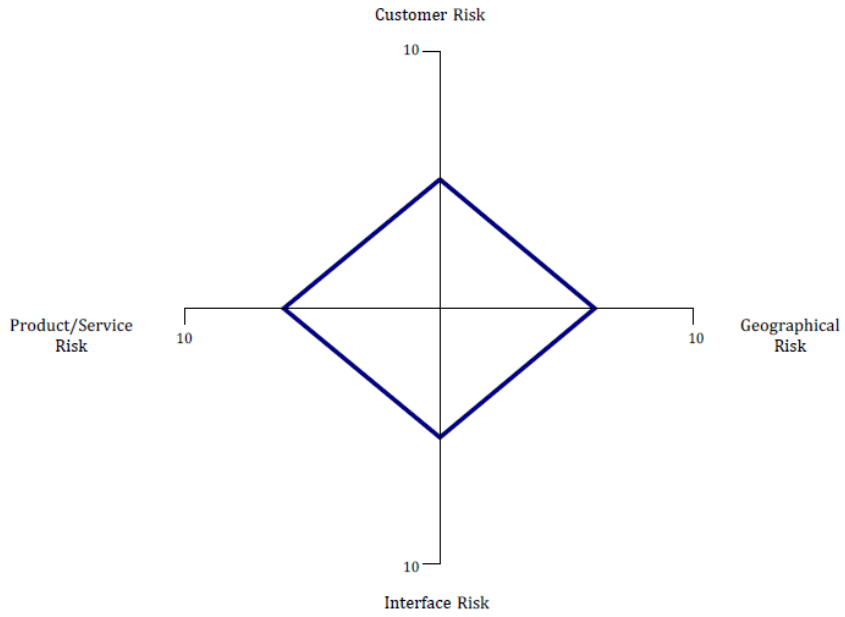

Figure 3 – Determination of risk appetite of the subject person

Once the risk appetite of the organisation is established, a risk rating of the prospective individual customer on the basis of the four risk categories should be conducted. Once the four risk elements are combined they shall provide the subject person with a risk profile for that prospective business relationship. The risk profile which is then obtained shall be viewed against the risk appetite of the subject person to determine the risk posed by the customer to the organisation – including whether to accept or refuse that business relationship.

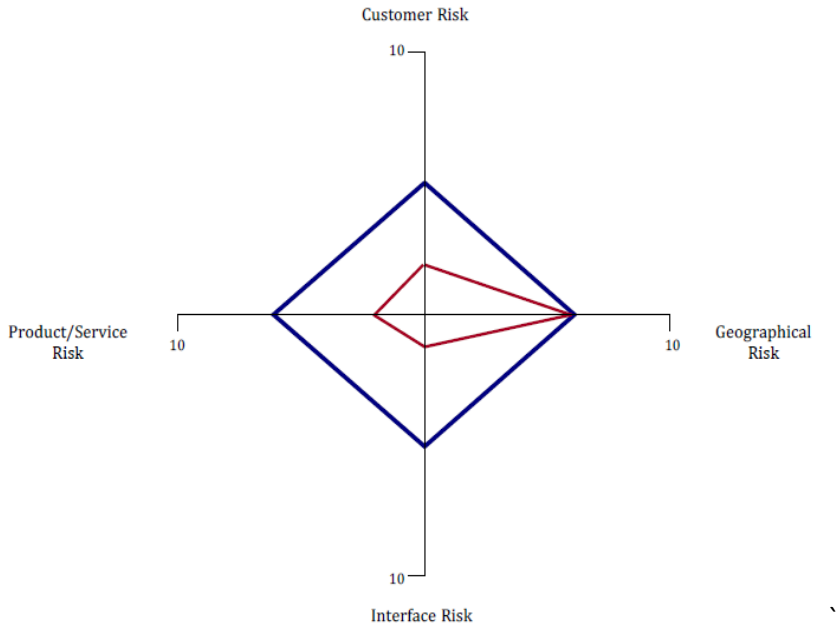

Figure 4 – Customer falling within the risk appetite of the subject person

Figure 4 above shows a graphic representation of a customer falling within the risk appetite of the subject person - in which case the subject person could accept the customer.

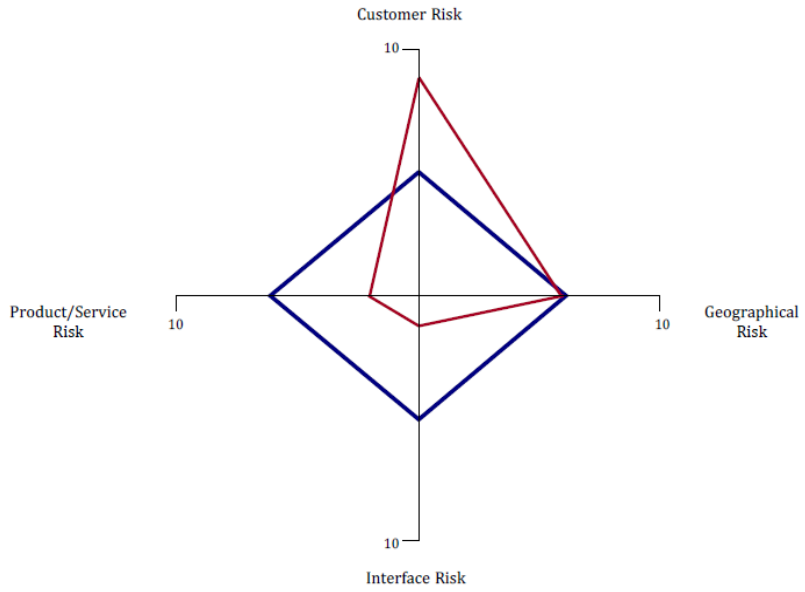

Figure 5 – Customer falling outside the risk appetite of the subject person

In Figure 5 above the customer falls outside the subject person's risk appetite. The customer would be considered as posing a higher risk to the institution and therefore could be accepted under higher monitoring or refused outrightly.

It is important to note that irrespective of whether the subject person has a high risk appetite, all high-risk customers must be subject to the application of enhanced due diligence measures. For instance, all non face-to-face customers and PEPs are considered to pose a higher risk of ML/FT and automatically require the application of enhanced due diligence. However, the extent of the enhanced due diligence measures to be applied may vary depending on the risks posed by each customer. Therefore, subject persons should ensure that the enhanced due diligence measures carried out in relation to, for instance, a high-net worth individual operating from a non-reputable jurisdiction on a non face-to-face basis should be much more stringent than the enhanced due diligence measures applied in relation to a student operating on a non face-to face basis.

4.2.2.3 Managing and controlling risks

Once the subject person has identified and assessed the risks and obtained a risk profile of the prospective business relationship, controls to manage and mitigate the risks must be devised and implemented. As a minimum these controls should include:[57]

(a) implementing a customer identification programme that varies the procedures in respect of customers in accordance with the identified and assessed ML/FT risks;

(b) requiring adequate standards in relation to the quality of documentary evidence obtained;

[57] This part of the Implementing Procedures is based on Chapter 4 of the JMLSG Guidance.

(c) obtaining additional information in accordance with the identified and assessed ML/FT risks; and
(d) adopting the extent of monitoring customer transactions/activities depending on the outcome of the risk assessment.

A customer identification programme should at least involve:[58]

(a) a standard information dataset, which may include a factsheet, to be held in respect of all customers;
(b) standard verification requirements for all customers;
(c) the possibility to apply more extensive due diligence on customer acceptance for higher-risk customers;
(d) the possibility to apply, where appropriate, more limited identity verification measures for specific lower risk customer/product combinations; and
(e) an approach to monitoring customer activities and transactions that reflects the risk assessed to be presented by the customer, which will identify those transactions or activities that may be unusual or suspicious.

It should be pointed out that identifying a customer as posing a higher risk of ML/FT does not automatically mean that such customer is a money launderer or a terrorist financier. Similarly, the fact that a customer is identified as presenting a low risk of ML/FT does not exclude the possibility that such customer may attempt to launder money or fund terrorism. In view of this, the risk-based criteria should not be applied rigidly without allowing past experience and available information to be taken into consideration in reaching a determination.[59]

4.2.2.4 Monitoring controls

It is essential that the controls to manage and mitigate the identified risks are constantly monitored. This should be done so that in the event of a change in circumstances, which might mitigate or exacerbate a particular risk, the respective control is modified accordingly.

For instance it is important that the subject person has a system in place to identify changes in customer characteristics, as this would obviously have a bearing on the risk profile of the customer. Similarly, the threat posed by a particular product or service may cease to exist which would lead to a re-consideration of the risk scoring of the business relationship. In view of this, the subject person must be in a position to identify such changes.

Subject persons should also carry out periodic internal audits or assessments to review the adequacy of the risk assessment, the internal controls and the compliance arrangements. Such audits or assessments should also review the effectiveness of liaison between the different departments of the organisation, and the effectiveness of the balance between technology-based and people-based systems.

[58] FATF RBA Guidance p. 38, paragraph 4.23.
[59] FATF RBA Guidance p. 38, paragraph 4.27.

4.2.2.5 Recording the action taken

As stated above, in applying a RBA, subject persons should be in a position to demonstrate to the FIAU that the measures adopted are appropriate in view of the ML/FT risks that the subject person may be or become exposed to. Therefore, it is of utmost importance that every determination and assessment taken in identifying, assessing, managing and mitigating risks, as well as the monitoring of such processes is duly recorded in writing. This will enable the subject person to support the procedures undertaken when an inspection is carried out by the FIAU or the relevant supervisory authority acting on its behalf.

CHAPTER 5 – RECORD KEEPING PROCEDURES

5.1 Purpose of keeping records

Subject persons shall retain records, including documentation and information, for use in an investigation into, or an analysis of, the possibility of ML/FT. These records can be requested by the FIAU or by other relevant competent authorities as required.

The records maintained by subject persons are extremely relevant to competent authorities responsible for analysis, investigation, law enforcement and prosecution since they may constitute evidence of the audit trail and of money flows. It is therefore crucial that subject persons adhere to the legal obligations applicable in this area.

5.2 Records to be retained

Subject persons should have procedures in place to ensure that the following records are maintained in relation to all business relationships formed and occasional transactions carried out:

(a) records indicating the nature of the evidence of the CDD documents required and obtained, which should include either a copy of the evidence required for the identity or a reference to the evidence required for identity. Such reference should provide sufficient information to enable the details as to a person's identity contained in the relevant evidence to be re-obtained. The records to be maintained should include the following:

- Where subject persons view the original CDD documents listed in Section 3.1.1.2(ii)(a)(1) and (2), a true copy of such original documents on file, signed and dated by an officer of the subject person should be maintained;
- Where subject persons receive a certified copy of the CDD documents listed in Section 3.1.1.2(ii)(a)(1) and (2), such copy should be maintained on file;
- Where subject persons verify the identity of the applicant for business by electronic means in accordance with Section 3.1.1.2(ii)(b), a print-out of the results of the search should be maintained on file;
- Where it is impossible for subject persons to take a copy of the documents listed in Section 3.1.1.2(ii)(a)(1) a record should be maintained of the type of document and its number, date and place of issue so that if necessary the document may be re-obtained from its source of issue. A record of the reasons for the impossibility to take a copy of the documents should be recorded;
- Where the verification of the residential address of the subject person is carried out by visiting the customer at such address, a record of the visit should be maintained on file;
- Where verification is carried out on the basis of alternative documents referred to in Section 3.3, a copy of such documents should be maintained on file;
- The documentation and other information obtained in fulfilment of the obligations set out in Sections 3.1.3.1 to 3.1.3.6, Section 3.4.1 and Sections 3.5.1 to 3.5.3 should be maintained on file.

(b) records containing details relating to the business relationship and all transactions carried out in the course of an established business relationship or occasional transaction. These records should include the following:

- files related to accounts held by the subject person, where applicable, and all business correspondence of the subject person in the course of an established business relationship; and
- details on all transactions, whether international or domestic, carried out by the customers. The details should include the customer's and beneficiary's name, address or other identifying information normally recorded by the subject person, the nature and date of the transaction, the type and amount of currency involved, the type and identifying number of any account involved in the transaction, the volume of funds flowing through the account, the origin of the funds, where necessary and the form in which the funds were placed or withdrawn.[60]

Such records should either consist of original documents or else copies which are admissible in court proceedings.

(c) records of the findings of the examination of the background and purpose of the relationship and transactions carried out in accordance with Regulation 15(1) and (2) of the PMLFTR (refer to Sections 3.1.5.1 and 3.1.5.2).

Subject persons should also retain the following records required as evidence of compliance with the PMLFTR and for statistical purposes:

- internal reports made to the MLRO;
- reports made by the subject person to the FIAU;
- a record of the reasons for not forwarding an internal report to the FIAU;
- a record of AML/CFT training provided, including:
  - the date on which the training was delivered;
  - the nature of the training;
  - the names of employees receiving the training;
  - the results of any assessment undertaken by employees;
  - a copy of any handouts or slides;
- other important records, including:
  - any reports by the MLRO 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;
  - the section of reports drawn up in relation to an internal audit or assessment dealing with AML/CFT issues.

[60] These requirements only apply to those subject persons who carry out transactions in the course of their business.

5.3 Period of retention of records

Subject persons shall maintain the records, referred to in Section 5.2, for a period of at least five (5) years. The date of commencement of this time period depends on the type of records to be retained.

5.3.1 CDD documentation

With respect to CDD documentation referred to in Section 5.2(a), the time period of five (5) years commences from the date on which the business relationship is terminated or the occasional transaction is carried out. This date varies depending on the following circumstances:

- *Where negotiations take place between the parties with a view to the formation of a business relationship between them:* The date of ending of such business relationship;
- *Where there is knowledge or suspicion that the applicant for business may have been, is or may be engaged in ML/FT or that the transaction is carried out on behalf of another person who may have been, is, or may be engaged in ML/FT:* The date when the suspicious transaction was reported. However, this five (5) year period may be extended by the FIAU as may be required;
- *Single Large Transaction as defined under the definition of 'Case 3' of the PMLFTR:* The date of carrying out the occasional transaction;
- *Series of Transactions as defined under the definition of 'Case 4' of the PMLFTR:* The date of carrying out the last transaction in a series of transactions.

Where the formalities necessary to end a business relationship have not been observed but the five (5) year period has elapsed since the date on which the last transaction was carried out, then the date of that transaction shall be deemed to be the date on which the business relationship was effectively completed, provided that the business relationship is then immediately terminated in a formal manner. Should the business relationship not be terminated formally as required above the subject person shall be required to maintain the records beyond the five-year period from the date of the last transaction.

5.3.2 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

The time period for the retention of documentation referred to in Section 5.2(b) 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.

Where a suspicious transaction report has been filed with the FIAU, transaction records related to that suspicious transaction should be retained for a period of five (5) years from the date of the

filing of the report, irrespective of whether the transaction is carried out within the context of an established business relationship or as an occasional transaction.

5.3.3 Records of the findings of the examination of the background and purpose of the relationship and transactions carried out in accordance with Regulation 15(1) and (2) of the PMLFTR

The time period for the retention of the findings of the examination of the background and purpose of the relationship and transactions carried out in accordance with Regulation 15(1) and (2) of the PMLFTR, commences from the date on which all dealings taking place in the course of the transaction in question were completed.

5.4 Form of records

There are certain specific instances set out in the Implementing Procedures which require subject persons to keep a hard copy of the documents on file. In all other cases subject persons may maintain their records in any one of the following forms:

- in physical files;
- in scanned form;
- in computerised or electronic form.

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 5.5.

5.5 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.

In particular, subject persons carrying out relevant financial business are required to provide the FIAU, the supervisory authority or other relevant competent authorities with information as might be required from time to time related to:

(a) whether they maintain or have maintained a business relationship with a specified natural or legal person/s during the previous five years; and
(b) the nature of that relationship.

To this effect, subject persons carrying out relevant financial business 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 or other relevant competent authorities 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, unless the subject person makes representations justifying why the requested information cannot be submitted within the said time. 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.[61]

[61] Regulation 15(11) of the PMLFTR.

CHAPTER 6 – REPORTING PROCEDURES AND OBLIGATIONS

Subject persons are required to have internal and external reporting procedures in place for the purpose of reporting knowledge or suspicion of ML/FT to the FIAU.

6.1 The Money Laundering Reporting Officer

The PMLFTR state that internal reporting procedures maintained by a subject person shall include the appointment of a Money Laundering Reporting Officer who shall be an officer of the subject person and who shall be of sufficient seniority and command:

(i) *Officer of the subject person*

The person to be appointed by the subject person to act as MLRO shall be a person who is an official in employment with, or the executive director of, the subject person and resident in Malta. In addition the functions of a MLRO may not be:

- outsourced;
- carried out by a non-executive director of the subject person;
- 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.

It should be noted that a sole practitioner may act as the MLRO himself.

(ii) *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 policy. The person occupying this position must have a direct reporting line to the Board of Directors and should not be precluded from posing effective challenge where necessary. 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 for the purposes of fulfilling his responsibilities.

The MLRO is responsible for the oversight of all aspects of the subject person's AML/CFT activities and is the focal point for all activity relating to AML/CFT. The senior management of the subject person must ensure that the MLRO has sufficient resources available to him, including appropriate staff and technology, to be able to monitor the day-to-day operations of the subject person to ensure compliance with the subject person's AML/CFT policy.

According to the PMLFTR the MLRO is responsible for:

(a) receiving reports of knowledge or suspicion of ML/FT;[62]
(b) considering such reports to determine whether a suspicion of ML/FT subsists;[63]
(c) reporting knowledge or suspicion of ML/FT to the FIAU;[64] and
(d) responding promptly to any request for information made by the FIAU.[65]

Once the appointment of the MLRO is duly approved by the relevant supervisory authority, where applicable, the appointment and any subsequent changes thereto, 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.

The subject person shall notify the FIAU of the resignation or removal of its MLRO upon becoming aware of the proposed resignation or removal. The MLRO shall also 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 shall be made within 15 days from the date of resignation or removal.

Notwithstanding the conditions set out under paragraph (i) of this section, it shall be permissible for the MLRO duties of a collective investment scheme to be carried out by the MLRO of the administrator of the scheme in accordance with the outsourcing agreement entered into between the scheme and the administrator. In such cases the MLRO of the administrator shall be responsible for carrying out the reporting obligations of the scheme. Notwithstanding the outsourcing arrangement between the scheme and the administrator, the scheme shall remain responsible for compliance with the requirements under the PMLFTR and the Implementing Procedures and for the carrying out of the measures specifically assigned to the scheme under sections 9.1 and 9.2.

Additionally, an insurance company that is subject to the PMLFTR and is managed by a company that is enrolled to act as an insurance manager in terms of the Insurance Intermediaries Act (Cap. 487 of the Laws of Malta) may enter into an arrangement with the insurance manager whereby an employee of the insurance manager is seconded to the insurance company for the purpose of acting as the MLRO of the insurance company. The seconded person shall be a person of sufficient seniority and command as referred to under paragraph (ii) of this section.

6.2 The designated employee

The subject person may appoint one or more designated employees to assist the MLRO in the fulfilment of his AML/CFT duties. The appointment of the designated employee must receive the approval of the MLRO and such appointed person shall work under his direction.

[62] Regulation 15(4)(a) of the PMLFTR.
[63] Regulation 15(4)(b) of the PMLFTR.
[64] Regulation 15(6) of the PMLFTR.
[65] Regulation 15(11) of the PMLFTR.

Designated employees assist the MLRO to consider reports received in order to determine whether or not the information, or other matter contained in the report, give rise to a knowledge or suspicion that a person may have been, is, or may be engaged in ML/FT.

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.

6.3 Internal reporting procedures

The internal reporting procedures of the subject person should clearly set out the steps to be followed when an employee knows or suspects that a person or transaction is related to ML/FT.

The procedure should clearly state that any knowledge or suspicion of ML/FT should be reported directly to the MLRO or, in his absence, to the designated employee. Therefore, it is crucial that all employees are informed of the identity of the MLRO and any designated employee. Internal reports should be submitted in a written form, preferably on a standard template, together with all related information and documentation. The name of the employee making the report shall not be disclosed by the MLRO to the FIAU.

It should be noted that ideally the reporting line between the employee having the suspicion and the MLRO should be as short as possible, thus ensuring speed, confidentiality and accessibility to the MLRO. However, in larger organisations the reporting lines can be such that an employee has to consult with his superior before the report is forwarded to the MLRO. Where the superior decides not to forward an internal report to the MLRO, the employee submitting the report should be informed of the decision. Additionally, the superior should maintain written records of internal report not forwarded to the MLRO containing the reasons why such a decision not to report was taken. Such records should be available to the MLRO to be in a position to carry out assessments at his discretion and to the internal auditors where applicable.

In cases were the superior does not forward the internal report to the MLRO and the employee still has a suspicion that ML/FT is occurring or has taken place, the reporting lines should still enable the employee to submit the report directly to the MLRO.

The MLRO is to consider every internal report in the light of all other relevant information in order to determine whether or not the information contained in the report does give rise to a knowledge or suspicion of ML/FT. In view of this the MLRO should be granted reasonable access to all relevant documentation.

Failure by the MLRO to diligently consider all relevant material may lead to vital information being overlooked and the suspicion not being disclosed to the FIAU. In order to ensure that no essential information is overlooked, the MLRO should take into consideration:

(a) previous transactions, transaction patterns and volumes, previous patterns of instructions, the length of the business relationship and CDD information;
(b) where possible, 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, trust account or other trust 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.

If the MLRO concludes, for justifiable reasons, that an internal report does not give rise to a suspicion, the MLRO need not inform the FIAU. In this case, the MLRO shall keep a written record of the internal reports 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, or in completing the Annual Compliance Report mentioned under Section 6.11, the MLRO will make such information available.

6.4 External reporting procedures

After considering the internal report and all the necessary documentation, where the MLRO knows, suspects or 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 shall file a report with the FIAU.[66]

The PMLFTR require the MLRO to report to the FIAU when he has **knowledge**, **suspicion** or **reasonable grounds to suspect** ML/FT. 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. If for any reason the MLRO, or any other employee of the subject person, is aware or is in possession of information that indicates 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 report 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 differ 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

[66] Regulation 15(6) of the PMLFTR.

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, is the situation where the subject person is unable to complete customer due diligence due 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 a 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"*.[67]

"*Although the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation."*[68]

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 v HSBC Private Bank (UK) Ltd, 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. 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"."

(iii) Reasonable Grounds to Suspect

The requirement to file a report 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, the subject person ought to have suspected that ML/FT existed, even though a suspicion was not formed.

[67] JMLSG Guidance Chapter 6, Paragraph 6.9 p. 121,
[68] *Ibid.*

Any disclosures made by the subject person to the FIAU should be made as soon as is reasonably practicable, but **not later than five (5) working days** from when the suspicion first arose. The suspicion shall be deemed to have first arisen when any person within the structure of the subject person first suspects the existence of ML/FT and thus submits an internal report to the MLRO.

Any disclosures made to the FIAU should be made through the completion of a Suspicious Transaction Report (STR). A template for this purpose may be downloaded from the FIAU website on http://www.fiumalta.org/report-suspicious-transaction.[69] In completing this report MLROs should provide as much detail as possible together with the relevant identification and other supporting documentation. In order to ensure the highest level of confidentiality subject persons should submit the STR using the FIAU's online portal and should refrain from making any disclosures by email. Any manual submission of the STR should be delivered by hand to the FIAU premises addressed to the Director at the hereunder address. In such cases the template downloaded from the FIAU website shall be signed by the MLRO.

Financial Intelligence Analysis Unit
67/4 South Street
Valletta VLT 1105

In cases of urgency an initial disclosure may be made by telephone on the number provided below, but a written report shall then be submitted within the shortest time possible, either through the FIAU's online portal or by hand.

Telephone Number: (+356) 21 231 333

It should be noted that STRs should only be filed with the FIAU and should not be copied to any supervisory authority.

6.5 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 Director who allocates the report to the financial analysts for further analysis.

In the course of the analysis of the STR, the FIAU may require further information and, in terms of the PMLFTR, it could request such information from the subject person filing the STR or any other subject person, the police, any Government Ministry, department, agency or other public authority, or any other person, physical or legal and from any supervisory authority. When the FIAU requests such information from a subject person, that subject person shall comply with the request as soon as is reasonably practicable but not later than five (5) working days from when the demand is first

[69] It is to be noted that a STR which is not submitted in the format provided by the FIAU on its website, will still be valid and acceptable to the FIAU. However, this should be an exceptional occurrence and, for the sake of consistency, subject persons are strongly encouraged to use the format provided by the FIAU.

made, 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.

If once a report is filed the subject person decides to maintain the business relationship with the customer who is the subject of the report, the subject person should classify the customer as a high -risk customer and monitor the activities of that customer to a larger extent. It is to be noted that in such circumstances subject persons should not automatically report every transaction carried out by that customer after the report 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 a 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.

Subject persons reporting a STR to the FIAU may request feedback from the FIAU on the progress of the analysis of the STR. In such cases, the FIAU shall provide such information to the reporting subject person that 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 should treat feedback information with utmost confidentiality.

6.6 Request to carry out a transaction known or suspected to be related to ML/FT

In accordance with Regulation 15(7), subject persons shall not carry out a transaction that is suspected or known to be related to ML/FT until they have informed the FIAU. This obligation is also found in Article 28 of the PMLA, which empowers the FIAU to delay the execution of such transactions by twenty-four (24) hours. In accordance with Article 28, where a subject person is aware or suspects that a transaction which is to be executed may be linked to ML/FT, that subject person shall inform the FIAU before executing the transaction, giving all the information concerning the transaction, including the period within which it is to be executed.

Such information may be given by telephone (telephone number: 21 231 333) but shall be forthwith confirmed by fax (fax number: 21 231 090) or by any other written means. The FIAU will acknowledge in writing the receipt of the information and it is only upon the receipt by the subject person of the FIAU's acknowledgement that the notification to the FIAU shall be deemed to have taken place.

After acknowledging the receipt of the information, the FIAU will determine whether the execution of the transaction should be delayed. The FIAU shall do its utmost to ensure that such determination is reached within the period of time within which the transaction is expected to be executed, as notified by the subject person. The execution of the transaction may be delayed by twenty-four (24) hours and notice of such delay of execution shall be immediately given to the subject person. Where the FIAU delays the transaction but upon further analysis determines that no suspicion of ML/FT subsists it may subsequently authorise the execution of the transaction before the expiry of the twenty-four (24) hour period.

There may be situations where the FIAU does not oppose the execution of the transaction. In this case, where the period of time provided by the subject person within which the transaction is expected to be executed lapses, the subject person may proceed with the execution of the transaction.

Where the execution of the transaction is opposed by the FIAU, the subject person may only proceed with the execution of the transaction upon the lapse of the twenty-four (24) hour period, unless in the meantime an attachment order issued by the competent court would have been served on the subject person.

In accordance with Regulation 15(7), where subject persons are not in a position to refrain from carrying out a transaction which is known or suspected to be related to ML/FT in view of the fact that such action is **impossible** because of the nature of the transaction or such action is likely to frustrate efforts of investigating or pursuing the beneficiaries of the suspected ML/FT operations, subject persons shall carry out the transaction and inform the FIAU immediately.

Similarly, Article 29 of the PMLA 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 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 impossible for the transaction not to be executed that the subject person may carry out the transaction and this impossibility must arise from the nature of the transaction itself.

6.7 Monitoring orders

In terms of Article 30B, 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 shall be made for a specified period of time. During the course of such order the subject person is required to monitor the transactions or, in the case of banks, banking operations:

- carried out through one or more accounts in the name of any natural or legal person suspected of a ML/FT offence; or
- carried out through one or more accounts suspected to have been used in the commission of a ML/FT offence; or
- which could provide information about a ML/FT offence or the circumstances thereof.

The FIAU may issue such a monitoring order whether 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.

6.8 Professional privilege

By virtue of Regulation 15(10), 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(6) 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(7), 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(10) extends the same principle to other members of the legal profession, 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.[70] Nevertheless, if 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 without informing the client in a situation where the client seeks to carry out a transaction with the aim of laundering money or funding terrorism

6.9 Prohibition of disclosures

When a subject person has a suspicion that ML/FT is occurring, both the subject person as well as any official or employee of a subject person, are prohibited from disclosing to the person under investigation or to a third party, that an investigation is being carried out, may be carried out, or that information has been or may be transmitted to the FIAU.[71] Disclosure of such information would give rise to the offence of tipping off and may prejudice an investigation. The elements of the offence of tipping off and the punishment set out by law are laid out in more detail in Section 8.5.1.6.

A subject person must however still retain the necessary contact with a customer and should enquire, in a tactful manner, about any transaction which is not consistent with the customer's normal pattern of activity. This is prudent practice and forms an integral part of CDD measures. Such enquiries would not in themselves give rise to tipping off.

6.10 Permissible disclosures

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 a breach of the PMLFTR.[72] 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) disclosure by the MLRO of a subject person undertaking relevant financial business to the MLRO of another person/persons who:
   (1) undertakes equivalent activities;

[70] Regulation 16(3) of the PMLFTR.
[71] Regulation 16(1) of the PMLFTR.
[72] Regulation 16(2) of the PMLFTR.

(2) forms part of the same group of companies; and
(3) is situated in Malta, within another Member State of the European Community or in a reputable jurisdiction;

(c) disclosure by the MLRO of a subject person undertaking relevant activity under paragraphs (a) and (c) of Regulation 2 of the PMLFTR (definition of 'relevant activity) to the MLRO of another person/persons who:
(1) undertakes equivalent activities;
(2) performs their activities whether as employees or not;
(3) 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; and
(4) is situated in Malta, within another Member State of the European Community or in a reputable jurisdiction;

(d) disclosures between the same professional category of subject persons referred to in paragraphs (b) and (c) above in cases:
(1) that relate to the same customer;
(2) that relate to the same transaction;
(3) that involve two or more institutions or persons situated in Malta, within another Member State of the European Community or in a reputable jurisdiction;
(4) such persons are subject to equivalent obligations of professional secrecy and personal data protection; and
(5) the information exchanged shall only be used for the purposes of the prevention of ML/FT.

However, if the FIAU determines, or is informed, that a jurisdiction does not meet the criteria of a reputable jurisdiction (refer to Section 8.1), it shall, in collaboration with the relevant supervisory authorities, prohibit subject persons from applying the provisions applicable to permissible disclosures with persons and institutions from that jurisdiction. It is to be noted that the FIAU has determined, by means of a guidance note which is contained within Appendix III, that certain categories of jurisdictions referred to in FATF public statements shall not be considered to be reputable thereby prohibiting subject persons from applying the provisions applicable to permissible disclosures with persons and institutions from those jurisdictions.

Furthermore, any *bona fide* communication or disclosure made by a subject person or by an employee or director of such subject person, shall not constitute a breach of the duty of professional secrecy, or any other restriction (whether imposed by statute or otherwise) and such person shall not be subject to liability of any kind.[73]

6.11 Annual Compliance Report

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

[73] Regulation 15(12) of the PMLFTR.

the PMLA empowering the FIAU to undertake both off-site and on-site examinations. Moreover, Article 27 empowers the FIAU to enter into agreements with relevant supervisory authorities to undertake compliance examinations on its behalf.

Monitoring of compliance by subject persons is partly conducted on an off-site basis which requires the gathering of relevant information from subject persons. In order to properly fulfil its off-site compliance function the FIAU has introduced a procedure whereby subject persons are required to submit an annual compliance report related to their activities, operations and preventative measures. This report ensures that the FIAU gathers information for compliance purposes on a systematic and timely basis.

The annual compliance report assists the FIAU in fulfilling another essential function, which is the compilation of statistics and records in order to review 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. It is pertinent to note that Regulation 14(2) extends the requirement to maintain comprehensive statistical data to subject persons, supervisory and other competent authorities which are required to make such data available to the FIAU upon request.

6.11.1 Contents of the Annual Compliance Report

The annual compliance report ("the Report") requires the completion of general details on the subject persons, as well as other information which, *inter alia*, includes:

(a) information on internal suspicious reports and STRs submitted to the FIAU;
(b) an overview of the policies and procedures on internal control, risk assessment, risk management and compliance management established by the subject person and their effective implementation;
(c) an overview of the manner through which the MLRO would have assessed internal compliance, including overall oversight by the internal audit function, where applicable, highlighting any non-compliance findings that may have been identified and corrective measures taken accordingly; and
(d) information concerning the AML/CFT training attended by the MLRO and any designated employees and AML/CFT training provided to staff members.

The information provided in the Report should be as at date of submission, with the exception of information detailed in the sections of the Report concerning suspicious transaction reports and AML/CFT training that cover the previous calendar year.

The Report, which in all circumstances shall be completed by the MLRO, shall be submitted for the approval of senior management as follows:

(a) where the subject person is a sole-practitioner, self-employed or where the MLRO is the sole director of the subject person, no senior management approval would be required;
(b) where the MLRO is one of two or more directors, then in line with good corporate governance principles, the Report shall be submitted to another director for review;

(c) where the MLRO is an employee of a subject person, the Report shall be reviewed by the chairman, managing director, chief executive officer or any other person who forms part of the senior management of the entity.

Once reviewed, the Report shall then be submitted electronically through the FIAU's online portal, within the time-frames envisaged in Section 6.11.2 below. When submitting the Report the MLRO is required to provide a declaration that the information provided in the Report is complete and accurate, and that the contents thereof were reviewed in accordance with the paragraph above. A template of the Report may be downloaded from the FIAU website on http://www.fiumalta.org/submit-annual-compliance-report.

Although the Report should be submitted electronically through the FIAU's online portal, this could be extraordinarily accepted in paper format so long as this is cleared beforehand with the FIAU Compliance Section. In this case, the MLRO and the person approving the completed Report, where applicable, will be required to sign it. Reports sent by email will not be considered as valid submissions.

Sole practitioners, being those natural persons who undertake any relevant financial business and/ or relevant activity in their own name or under a trade name and who do not employ or otherwise engage anyone else to handle any such business or activity, are entitled to complete an abridged Report instead of the standard Report. An entity, regardless of its legal form, carrying out relevant financial business and/or relevant activity shall be considered to qualify as a sole practitioner for the purposes of this section if it is owned and managed by one person and does not employ or otherwise engage anyone else to handle any such business or activity. Such entities will also be entitled to submit the abridged version. A template of the abridged Report, is available to be downloaded from the FIAU website on http://www.fiumalta.org/submit-annual-compliance-report.

As from the 1 January 2015 a fee for processing the Report submitted by subject persons is payable to the FIAU. The fees are set as follows:

i. € 50.00 – when the Report is submitted in electronic format as explained above;
ii. € 65.00 – when the Report is submitted manually in paper format.

6.11.2 The submission period

Subject persons will be required to submit the Report in accordance with the time-frames provided below:

By not later than 28th February of every year:

- Entities licensed under the Banking Act
- Entities licensed under the Financial Institutions Act
- Entities licensed under the Insurance Business Act, Insurance Intermediaries Act, Insurance Business (Companies Carrying on Business of Affiliated Insurance) Regulations, the Companies Act (Cell Companies Carrying on Business of Insurance) Regulations and the Companies Act (Incorporated Cell Companies Carrying on Business of Insurance) Regulations

By not later than 31st March of every year:

- Entities licensed under the Investment Services Act other than Collective Investment Schemes
- Entities licensed under the Retirement Pensions Act
- Central Securities Depository / Financial Markets

By not later than 30th April of every year:

- Trust & Company Service Providers
- Persons providing trustee or any other fiduciary service
- Real Estate Agents
- Casinos

By not later than 31st May of every year:

- Other categories of non-financial subject persons

By not later than 30th June of every year:

- Collective Investment Schemes licensed or recognised under the Investment Services Act

Nominee companies holding a warrant under the Malta Financial Services Authority Act and acting in relation to dissolved companies registered under the said Act, shall be exempted from the requirement to submit a Report.

It shall be the MLRO's responsibility to ensure that the Report is completed and submitted by the designated date. Where the same entity or person carries out more than one activity falling within the definition of relevant financial business and relevant activity, such entity or person shall not be required to submit a separate Report in relation to each individual activity carried out and should submit the Report on the earliest date on which the Report is due.

6.11.3 Actions by the FIAU after receiving the Report

On the basis of the contents of the Report the FIAU may provide a number of recommendations or require remedial action where these are deemed to be necessary. The FIAU may also require subject persons to provide further information in relation to matters that raise concerns. The Report will also assist the FIAU in planning its on-site monitoring programme on a risk-based approach in respect of all subject persons.

CHAPTER 7 – AWARENESS, TRAINING AND VETTING OF EMPLOYEES

Every subject person is required to ensure that employees are kept aware of the subject person's AML/CFT policies and procedures and the relevant legislation and to provide training in relation thereto, as well as in relation to the recognition and handling of transactions carried out by, or on behalf of, any person who may have been, is, or appears to be engaged in ML/FT.[74]

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. Indeed, policies and procedures to prevent ML/FT cannot be implemented effectively unless employees are made fully aware of their obligations and are provided with the necessary 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,[75] irrespective of their level of seniority, in view of the fact that such employees will be in a position to detect transactions which may be related to ML/FT. This includes directors, senior management, the MLRO himself, compliance staff and generally all members of staff involved in the activities of the subject person which fall within the definition of relevant financial business and relevant activity.

7.1 Employee awareness

All employees should be made aware of the subject person's:

(a) customer due diligence measures;
(b) record-keeping procedures;
(c) internal reporting procedures;
(d) policies and procedures on internal control;
(e) policies and procedures on risk assessment and risk management; and
(f) policies and procedures on compliance management and communication.

All employees should be informed of the identity of the MLRO and designated employee(s), where applicable, and of their functions and responsibilities.

Employees should also be made aware of the following:

(a) the provisions of the PMLA;
(b) the provisions in the Criminal Code on funding of terrorism;
(c) the provisions of the PMLFTR;
(d) the offences and penalties in relation to any breach of the PMLA or the PMLFTR; and
(e) the Implementing Procedures.

[74] Regulation 4(1)(d) and (e) of the PMLFTR.
[75] Regulation 4(3) of the PMLFTR.

All the above-mentioned information should be made readily available to all employees to enable them to refer to such information as and when appropriate throughout the conduct of their duties.

7.2 Nature of training

The Regulations specify that every subject person is required to provide training to employees in order to recognise and handle transactions carried out by, or on behalf of, any person who may have been, is, or appears to be engaged in ML/FT.

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 the purposes of ML/FT and the manner in which such vulnerabilities should be managed. Training should be tailored in accordance with the specific responsibilities and functions of the respective employees and the business carried out by the subject person. For instance, front-office employees should be provided with a different kind of training to that provided to employees carrying out back-office functions and the training provided by a credit institution would naturally differ from the training provided by a company carrying out the business of insurance or a real-estate agent.

Additionally, training should be of a more practical nature rather than simply theoretical. This means that the training provided should make references to real-life situations such as, for instance, the steps to be followed when accepting customers, the handling of high-risk customers and the behaviour to be adopted when faced with a request for a transaction which is suspicious. Typology reports prepared by the FATF, Moneyval or other FSRBs play an important role in preparing training material.

Subject persons need to determine the method in which training is to be delivered, as the most appropriate method may vary from one organisation to the other. The method generally depends on the size of the organisation. On-line learning systems can often provide an adequate solution for general training to all employees who deal with clients, while focused classroom training for higher-risk areas can be more effective.

It is vital to maintain comprehensive records of training sessions which, as already stated in Chapter 5, should include:

(a) the date on which the training was delivered;
(b) the nature of the training;
(c) the names of employees receiving the training;
(d) the results of any assessment undertaken by employees; and
(e) a copy of any handouts or slides.

7.3 Timing of awareness training

Measures adopted to increase employee awareness and other training in accordance with Regulation 4 of the PMLFTR should be provided from time to time. The frequency of awareness and training depends on a number of factors including the size and nature of business, the ML/FT risks of the subject person and the functions and responsibilities of the particular employees. However,

the established principle is that awareness and training should be an ongoing exercise to ensure that employees are constantly kept up-to-date with any developments or changes in the operations of the subject person and any changes in the applicable laws.

Subject persons should preferably prepare an annual training programme for AML/CFT which should include both internal and external sessions. Although the annual training programme should vary from year to year according to the requirements of the subject person at the time, training programmes should include ongoing refresher courses, where the need arises, for those employees who would have already received training during previous programmes.

Subject persons must also provide training at appropriate intervals as follows:

(a) to new employees during the induction training upon commencement of work;
(b) to specific employees where there is a change in the employee's role at some stage after employment;
(c) to all employees, including senior management and the directors, where there is a substantial change in requirements and obligations in the pertinent legislation.

7.4 Vetting of new employees

Subject persons shall ensure that they have in place appropriate procedures for due diligence when hiring employees.[76] This would generally include obtaining professional references, confirming employment history and qualifications and requesting a recent police conduct certificate. This requirement must be applied whenever recruitment is taking place irrespective of the position of the employee.

[76] Regulation 4(2) of the PMLFTR.

CHAPTER 8 – OTHER ANCILLARY MATTERS

8.1 The notion of reputable jurisdiction

The definition of reputable jurisdiction under Regulation 2 refers to '*any country having appropriate legislative measures for the prevention of money laundering and the funding of terrorism, taking into account that country's membership of, or any declaration or accreditation by, any international organisation recognised as laying down internationally accepted standards for the prevention of money laundering and for combating the funding of terrorism, and which supervises natural and legal persons subject to such legislative measures for compliance therewith*'.

The PMLFTR do not require the FIAU to issue a list of "reputable jurisdictions" but provide for subject persons themselves to determine the level of AML/CFT legislation and supervision of a particular country. Primarily, for a country to be deemed to be reputable, it should be established that that country has "appropriate legislative measures" in place for the prevention of ML/FT. The definition itself then guides subject persons to take into account *inter alia* that country's membership of, or any declaration or accreditation by, any international organisation recognised as laying down internationally accepted standards for the prevention of ML/FT. For this purpose subject persons should refer to mutual evaluation reports or public statements on that country issued by the FATF, MONEYVAL or other FSRBs.

Subject persons may be required to establish whether a jurisdiction is to be considered a "reputable jurisdiction", as defined in Regulation 2 of the PMLFTR, for a number of reasons, including the risk assessment of an applicant for business and qualification for SDD or EDD in terms of Regulations 10 and 11 respectively; whether a subject person can rely on a third party's customer due diligence under Regulation 12; whether the provisions under Regulation 16 on permissible disclosures apply; or whether the prohibition laid down in Regulation 6 (cross border branches and subsidiaries) applies to a particular jurisdiction.

It is to be noted that in determining whether a jurisdiction is reputable or otherwise subject persons are required to comply with the FIAU Guidance Note on High-Risk and Non-Cooperative Jurisdictions. Additionally, reference may be made to the EU Common Understanding on Third Country Equivalence.

8.1.1 FIAU Guidance Note on High-Risk and Non-Cooperative Jurisdictions

The FIAU Guidance Note on High-Risk and Non-Cooperative Jurisdictions, which is contained in Appendix III, provides guidance on the application of certain obligations under the PMLFTR within the context of the public documents issued by the FATF on high-risk and non-cooperative jurisdictions. In particular, the guidance note provides guidance on the interpretation of the notion of reputable jurisdiction and clearly establishes that certain jurisdictions listed in the FATF public documents shall not be considered to be reputable jurisdictions.

8.1.2. EU Common Understanding on Third Country Equivalence

While Member States of the European Community, on the basis of the principle of mutual recognition applicable in view of the implementation of the 3rd AML Directive, may be automatically presumed to satisfy the criteria of "reputable jurisdiction", acceptance of business or transactions from third countries would require a more detailed assessment by subject persons. The list of countries contained in the Common Understanding on Third Country Equivalence issued by the Member States (refer to Appendix II), which list is a voluntary, non-binding measure that nevertheless represents the common understanding of Member States, is to be seen to be an added tool to assist subject persons in this assessment. It should be noted, however, that the mere omission of a jurisdiction from the said list does not necessarily mean that the AML/CFT and due diligence standards in those countries are low and should therefore be classified as a non-reputable jurisdiction. Neither does it mean that states included in the list are to be automatically deemed to classify as a reputable jurisdiction, although a lighter assessment would, under normal circumstances, suffice.

These third countries are currently considered by EU Member States as having equivalent AML/CFT systems to the EU. The list may, however, be reviewed, in particular in the light of public evaluation reports adopted by the FATF, MONEYVAL or other FSRBs, the IMF or the World Bank according to the FATF Recommendations and Methodology.

Consequently, domestically, the common list, which is also endorsed by the FIAU, should be seen to be particularly relevant to assist subject persons in their assessment as to whether a jurisdiction is to be considered a reputable jurisdiction in terms of and for the purposes of the PMLFTR.

The onus remains on subject persons to carry out their own assessment of particular countries based on up-to-date information on that country. Not only should the subject person consider its own knowledge and experience of the country concerned, but particular attention should be paid to any FATF, MONEYVAL or other FSRBs or IMF/World Bank evaluations undertaken, membership of groups that only admit those meeting a certain benchmark, contextual factors, incidence of trade with the particular jurisdiction, public announcements of non-cooperation and other relevant factors.

In this regard subject persons should document in writing the reasons for determining that a particular jurisdiction is considered to be a "reputable jurisdiction".

8.2 Branches and subsidiaries

The PMLFTR[77] provide that subject persons carrying out relevant financial business shall not establish or acquire branches or majority owned subsidiaries in jurisdictions that do not meet the criteria for a reputable jurisdiction (refer to Section 8.1).

Moreover, subject persons carrying out relevant financial business through a branch or a majority owned subsidiary in a reputable jurisdiction shall:

[77] Regulation 6(1) of the PMLFTR.

(a) communicate to such branches and majority owned subsidiaries its relevant AML/CFT internal policies and procedures established in accordance with the PMLFTR; and
(b) apply in such branches and majority owned subsidiaries, where applicable, measures relating to customer due diligence and record keeping that, as a minimum, are equivalent to those under the PMLFTR.

Where the legislation of that reputable jurisdiction does not permit the application of such equivalent measures, subject persons shall immediately inform the FIAU and shall take additional measures to effectively handle the risk of ML/FT. The PMLFTR do not establish the nature of the 'additional measures' to be applied and therefore leave this at the discretion of the subject person. Such measures could, for example, include the application of EDD to all customers, transactions or products related to such jurisdiction, the imposition of limits on particular transactions or any similar obligations.

If the subject person is unable to apply such additional measures, the subject person shall immediately inform the FIAU who, in collaboration with the supervisory authority, may require the closure of the branch or majority owned subsidiary in accordance with the applicable law.

8.3 Written procedures

Subject persons are required to draw up a written procedures manual setting out in detail the procedures implemented by the subject person in order to comply with all the obligations emanating from the PMLFTR and the PMLA, which procedures manual should receive the approval of senior management or the Board of Directors, where applicable.

All relevant employees should have access to the procedures manual and subject persons should ensure that employees acknowledge that they have received and understood such procedures manual. The employees' awareness of the procedures manual should be tested periodically and records of such tests should be available for inspection by the FIAU. In terms of Section 7.2 the procedures manual should be the basis for the training programmes of the subject persons.

Subject persons shall, when so requested, provide a copy of their written procedures to the FIAU.

8.4 Internal controls

Regulation 4(1)(c) requires subject persons to establish policies and procedures on internal control, compliance management and communications that are adequate and appropriate to prevent the carrying out of operations that may be related to ML/FT. This entails that apart from the internal reporting procedures referred to in Section 6.3, subject persons must ensure that the policies and procedures implementing the provisions of the PMLFTR and the Implementing Procedures are adequately controlled and monitored. Such function should ideally be vested in the internal audit department of the subject person. Where an internal audit department is not set up, subject persons are expected to take other measures, such as for instance assigning this task internally to a person other than the MLRO or engaging the services of an external assessor, to control and monitor their policies and procedures.

8.5 Offences and penalties

A number of offences and breaches of an administrative nature are contemplated under the PMLA and the PMLFTR. The procedure for the imposition of a penalty further to a failure to comply with the law varies depending on the nature of the breach. Those offences which are punishable with a fine (*multa*) or imprisonment are subject to proceedings before the criminal courts of Malta. Where an administrative penalty is contemplated, these may be imposed by the FIAU without recourse to a court hearing.

When any sanction contemplated in the PMLFTR or any written warning is to be imposed by the FIAU the following procedure shall be followed:

(a) the subject person is informed of the potential breach detected by the FIAU and the possibility of the imposition of an administrative penalty;
(b) the subject person is requested to make any representations in writing explaining why such administrative penalty should not be imposed and providing all material information which the subject person may deem to be relevant in order for the FIAU to reach its determination as to whether the penalty is to be imposed;
(c) the subject person is required to make such representations and provide such information within thirty days from the date of the FIAU's request;
(d) upon receipt of the representations of the subject person an internal evaluation will be carried out by the FIAU and a determination is reached as to whether the sanction is to be imposed;
(e) in the event that an administrative penalty is imposed, the FIAU will inform the subject person of such penalty explaining the reasons why such a determination was reached;
(f) administrative penalties are to be paid within fourteen days from the date on which the subject person is informed of such penalty;
(g) if, on the basis of representations made and the information provided, the FIAU determines that the breach does not subsist and therefore the imposition of an administrative penalty is not warranted, the FIAU may still conclude that the circumstances warrant a warning which shall be given in writing by the FIAU;
(h) written warnings may also be issued by the FIAU at its discretion in the course of the carrying out of its compliance monitoring function under Article 16(1)(c) of the PMLA in situations other than those mentioned in paragraph (g) above.

8.5.1 Offences and breaches of an administrative nature under the PMLFTR

This section contains a list of offences and breaches of an administrative nature, together with their respective penalties, which can be found under the various regulations of the PMLFTR.

8.5.1.1 Non-compliance with procedures to prevent ML/FT

Regulation: 4(5)

Offence: Contravention of the provisions of Regulation 4 of the PMLFTR by a subject person by not maintaining appropriate procedures for CDD, record keeping and reporting or does not provide the necessary training to its employees.

Penalty: Subject persons shall on conviction be liable to a fine (*multa*) not exceeding fifty thousand euro (€50,000) or to imprisonment for a term not exceeding two years, or to both such fine and imprisonment.

8.5.1.2 Non-compliance with procedures to prevent ML/FT by corporate/unincorporated bodies/other associations of persons

Regulation: 5

Offence: Contravention of the provisions of Regulation 4 of the PMLFTR, where the offence is committed by a body corporate or other association of persons, be it corporate or unincorporated, or by a person within and for the benefit of that body or other association of persons consequent to the lack of supervision or control that should have been exercised on him.

Penalty: Such body or association shall be liable to an administrative penalty of not less than one thousand two hundred euro (€1,200) and not more than five thousand euro (€5,000). Such penalty shall be imposed by the FIAU without recourse to a court hearing and may be imposed either as a one time penalty or on a daily cumulative basis until compliance, provided that in the latter case the accumulated penalty shall not exceed fifty thousand euro (€50,000).

Every person who at the time of the commission of the offence was a director, manager, secretary or similar officer of such body or association or was purporting to act in any such capacity, shall be guilty of that offence, unless he proves that the offence was committed without his knowledge and that he exercised all due diligence to prevent the commission of the offence.

Where such person is found guilty the penalty envisaged under Regulation 4(5) shall apply.

8.5.1.3 False declaration/false representation by an applicant for business

Regulation: 7(10)

Offence: A false declaration or false representation or the production of false documentation by an applicant for business.

Penalty: The applicant for business shall on conviction be guilty of an offence and shall be liable to a fine (*multa*) not exceeding fifty thousand euro (€50,000), or to

imprisonment for a term not exceeding two (2) years or to both such fine and imprisonment.

8.5.1.4 Contravention of the provisions on customer due diligence

Regulation: 7(12)

Offence: Contravention of the provisions of Regulation 7 of the PMLFTR or of the provisions of Regulation (EC) No. 1781/2006 of the European Parliament and of the Council of 15th November 2006 on information on the payee accompanying transfers of funds.

Penalty: Administrative penalty of not less than two hundred and fifty euro (€250) and not more than two thousand five hundred euro (€2,500), which shall be imposed by the FIAU without recourse to a court hearing.

8.5.1.5 Contravention of the provisions on reporting procedures and obligations

Regulation: 15(15)

Offence: Contravention of the provisions of Regulation 15 of the PMLFTR or failure to disclose information in accordance with Regulation 15(6) and (7) or failure to submit information in accordance with Regulation 15(11).

Penalty: Administrative penalty of not less than two hundred and fifty euro (€250) and not more than two thousand five hundred euro (€2,500), which shall be imposed by the FIAU without recourse to a court hearing and may be imposed either as a one time penalty or on a daily cumulative basis until compliance, provided that in the latter case the accumulated penalty shall not exceed twelve thousand five hundred euro (€12,500).

8.5.1.6 Tipping off

Regulation: 16(1)

Offence: Disclosure by a subject person, a supervisory authority, or any official or employee of a subject person or a supervisory authority, to a person concerned or to a third party, other than as provided for in Regulation 16, that an investigation is being or may be carried out or that information has been or may be transmitted to the FIAU pursuant to the PMLFTR.

Penalty: The subject person, a supervisory authority, or any official or employee of a subject person or a supervisory authority shall on conviction be guilty of an offence and liable to a fine (*multa*) not exceeding fifty thousand euro (€50,000), or to imprisonment for a term not exceeding two (2) years or to both such fine and imprisonment.

8.5.1.7 Non-compliance with the Implementing Procedures

Regulation: 17(2)

Offence: A subject person who fails to comply with the provisions of any procedures and guidance issued by the FIAU with the concurrence of the relevant supervisory authority shall be liable to an administrative penalty.

Penalty: Administrative penalty of not less than two hundred and fifty euro (€250) and not more than two thousand five hundred euro (€2,500), which shall be imposed by the FIAU without recourse to a court hearing and may be imposed either as a one time penalty or on a daily cumulative basis until compliance, provided that in the latter case the accumulated penalty shall not exceed twelve thousand five hundred euro (€12,500).

As stated under Section 1.4, the FIAU shall not impose a penalty for non-compliance with the Implementing Procedures where a subject person has already been sanctioned for the same act or omission in terms of the PMLFTR.

8.5.2 Offences under the PMLA

This section contains a list of offences, together with their respective penalties, which can be found under the various articles of the PMLA.

8.5.2.1 Money laundering offence

Article: 3(1)

Offence: Money laundering

Penalty: Any person committing any act of money laundering shall on conviction be guilty of an offence and liable to a fine (*multa*) not exceeding two million and three hundred and twenty-nine thousand and three hundred and seventy-three euro and forty cents (€2,329,373.40), or to imprisonment for a term not exceeding fourteen (14) years or to both such fine and imprisonment.[78]

Where the offence is committed by a body of persons, whether corporate or unincorporate, every person who at the time of the commission of the offence was a director, manager, secretary or other similar officer of such body or association or was purporting to act in any such capacity, shall be guilty of that offence, unless he proves that the offence was committed without his knowledge and that he exercised all due diligence to prevent the commission of the offence.

Where the person found guilty of an offence of money laundering under the PMLA is an officer of a body corporate or is a person having a power of representation or having such authority and the

[78] The amounts in Euro correspond to the equivalent sum in Maltese liri at the fixed Maltese lira/Euro exchange rate of 0.4293.

offence of which that person was found guilty was committed for the benefit, in part or in whole, of that body corporate, the said person shall for the purposes of the PMLA be deemed to be vested with the legal representation of the same body corporate which shall be liable to the payment of a fine (*multa*) of not less than one thousand and one hundred and sixty-four euro and sixty-nine cents (€1,164.69) and not more than one million and one hundred and sixty-four thousand and six hundred and eighty-six euro and seventy cents (€1,164,686.70).

The court shall, in addition to any punishment to which the person convicted of an offence of money laundering under the PMLA may be sentenced and in addition to any penalty to which a body corporate may become liable, order the forfeiture in favour of the Government of Malta of the proceeds or of such property the value of which corresponds to the value of such proceeds whether such proceeds have been received by the person found guilty or by the body corporate and any property of or in the possession or under the control of any person found guilty as aforesaid or of a body corporate shall, unless proved to the contrary, be deemed to be derived from the offence of money laundering and liable to confiscation or forfeiture by the court.

8.5.2.2 Disclosure of an investigation/attachment order

Article: 4(2)/4(6A)

Offence: Disclosure that an investigation/attachment order has been made or applied for.

Penalty: Any person disclosing that an investigation/attachment order has been made or applied for shall on conviction be liable to a fine (*multa*) not exceeding eleven thousand and six hundred and forty-six euro and eighty-seven cents (€11,646.87), or to imprisonment for a term not exceeding twelve (12) months or to both such fine and imprisonment.[79]

8.5.2.3 Acting in contravention of an investigation/attachment order

Article: 4(5)/4(10)

Offence: Acting in contravention of an investigation/attachment order.

Penalty: Any person acting in contravention of an investigation/attachment order shall on conviction be liable to a fine (*multa*) not exceeding eleven thousand and six hundred and forty-six euro and eighty-seven cents (€11,646.87), or to imprisonment for a term not exceeding twelve (12) months or to both such fine and imprisonment.[80]

[79] *Ibid.*
[80] *Ibid.*

8.5.2.4 Acting in contravention of a freezing order

Article: 6

Offence: Acting in contravention of a freezing order

Penalty: Any person acting in contravention of a freezing order shall on conviction be liable to a fine (*multa*) not exceeding eleven thousand and six hundred and forty-six euro and eighty-seven cents (€11,646.87), or to imprisonment for a term not exceeding twelve (12) months or to both such fine and imprisonment and any act so made in contravention of such court order shall be null and without effect at law and the court may, where such person is a garnishee, order the said person to deposit in a bank to the credit of the person charged the amount of moneys or the value of other movable property paid or delivered in contravention of the freezing order.[81]

8.5.3 Offence of Funding of Terrorism (Criminal Code)

Article: 328F to 328I

Offence: Funding of Terrorism

Penalty: Any person committing any of the offences under the above-mentioned articles shall on conviction be guilty of an offence and be liable to a fine (*multa*) not exceeding eleven thousand and six hundred and forty-six euro and eighty-seven cents (€11,646.87), or to imprisonment for a term not exceeding four (4) years or to both such fine and imprisonment.[82]

[81] *Ibid.*
[82] *Ibid.*

CHAPTER 9 – OUTSOURCING OF THE REQUIREMENTS UNDER THE PMLFTR BY A COLLECTIVE INVESTMENT SCHEME

The PMLFTR and the Implementing Procedures apply to "a collective investment scheme marketing its units or shares". For the purposes of compliance with the PMLFTR and these Implementing Procedures, the phrase "marketing its units or shares" is interpreted to mean 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. Therefore all collective investment 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.

It shall be permissible for a collective investment scheme that does not have a physical operational set-up in Malta other than its 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 outsource the implementation of the measures and procedures applicable to it under the PMLFTR in relation to its unit holders, including customer due diligence, record-keeping, risk-assessment procedures and reporting obligations ("AML/CFT measures and procedures"), to the entity providing administration services to the scheme ("the administrator").

It shall therefore be permissible for the duties attributable to the MLRO of a collective investment scheme to be carried out by the MLRO of the administrator of the scheme. In such cases the MLRO of the administrator shall be responsible for carrying out the reporting obligations of the scheme.

The above outsourcing arrangements may only be entered into with an administrator licensed or recognised under the Investment Services Act (Cap. 370 of the Laws of Malta) or with an administrator which is authorised or otherwise recognised within a Member State of the Community or in a reputable jurisdiction. Those administrators that are subject to the PMLFTR shall apply the outsourced AML/CFT measures and procedures in accordance with the requirements set out under the PMLFTR and the Implementing Procedures. Where the scheme enters into an outsourcing arrangement with an administrator which is licensed or recognised within a Member State of the Community or in a reputable jurisdiction, the scheme shall ensure that the administrator shall apply measures that, as a minimum, are equivalent to those under the PMLFTR and the Implementing Procedures.

The outsourcing of the AML/CFT measures and procedures should be made by means of a written agreement between the scheme and the administrator, which may form part of the scheme administration agreement. The written agreement should clearly detail the respective responsibilities of each entity for the prevention of ML/FT and should expressly state that any document, data or information obtained by the administrator pursuant to such agreement shall be made available to the scheme upon request.

Notwithstanding the outsourcing arrangement between the scheme and the administrator, the scheme shall remain responsible for compliance with the requirements under the PMLFTR and the Implementing Procedures.

9.1 Compliance with CDD requirements

For the purpose of complying with its CDD requirements, the scheme shall require the administrator to submit a periodic report, at least once quarterly, which shall include a complete list of unit holders of the scheme, details of subscriptions and redemptions carried out by the unit holders within that period of time and a description of the CDD measures carried out by the administrator on the unit holders. The report should be drawn up by the MLRO of the administrator and transmitted to the Board of Directors of the scheme who shall be collectively responsible for reviewing the report.

On the basis of the report received from the administrator, the Board of Directors of the scheme shall ensure that the CDD measures being conducted by the administrator are in line with the requirements of the PMLFTR and the Implementing Procedures or, where the administrator is situated within a Member State of the Community other than Malta or in a reputable jurisdiction, with equivalent requirements.

Notwithstanding the fact that the reporting obligations have been outsourced to the administrator, should a suspicion of ML/FT be identified by the any member of the Board of Directors of the scheme, a report should be filed with the FIAU in accordance with Section 6.4.

9.2 Compliance with other AML/CFT requirements

Where the scheme has outsourced the implementation of AML/CFT measures and procedures to an administrator, such administrator shall be required to confirm to the Board of Directors of the scheme that the record-keeping, reporting, ongoing monitoring, risk management and any other measures being conducted by the administrator are in line with the requirements of the PMLFTR and the Implementing Procedures. Where the administrator is situated within a Member State of the Community other than Malta or in a reputable jurisdiction, the administrator will be required to confirm to the Board of Directors of the scheme that the record-keeping, reporting, ongoing monitoring, risk management and other measures comply with requirements within that jurisdiction which are equivalent to the measures under the PMLFTR and the Implementing Procedures.

9.3 When outsourcing is not permitted

This chapter shall only apply to those schemes which have no physical operational set-up in Malta as described in the first paragraph of this chapter. A scheme having a physical operational set-up in Malta and which is involved in the acceptance and processing of subscriptions and the collection of funds from investors may not outsource the implementation of their AML/CFT requirements.

APPENDIX I – Open Sources

- CIA World Factbook
  https://www.cia.gov/library/publications/the-world-factbook/index.html

- FATF
  http://www.fatf-gafi.org

- International Monetary Fund
  http://www.imf.org/

- International Narcotics Control Strategy Report
  http://www.state.gov/p/inl/rls/nrcrpt/2009/

- Malta Financial Services Authority (MFSA) (Sanctions Implementation)
  www.mfsa.com.mt

- NASD
  http://www.finra.org/index.htm

- OECD: uncooperative tax havens
  http://www.oecd.org/document/57/0,3343,en_2649_33745_30578809_1_1_1_1,00.html

- Transparency International's Corruption Perception Index
  http://www.transparency.org/policy_research/surveys_indices/cpi

- US Office of Foreign Assets Control
  http://www.treas.gov/offices/enforcement/ofac/sdn/index.shtml

- US State Department's list of major drug transit and major illicit drug producing countries
  http://www.state.gov/p/inl/rls/rpt/109777.htm

APPENDIX II – Common Understanding

COMMON UNDERSTANDING
between Member States on third country equivalence[1,2]
under the Anti-Money Laundering Directive (Directive 2005/60/EC)
June 2012

These third countries are currently considered as having equivalent AML/CFT systems to the EU. **The list may be reviewed**, in particular in the light of public evaluation reports adopted by the FATF, FSRBs, the IMF or the World Bank according to the revised 2003 FATF Recommendations and Methodology.

It should be noted that the list does not override the need to continue to operate the risk-based approach. The fact that a financial institution is based in a 3rd country featuring on the list only constitutes a refutable presumption of the application of simplified CDD. Moreover, the list does not override the obligation under article 13 of the Directive to apply enhanced customer due diligence measures in all situations which by their nature can present a higher risk of money laundering or terrorist financing, when dealing with credit and financial institutions, as customers, based in an equivalent jurisdiction.

List after the Meeting on 26 June 2012

Australia
Brazil
Canada
Hong Kong
India
Japan
South Korea
Mexico
Singapore
Switzerland
South Africa
The United States of America

1 Directive 2005/60/EC does not grant the European Commission a mandate to establish a positive list of equivalent third countries. The Common Understanding between EU Member States on Third Country Equivalence is drafted, managed and agreed by the EU Member States.

2 The list does not apply to Member States of the EU/EEA which benefit de jure from mutual recognition through the implementation of the 3rd AML Directive. The list also includes the French overseas territories (Mayotte, New Caledonia, French Polynesia, Saint Pierre and Miquelon and Wallis and Futuna) and Aruba, Curacao, Sint Maarten, Bonaire, Sint Eustatius and Saba. Those countries and territories are not members of the EU/EEA but are part of the membership of France and the Kingdom of the Netherlands of the FATF. The UK Crown Dependencies (Jersey, Guernsey, Isle of Man) may also be considered as equivalent by Member States.

APPENDIX III

GUIDANCE NOTE
ON
HIGH-RISK AND NON-COOPERATIVE JURISDICTIONS

A GUIDANCE NOTE ISSUED BY THE FIAU ON THE APPLICATION OF CERTAIN OBLIGATIONS UNDER THE PREVENTION OF MONEY LAUNDERING AND FUNDING OF TERRORISM REGULATIONS WITHIN THE CONTEXT OF THE PUBLIC DOCUMENTS ISSUED BY THE FINANCIAL ACTION TASK FORCE ON HIGH-RISK AND NON-COOPERATIVE JURISDICTIONS

Issued: 4th April 2012

1. A number of obligations under the Prevention of Money Laundering and Funding of Terrorism Regulations ("PMLFTR") require subject persons to assess the level of money laundering/funding of terrorism ("ML/FT") risk emanating from a particular jurisdiction and to determine whether a jurisdiction meets the criteria of a 'reputable jurisdiction' as defined under Regulation 2 of the PMLFTR. This guidance note 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.

The FATF Public Documents

2. 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 anti-money laundering/combating the financing of terrorism ("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 by each jurisdiction in addressing the deficiencies identified in their respect.[1]

3. 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 on-going 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.

4. 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.

5. Three different categories of higher-risk jurisdictions are therefore identified in the FATF public documents:

[1] For the latest list please refer to the website of the FIAU under the section 'Statements' (www.fiumalta.org/Statements).

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

Assessing and managing the ML/FT risk posed by a higher-risk jurisdiction

6. Regulation 4(1) requires subject persons to have in place procedures to manage the ML/FT risks posed by their customers, products and services. This obligation requires the development and establishment of effective customer acceptance policies in terms of Regulation 7(9). These procedures are mandatorily required in order for subject persons to be able to determine, *inter alia*, whether an applicant for business or a beneficial owner is likely to pose a higher risk of ML/FT. Among other things, a customer acceptance policy should include the identification of risks posed by a business relationship or a transaction to be established or carried out with a natural or legal person from a particular jurisdiction which is considered to pose a higher risk of ML/FT.

7. Section 4.1.1.2 (iv) of the FIAU's Implementing Procedure, citing the FATF Risk-Based Approach Guidance, 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 falling within Categories 1, 2 and 3 (refer to paragraph 5 above) 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 within their customer acceptance policy.

8. Where, on the basis of the subject person's customer acceptance policy, it is determined that a business relationship or a transaction is connected to a jurisdiction falling within Categories 1, 2 and 3, Regulation 7(9)(c) requires subject persons to conduct enhanced customer due diligence ("ECDD") in accordance with Regulation 11(1).[2] A connection to a jurisdiction falling within Categories 1, 2 and 3 may take various forms. For instance, a business relationship or a transaction shall be considered to be connected to a higher-risk jurisdiction falling within Categories 1, 2 and 3 if the applicant for business,[3] the beneficial owner, the source of funds/wealth or the business/economic activity is situated in or originates from such a

[2] It should be noted that the PMLFTR do not prohibit the establishment of a business relationship or the carrying out of a transaction with a person from a higher-risk jurisdiction but requires subject persons to apply enhanced due diligence measures.

[3] Whether such an application for business is a natural or legal person, including a financial institution as defined under the FATF Recommendations.

jurisdiction and shall therefore be subject to ECDD. However, not every form of connection to a higher-risk jurisdiction shall give rise to the requirement to apply ECDD. For instance, where a business relationship or a transaction involves an applicant for business who is a citizen of a higher-risk 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 a higher-risk jurisdiction, the requirement to apply ECDD does not arise.

9. Since Regulation 11(1) does not provide for any specific ECDD measures that must mandatorily be applied in situations which present a higher risk of ML/FT, subject persons are required to use their discretion in relation to business relationships or transactions connected to the jurisdictions falling within Categories 1, 2 and 3. However, the measures adopted must be applied on a risk-sensitive basis and be effective and proportionate to counter the ML/FT risk posed by each such jurisdictions.

10. Therefore, the enhanced due diligence measures to be applied in relation to a business relationship or a transaction connected to a jurisdiction falling within Category 1 should be more stringent than those applied in relation to a business relationship or a transaction connected to a jurisdiction falling within Category 2, since the ML/FT risks posed by the former category are considered to be higher. With respect to business relationships or transactions connected to a jurisdiction falling within Category 3, subject persons are required to assess the particular risk posed by the specific deficiencies identified by the FATF to determine which particular measures are effective and proportionate to counter that specific risk.

11. In order to assist subject persons in determining which enhanced due diligence measures should be applied, reference may be made to Section 4.1.2 of the FIAU's Implementing Procedures which provides for the procedures to be applied to control and mitigate higher-risk situations. Such procedures include the following:
    (a) the implementation of a programme which sets out the additional measures to be applied by the subject person in relation to the jurisdictions listed in the FATF public documents, such as for instance requiring additional information and documentation to be supplied by the customer than would normally be required;
    (b) requiring a higher standard in relation to the quality of documents obtained;
    (c) monitoring transactions/activities to a higher degree.

12. In relation to paragraph (c) above, it should be noted that Regulation 15(2) specifically requires subject persons to pay special attention to business relationships and transactions with persons, companies and undertakings, including those carrying out relevant financial business or a relevant activity, from a non-reputable jurisdiction (refer to paragraph 13 below), and, whenever the transactions involved have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible, be examined. In such cases, written findings should be made available to the FIAU and the relevant supervisory authority.[4] Therefore, subject persons are required to pay special attention to business

[4] The findings established by subject persons should not be automatically reported to the FIAU but should be made available to the FIAU and the relevant supervisory authority if and when the subject person is requested to do so. However, in the event that the findings of the subject person indicate a suspicion or knowledge of ML/FT, a report should be filed with the FIAU in accordance with Regulation 15(6) of the PMLFTR.

relationships and transactions with persons from the jurisdictions falling within Categories 1 and 2 and where considered necessary Category 3. Whenever the transactions involved have no apparent economic or visible lawful purpose subject persons shall proceed in accordance with the measures set out in this paragraph.

The reputability of a jurisdiction

13. Regulation 2 defines a reputable jurisdiction as any country having legislative measures for the prevention of ML/FT, taking into account that country's membership of, or any declaration or accreditation by, any international organisation recognised as laying down internationally accepted standards for the prevention of money laundering and for combating the funding of terrorism, and which supervises natural and legal persons subject to such legislative measures for compliance therewith. Hence, for the purpose of the PMLFTR, the jurisdictions falling within Categories 1 and 2 shall not be considered to meet the criteria of a reputable jurisdiction as they do not have adequate legislative measures for the prevention of ML/FT and a clear and unequivocal declaration has been issued by the FATF in that respect. Those jurisdictions falling within Category 3 shall not automatically be considered to be non-reputable and subject persons are required to determine the reputability of each jurisdiction on the basis of the deficiencies identified by the FATF.

14. Subject persons shall not apply the simplified due diligence measures set out under Regulation 10, the reliance provisions set out under Regulation 12 and the provisions on permissible disclosures set out under Regulation 16 in relation to a business relationship or transaction connected to jurisdictions falling within Categories 1 and 2 and, where considered necessary, Category 3.

15. Additionally, in terms of Regulation 6(1) subject persons carrying out relevant financial business may not establish or acquire branches or majority owned subsidiaries in a jurisdiction falling within Categories 1 and 2 and, where considered necessary, Category 3.

Counter-measures

16. The FATF has called on its members and has urged all other jurisdictions, including Malta, to apply effective counter-measures to protect their financial sectors from ML/FT risks emanating from the jurisdictions falling within under Category 1. Such jurisdictions have not achieved any progress and have not made any commitment to implement an action plan to address their deficiencies, despite the numerous attempts by the FATF to engage in such a process.

17. Since the FATF does not specify the counter-measures which are to be applied in relation to such jurisdictions, every jurisdiction may determine the counter-measures that are to be applied. In this regard, reference shall be made to Regulation 15(3) which states that subject persons are required to inform the FIAU of any business relationships or transactions with persons, companies and undertakings, including those carrying out relevant financial business or a relevant activity from a non-reputable jurisdiction which continues not to apply measures equivalent to those laid down in the PMLFTR. In relation to such business relationships or transactions, the FIAU may, in collaboration with the relevant supervisory authority, require

such business relationships not to continue or such transactions not to be carried out. The FIAU may also apply any counter-measures as may be adequate under the respective circumstances.

18. For the purpose of Regulation 15(3) the jurisdictions falling under Category 1 shall be considered to be non-reputable jurisdictions which continue not to apply measures equivalent to those laid down in the PMLFTR. Subject persons are therefore required to inform the FIAU, in writing, of any business relationships or transactions with such jurisdictions, in relation to which the FIAU may take the actions set out under Regulation 15(3).

19. In addition to informing the FIAU, banks are required to take measures to ensure that any correspondent banking relationships they may have in place are not being used to bypass or evade any counter-measures and risk mitigation practices by any person having a link to the jurisdictions falling within the first category of the FATF Public Statement.

Status of this Guidance Note

20. This guidance note is being issued in terms of Regulation 17(1), which shall therefore be binding on all subject persons. Failure to comply with this guidance note shall render subject persons liable to an administrative penalty of not less than two hundred and fifty euro (€250) and not more than two thousand five hundred euro (€2,500) in terms of Regulation 17(2). Penalties imposed under Regulation 17(2) shall be imposed by the FIAU without recourse to a court hearing and may be imposed either as a one time penalty or a daily cumulative basis until compliance, provided that in the latter case the accumulated penalty shall not exceed twelve thousand five hundred euro (€12,500).