PROCEDURES AND GUIDANCE
IMPLEMENTING THE PROVISIONS OF THE
PREVENTION OF MONEY LAUNDERING AND
FUNDING OF TERRORISM REGULATIONS

PART I

Consultation Document

Issued: August 2010
CONTENTS PAGE

ABBREVIATIONS 07

CHAPTER 1 – INTRODUCTION 08
1.1 Who are the Procedures and Guidance for? 08
1.2 Purpose of the Procedures and Guidance 10
1.3 How should the Procedures and Guidance be used? 10
1.4 Status of the Procedures and Guidance 11

CHAPTER 2 – OVERVIEW 12
2.1 What is money laundering? 12
2.2 What is funding of terrorism? 13
2.3 Legislation on money laundering and funding of terrorism 14
   2.3.1 The Prevention of Money Laundering Act 14
   2.3.2 The Prevention of Money Laundering and Funding of
       Terrorism Regulations 15
2.4 The Financial Intelligence Analysis Unit 16

CHAPTER 3 – CUSTOMER DUE DILIGENCE 17
3.1 Application of CDD measures 17
   3.1.1 Identification and verification of the applicant for business 18
      3.1.1.1 Who is the applicant for business? 18
      3.1.1.2 The nature of identification and verification of a
          natural person 19
      3.1.1.3 The nature of identification and verification of a
          legal person 21
   3.1.2 Identification and verification of the beneficial owner 21
      3.1.2.1 Who is the beneficial owner? 22
      3.1.2.2 Verification of the identity of the beneficial owner 26
   3.1.3 Applicant for business not acting as principal 26
      3.1.3.1 When the principal is a natural person 26
      3.1.3.2 When the principal is a public company 26
      3.1.3.3 When the principal is a private company 28
      3.1.3.4 When the principal is a commercial partnership 30
      3.1.3.5 When the principal is a foundation or association 31
      3.1.3.6 When the principal is a trustee of a trust 32
3.1.4 Information on the purpose and intended nature of the business relationship

3.1.5 Ongoing monitoring of the business relationship

3.1.6 Source of wealth and source of funds

3.2 Timing of CDD procedures

3.2.1 Timing of CDD when establishing a business relationship

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

3.2.2 Timing of CDD in relation to existing customers

3.2.3 Timing of CDD when an occasional transaction is carried out

3.2.4 Timing of CDD when there is a suspicion of ML/FT

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

3.3 Failure to complete CDD measures laid out in Regulation 7(1)(a) to (c)

3.4 Simplified Due Diligence

3.4.1 Categories of applicants for business qualifying for SDD

3.4.2 Circumstances where SDD shall not apply

3.5 Enhanced Due Diligence

3.5.1 Non face-to-face applicants for business

3.5.2 Correspondent banking relationships

3.5.3 Politically Exposed Persons

3.5.3.1 Who qualifies as a PEP?

3.5.3.2 EDD measures to be applied in relation to PEPs

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

3.6 Reliance on other subject persons or third parties

3.6.1 CDD measures that may be relied on

3.6.2 Who qualifies as a third party?

3.6.3 Responsibility for compliance with CDD measures

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

3.6.4.1 Exception

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

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

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

3.6.8 When reliance is not applicable
CHAPTER 4 – MANDATORY RISK PROCEDURES AND THE RISK-BASED APPROACH

4.1 Mandatory risk procedures
4.1.1 Risk-assessment procedures
4.1.1.1 Purpose of risk-assessment procedures
4.1.1.2 Identifying and assessing the risks
4.1.2 Risk-management procedures

4.2 The Risk-Based Approach
4.2.1 The purpose of the RBA
4.2.2 The application of the RBA
4.2.2.1 Identifying and assessing the risks
4.2.2.2 Obtaining a risk profile
4.2.2.3 Managing and controlling risks
4.2.2.4 Monitoring controls
4.2.2.5 Recording the action taken

CHAPTER 5 – RECORD KEEPING PROCEDURES

5.1 Purpose of keeping records
5.2 Records to be retained
5.3 Period of retention of records
5.3.1 CDD documentation
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
5.3.3 Records in relation to the background and purpose of a complex or large transaction
5.4 Form of records
5.5 Retrieval of records

CHAPTER 6 – REPORTING PROCEDURES AND OBLIGATIONS

6.1 The Money Laundering Reporting Officer
6.2 The designated employee
6.3 Internal reporting procedures
6.4 External reporting procedures
6.5 Actions after reporting
6.6 Request to carry out a transaction known or suspected to be related to ML/FT
6.7 Professional privilege 70
6.8 Complex or large transactions 70
6.9 Business relationships and transactions with persons from a non-reputable jurisdiction 71
6.10 Prohibition of disclosures 71
6.11 Permissible disclosures 72
6.12 Annual Compliance Report 73
6.12.1 Contents of the Annual Compliance Report 74
6.12.2 The submission period 74
6.12.3 Actions by the FIAU after receiving the Report 75

CHAPTER 7 – AWARENESS, TRAINING AND VETTING OF EMPLOYEES 76
7.1 Employee awareness 76
7.2 Nature of training 77
7.3 Timing of awareness training 77
7.4 Vetting of new employees 78

CHAPTER 8 – OTHER ISSUES 79
8.1 The notion of reputable jurisdiction 79
8.2 Branches and subsidiaries 81
8.3 Written procedures 81
8.4 Offences and penalties 82
8.4.1 Offences and contraventions under the PMLFTR 82
8.4.1.1 Non-compliance with procedures to prevent ML/FT 82
8.4.1.2 Non-compliance with procedures to prevent ML/FT by corporate/unincorporated bodies/other associations of persons 82
8.4.1.3 False declaration/false representation by an applicant for business 83
8.4.1.4 Contravention of the provisions on customer due diligence 83
8.4.1.5 Contravention of the provisions on reporting procedures and obligations 83
8.4.1.6 Tipping off 83
8.4.2 Offences under the PMLA 84
8.4.2.1 Money laundering offence 84
8.4.2.2 Disclosure of an investigation/attachment order 85
8.4.2.3 Acting in contravention of an investigation/attachment order 85
8.4.2.4 Acting in contravention of a freezing order 85
8.4.3 Offence of Funding of Terrorism (Criminal Code) 86
APPENDICES

Appendix I – Open Sources 87
Appendix II – STR Template 88

FIGURES

Figure 1 – Illustration I of beneficial owner 23
Figure 2 – Illustration II of beneficial owner 24
Figure 3 – Determination of risk-appetite 57
Figure 4 – Customer falling within the risk-appetite 58
Figure 5 – Customer falling outside the risk-appetite 58

TABLES

Table 1 – Definition of a beneficial owner 22
Table 2 – Risk scoring grid 57
## ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML/CFT</td>
<td>Anti-money laundering/combating funding of terrorism</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer due diligence</td>
</tr>
<tr>
<td>EDD</td>
<td>Enhanced customer due diligence</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>FSRB</td>
<td>FATF Style Regional Body</td>
</tr>
<tr>
<td>FIAU</td>
<td>Financial Intelligence Analysis Unit</td>
</tr>
<tr>
<td>FIU</td>
<td>Financial Intelligence Unit</td>
</tr>
<tr>
<td>JMLSG</td>
<td>Joint Money Laundering Steering Group</td>
</tr>
<tr>
<td>MFSA</td>
<td>Malta Financial Services Authority</td>
</tr>
<tr>
<td>ML/FT</td>
<td>Money laundering and funding of terrorism</td>
</tr>
<tr>
<td>MLRO</td>
<td>Money Laundering Reporting Officer</td>
</tr>
<tr>
<td>MONEYVAL</td>
<td>The Council of Europe Select Committee of Experts on the Evaluation of anti-Money Laundering Measures and the Financing of Terrorism</td>
</tr>
<tr>
<td>PEP</td>
<td>Politically exposed person</td>
</tr>
<tr>
<td>PMLA</td>
<td>Prevention of Money Laundering Act</td>
</tr>
<tr>
<td>PMLFTR</td>
<td>Prevention of Money Laundering and Funding of Terrorism Regulations</td>
</tr>
<tr>
<td>RBA</td>
<td>Risk-Based Approach</td>
</tr>
<tr>
<td>SDD</td>
<td>Simplified customer due diligence</td>
</tr>
<tr>
<td>STR</td>
<td>Suspicious transaction report</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
</tbody>
</table>
CHAPTER 1 – INTRODUCTION

1.1 Who are the Procedures and Guidance for?

The Procedures and Guidance Implementing the Provisions of the Prevention of Money Laundering and Funding of Terrorism Regulations, hereinafter referred to as ’Procedures and Guidance’, are intended for those persons, whether natural or legal, referred to in the PMLA and the PMLFTR 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.
3 Article 14 of the PMLA and Regulation 2 of the PMLFTR respectively.
4 Regulation 2 of the PMLFTR.
Consultation Document

(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' 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;

(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 Procedures and Guidance to 'Community' shall be construed in accordance with the definition provided in the PMLFTR.
1.2 Purpose of the Procedures and Guidance

The purpose of these Procedures and Guidance 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 Procedures and Guidance 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 Procedures and Guidance may be subject to amendments to maintain them continually 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

1.3 How should the Procedures and Guidance be used?

The Procedures and Guidance 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, nature and business activity. The manner in which this flexibility is to be exercised is explained in detail in different parts of these Procedures and Guidance.

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. 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

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 blueprint 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_1,00.html.
rule subject persons are required to manage their ML/FT risks in the most appropriate and proportionate manner in accordance with the risks identified pursuant to the carrying out of a risk assessment. The Procedures and Guidance assist subject persons in achieving this objective within the parameters of the law.

The Procedures and Guidance are divided into two parts. Part I contains general guidance that applies across all sectors falling within the definition of ‘relevant activity’ and ‘relevant financial business’. Part II comprises sector-specific guidance, which is incomplete on its own and must be read in conjunction with Part I of the Procedures and Guidance.³⁸

A reading of the Procedures and Guidance should not be construed as a substitute for a reading of the PMLFTR.

1.4 Status of the Procedures and Guidance

These Procedures and Guidance are being issued under Regulation 17 of the PMLFTR, which empowers the FIAU to issue such Procedures and Guidance for the carrying into effect of the provisions of the PMLFTR. In accordance with this Regulation, these Procedures and Guidance are binding on all subject persons. A subject person who fails to comply with these Procedures and Guidance shall be 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).³⁹ The PMLFTR provide that 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 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).⁴⁰

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

---

³⁸ Part I of the Procedures and Guidance will be issued prior to the completion of Part II and shall be binding on subject persons as from the date of such issuance and upon being placed on the FIAU website.
³⁹ Regulation 15(15) of the PMLFTR.
⁴⁰ Regulation 15(16) of the PMLFTR.
CHAPTER 2 – OVERVIEW

2.1 What is money laundering?

Money laundering is the process by which the illegal nature of criminal proceeds is 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 were 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 laundering¹¹ 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;"

¹¹ 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 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. 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.

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.

---

^* Article 328A of the Criminal Code (Cap. 9 of the Laws of Malta) provides a definition of acts of terrorism.

13 FATF, Guidance for Financial Institutions in Detecting Terrorist Financing, April 2002, pp. 4-5, paragraph 12, 13 and 16.

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.\textsuperscript{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 1994, when the PMLA was enacted together with the original regulations issued thereunder. The PMLA was eventually amended to include the funding of terrorism which was criminalised through 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 reflect Malta’s 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 23\textsuperscript{rd} 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 XXI of 2008.

The first part of the PMLA provides a definition of money laundering (refer to Section 2.1) and criminalises the act of money laundering.\textsuperscript{16} 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.\textsuperscript{17} 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.\textsuperscript{18} The PMLA also provides a definition of criminal activity\textsuperscript{19} and property.\textsuperscript{20} Originally, the PMLA only applied to a limited list of predicate offences,\textsuperscript{21} however since 31\textsuperscript{st} 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

\textsuperscript{15} Ibid, p.5, paragraph 15.
\textsuperscript{16} Article 3(1) of the PMLA.
\textsuperscript{17} 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.
\textsuperscript{18} Article 3(2) of the PMLA.
\textsuperscript{19} Article 2(1) of the PMLA.
\textsuperscript{20} Article 2(1) of the PMLA.
\textsuperscript{21} The predicate offence is the underlying criminal activity from which the illegal funds originate.
offence’, whenever or wherever it is carried out, may constitute the basis for the offence of money laundering.  

The PMLA lays down the procedures for the prosecution of a money laundering offence as well as the measures for the confiscation of property upon a conviction of money laundering, measures for the freezing of assets when a person is charged with an offence of money laundering 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. 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 legislative developments within the European Union and at an international level. In fact the PMLFTR transpose the 3rd AMLDirective which, in turn, is modelled on the FATF Forty Recommendations and the Nine Special Recommendations.

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:

- customer due diligence;
- record keeping;
- internal reporting;
- training; and

---

22 Article 2(1) of the PMLA.
23 Article 3(2A), (3), (4), (6) and (7) of the PMLA.
24 Article 3(5) of the PMLA.
25 Article 5 of the PMLA.
26 Article 4 of the PMLA.
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 and is the authority responsible for the administration and 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 remain in the domain of 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 receiving and analysing 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, and monitoring and ensuring compliance by subject persons with their obligations under the PMLFTR.

The Unit has a wide-ranging power to demand information. In fact, where a suspicion of ML/FT exists or upon receipt of a suspicious transaction report, 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 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.
CHAPTER 3 – CUSTOMER DUE DILIGENCE

This chapter provides procedures and guidance 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 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);
- 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.  

28 Regulation 7(4) of the PMLFTR.
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. For the purposes of fulfilling the obligation imposed on subject persons for the purposes of combating the funding of terrorism, such procedures should also include a system which detects whether an applicant for business is subject to any financial sanctions issued by the UN Security Council or the EU. For reference to such sanctions subject persons may wish to consult the ‘Sanctions Implementation’ section on the website of the MFSA.29

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.30

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 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.

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,31 must comprise three important cumulative elements, which are the following:

(i) the relationship must be of a business, professional or commercial nature;
(ii) the relationship must subsist for a period of time; and
(iii) 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.32

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:

30 Regulation 2 of the PMLFTR.
31 Ibid.
32 Ibid.
(i) 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;
(ii) a transaction which involves a money transfer or remittance amounting to one thousand euro (€1,000) or more; and
(iii) a transaction amounting to two thousand euro (€2,000) or more referred to in Regulation 9 of the PMLFTR.33

It is worth noting that the PMLFTR do not define ‘customer’. The meaning of this word, therefore, has to be inferred from the definition of ‘business relationship’ in the PMLFTR, 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.

**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:

- official full name;
- place and date of birth;
- permanent residential address;
- identity reference number, where available; and
- nationality.

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

**Verification** takes place by making reference to documents, data or information obtained 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 EU34 or in a reputable jurisdiction, since these entities would have already checked the existence and characteristics of the persons concerned.

The verification of the details provided by the person on his identity may be carried out through the following methods:35

---

33 This obligation only applies to casino licensees.
34 For the purpose of this document, references to an EU Member State include reference to an EEA State.
35 These methods apply only in those instances where verification is carried out on a face-to-face basis. For guidance on the measures to be carried out in relation to verification on a non face-to-face basis reference should be made to Section 3.5.1.
(a) Reference to a government-issued document providing photographic evidence of identity:
   - valid unexpired passport; or
   - valid unexpired national identity card; or
   - valid unexpired driving licence.

In order to verify the identity of the applicant for business where the applicant for business is present for verification purposes, 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 subject person.

In those situations where the applicant for business is not present for verification purposes, subject persons are required to obtain a certified true copy of the original documents provided by the applicant for business. Certification should be carried out by a legal professional, accountancy professional, a notary, a person undertaking relevant financial business or any other third party, as defined in Section 3.6.2, undertaking equivalent activities to such persons.

Generally, such certification is 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 in capitals underneath) and clearly indicate his position 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 considering certified copy documents, especially where such documents originate from a country or territory perceived to represent a higher risk.

(b) Residential address:
   - recent statement from a recognised credit institution;
   - 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 (a) above, where a clear indication of residential address is provided.

Documents, other than official government issued ones, must not be more than three months old.

Subject persons may also verify the identity of a natural person through electronic means, especially in non face-to-face situations. 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 rely on the services provided by such a provider for the purposes of verification if the provider satisfies all of the following criteria:

- it is authorised by the relevant authorities in that jurisdiction to provide such services;
- it carries out processes to identify and verify the identity of the applicant for business and/or the beneficial owner on a face-to-face basis; and
- it is authorised to store personal data and is not precluded from transferring information maintained in relation to the applicant for business and/or beneficial owner to the subject person.

### 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. For the purposes of fulfilling the obligation imposed on subject persons for the purposes of combating the funding of terrorism, subject persons should have a system in place to detect whether the legal person is subject to any financial sanctions issued by the UN Security Council or the EU. For reference to such sanctions subject persons may wish to consult the ‘Sanctions Implementation’ section on the website of the MFSA.36

### 3.1.2 Identification and verification of the beneficial owner

Subject persons are required to identify the beneficial owner, where applicable, 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.37

In certain exceptional circumstances, where it may be difficult to determine who the beneficial owner is with certainty, subject persons may 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 himself.

For the purposes of fulfilling the obligation imposed on subject persons for the purposes of combating the funding of terrorism, subject persons should have a system in place to detect whether the beneficial owner is subject to any financial sanctions issued by the UN Security Council or the EU. For reference to such sanctions subject persons may wish to consult the ‘Sanctions Implementation’ section on the website of the MFSA.38

37 Regulation 7(1)(b) of the PMLFTR.
3.1.2.1 Who is the beneficial owner?

Regulation 2 defines a beneficial owner as a:

(a) **natural** person who ultimately owns or controls the customer; and/or
(b) **natural** person on whose behalf 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.

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.

<table>
<thead>
<tr>
<th>(a) Body corporate or body of persons</th>
<th>(i) A natural person/s that has:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Direct ownership of 25% shares (including bearer shares); or</td>
</tr>
<tr>
<td></td>
<td>• Direct ownership of 25% voting rights; or</td>
</tr>
<tr>
<td></td>
<td>• Direct control of 25% shares (including bearer shares); or</td>
</tr>
<tr>
<td></td>
<td>• Direct control of 25% voting rights; or</td>
</tr>
<tr>
<td></td>
<td>• Indirect ownership of 25% shares (including bearer shares) ; or</td>
</tr>
<tr>
<td></td>
<td>• Indirect ownership of 25% voting rights; or</td>
</tr>
<tr>
<td></td>
<td>• Indirect control of 25% shares (including bearer shares); or</td>
</tr>
<tr>
<td></td>
<td>• Indirect control of 25% voting rights.</td>
</tr>
<tr>
<td>(ii)</td>
<td>A natural person who otherwise exercises control over the management of that body corporate or body of persons.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(b) Legal entity or legal arrangement which administers and distributes funds</th>
<th>(i) Determined beneficiaries - natural persons who are the beneficiaries of at least 25% of the property</th>
</tr>
</thead>
<tbody>
<tr>
<td>(ii)</td>
<td>Non-determined beneficiaries – the class of persons in whose main interest the legal entity or arrangement is set up or operates</td>
</tr>
<tr>
<td>(iii)</td>
<td>A natural person who controls at least 25% of the property of the legal entity or arrangements</td>
</tr>
</tbody>
</table>

| (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.

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.

- Natural persons not required to be identified as a beneficial owner
- Legal persons
- Natural persons required to be identified as a beneficial owner

**Figure 1 - Illustration I of beneficial owner**

In Figure 1 subject persons are required to determine the natural persons who ultimately own 25% or more 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 3 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 person 2 and natural person 4 ultimately hold 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 25% or more 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.
This provision refers to those natural persons who, notwithstanding the fact that they own or control less than 25% 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. For instance, a natural person holding 20% of the shares in a company would be considered to exercise control over the management of that company where all the other beneficial owners own 1% each of the shares in that company. Similarly, in a situation where five natural persons own 20% each of the shares in a company, subject persons should identify such persons as the beneficial owners of that company.

Reference should also 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. Subject persons are therefore required to request such information directly from the
applicant for business, and where the applicant for business confirms that such person exists, a
document 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, 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 the person who is the beneficiary of at least 25% of the property of a trust, subject persons are required to request the trustee of the trust to produce the trust deed or an extract thereof 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.

(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 or an extract thereof 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 be controlling the beneficiary stated in the trust deed and would therefore be the actual beneficiary for the purposes of this sub-regulation. The beneficiary appearing on the trust deed should therefore be made to sign a declaration stating that he is not acting on behalf of anyone else. This would obviously not apply in the case of beneficiaries who are not aware of the existence of the trust. In such cases the trustee would be required to make a declaration himself.

39 In certain jurisdictions a trust is considered by law to have a legal personality separate from that of the trustee.
(c) in the case of long-term insurance business, the beneficial owner shall be construed to be the beneficiary under the policy.

In order to determine the beneficial owner in the case of long-term insurance business, subject persons are required to request a copy of the policy document revealing the identity of the beneficiary of the policy.

3.1.2.2 Verification of the identity of the beneficial owner

The verification of identity of the beneficial owner should be carried out in accordance with Section 3.1.1.2. Where the beneficial owner is not present for the purposes of verification, subject persons are required to apply EDD measures in accordance with Section 3.5.1.

In the case of a body corporate, a trust and similar legal arrangements, subject persons must take reasonable measures to understand its ownership and control structure. Such measures are laid out in more detail in Sections 3.1.3.2 to Section 3.1.3.6 below.

3.1.3 Applicant for business not acting as principal

The applicant for business may be acting on behalf of someone else, in which case subject persons must not only identify and verify the applicant for business but they are also required to apply additional measures.

These additional measures will depend on whether the person on whose behalf the applicant for business is acting is a natural or legal person. 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.

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 procedures to be applied with respect to the principal are those laid out in Section 3.1.1.2, whereas the verification procedures to be applied are those laid out in Section 3.1.2.2.

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 may not be applied. In this case the subject person must first identify the public company by gathering the following information:
Consultation Document

- official full name;
- registration number;
- date of incorporation or registration; and
- 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 on the basis of one or more of the following documents, as the case may be:

- a copy of 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;
- a copy of the Memorandum and Articles of Association or other statutory document.

Where the documents provided are copies of the originals, subject persons must ensure that the copies are certified by the company secretary, a director or an officer occupying an equivalent position.

Once the verification is complete, the subject person must identify all the directors. This may be done by either referring to the Memorandum and Articles of Association, by performing a company registry search or by obtaining a copy of the directors’ register of the company. 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 an explanation of the ownership and control structure of the company from the applicant for business, as well as an organisation chart of the company. Once these are obtained subject persons should then conduct independent research by consulting online commercial databases or company registries. In order to verify the ownership and control structure, subject persons should obtain a certificate of good standing or any similar or equivalent document (such as a certificate of incumbency) or else by requesting a company registry scan, where applicable.

Finally, the subject person 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 ensure that the applicant for business keeps the subject person informed of any changes in the beneficial ownership.

This procedure 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 should also be noted that where any one of the shareholders of the company is a public company, a private company or other legal entity, then the subject person is required to repeat the specific procedures applicable under Section 3.1.3 in relation to such shareholder.
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. Therefore, subject persons should consider alternative ways of conducting their identification and verification procedures.

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;
- a copy of the Board Resolution authorising the entering into of a business relationship or an occasional transaction; 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, dated, signed and certified.

### 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:
- the company's official full name;
- the company's registration number;
- the company's date of incorporation or registration; and
- 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 on the basis of one or more of the following documents, as the case may be:
- a copy of 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; or
- a copy of the Memorandum and Articles of Association or other statutory document.

Where the documents provided are copies of the originals, subject persons must ensure that the copies are certified by the company secretary, a director, or an officer occupying an equivalent position.

Once the verification is complete, the subject person must identify all the directors. This may be done by either referring to the Memorandum and Articles of Association, by performing a company
registry search or by obtaining a copy of the directors' register of the company. 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 an explanation of the ownership and control structure of the company from the applicant for business, as well as an organisation chart of the company. Once these are obtained subject persons should then conduct independent research by consulting online commercial databases or company registries. In order to verify the ownership and control structure, subject persons should obtain a certificate of good standing or any similar or equivalent document (such as a certificate of incumbency) or else by requesting a company registry scan, where applicable.

Finally, the subject person 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 ensure that the applicant for business keeps the subject person informed of any changes in the beneficial ownership.

This procedure 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 should also be noted that where any one of the shareholders of the company is a public company, a private company or other legal entity, then the subject person is required to repeat the specific procedures applicable under Section 3.1.3 in relation to such shareholder.

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 Regulations. Therefore, subject persons should consider alternative ways of conducting their identification and verification procedures.

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;
- a copy of the Board Resolution authorising the entering into a business relationship or an occasional transaction; 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, dated, signed and certified.

**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:

- the partnership’s official full name;
- the partnership’s registration number;
- the partnership’s date of incorporation or registration; and
- 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 on the basis of one or more of the following documents, as the case may be:

- a copy of 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;
- a copy of the partnership agreement or other statutory document.

Where the documents provided are copies of the originals, subject persons must ensure that the copies are certified by the partners.

Once the verification is complete, the subject person must identify all the persons vested with the partnership’s administration and representation. This may be done by either referring to the partnership agreement or by performing a registry search. 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 an explanation of the ownership and control structure of the partnership from the applicant for business, as well as an organisation chart of the partnership. Once these are obtained subject persons should then conduct independent research by consulting online commercial databases or company registries. In order to verify the ownership and control structure, subject persons should obtain a certificate of good standing or any similar or equivalent document (such as a certificate of incumbency) or else by requesting a registry scan, where applicable.

Finally, the subject person 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 ensure that the applicant for business keeps the subject person informed of any changes in the beneficial ownership.
This procedure 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 should also be noted that where any one of the partners of the partnership is a public company, a private company or other legal entity, then the subject person is required to repeat the specific procedures applicable under Section 3.1.3 in relation to such partner.

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. Therefore subject persons should consider alternative ways of conducting their identification and verification procedures.

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 Partnership’s Register;
- information from independent sources such as, for instance, business information services;
- a copy of the Resolution authorising the entering into of the business relationship or an occasional transaction; 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, dated, signed and certified.

### 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:

- the foundation or association’s official full name;
- the foundation or association’s registration number;
- the foundation or association’s date of registration; and
- the foundation or association’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 foundation or association on the basis of one or more of the following documents, as the case may be:

- a copy of the certificate of registration;
- a copy of the constitutive document.
Where the documents provided are copies of the originals, subject persons must ensure that the copies are certified by the administrators.

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 may 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 an explanation of the ownership 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.

Finally, the subject person 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 ensure that the applicant for business keeps the subject person informed of any changes.

This procedure 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, dated, signed and certified.

3.1.3.6 When the principal is a trustee of a trust

Where the applicant for business is a trustee acting on behalf 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:

- the full name of the trust;
- the nature and purpose of the trust; and
- the country of establishment.

This information may 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 containing the necessary information would suffice.

The subject person may also consider obtaining a copy of the MFSA's authorisation for that person to act as a trustee.

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 (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 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.

### 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 only 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);
- (d) the anticipated level and nature of the activity that is to be undertaken through the relationship;
- (e) in the case of a business activity, copies of recent and current financial statements.
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:\(^{40}\)

(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. The PMLFTR further require that in monitoring a business relationship subject persons should pay special attention to any large, unusual complex transactions or unusual patterns of transactions which have no apparent or visible economic or lawful purpose (refer to Section 6.8). Where it is revealed that the customer’s business and 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 subject person. The subject person 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 accordance with paragraph (b) above, subject persons are not only required to keep up-to-date documents, data or information held by the subject person in the fulfilment of its CDD obligations but are also required to ensure that any documents, data or information in relation to the transactions conducted by the customer are updated on an ongoing basis. 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.

\(^{40}\) Regulation 7(2) of the PMLFTR.
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 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 updated from time to time in the case of new material developments arising 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 for a particular transaction or utilised generally in the context of a business relationship.

Depending on circumstances surrounding that transaction, the scrutiny of transactions may take place either in real time as the transaction is taking place or after the event, through a review of the transactions or activities that the customer has carried out. Monitoring should 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 Procedures and Guidance 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:

(a) to all applicants for business when seeking to establish a business relationship;

---

41 Regulation 7(5) to (7) of the PMLFTR.
(b) to existing customers when appropriate or when the subject person becomes aware that changes have occurred in the circumstances surrounding the established business relationship;
(c) to all applicants for business when seeking to carry out an occasional transaction;
(d) when the subject person suspects that a transaction may involve ML/FT; or
(e) 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.

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

(i) Specific exceptions in relation to certain circumstances

Notwithstanding the obligation to complete verification procedures prior to the establishment of a business relationship, the PMLFTR provide that verification procedures may be completed during the establishment of a business relationship where:

(a) it is necessary for the continued normal conduct of business; provided that
(b) the risk of ML/FT is low; and provided further that
(c) the verification procedures be completed as soon as is reasonably practicable after the initial contact. 42

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.

42 Regulation 8(2) of the PMLFTR.
(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, provided that adequate measures are put in place such that no transactions are carried out through the account until the verification procedures have been satisfactorily completed.

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

There may be other situations, particularly in the area of trusts 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 identified. 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 their identity is established.

### 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.

This provision 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 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 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.

Subject persons are also required to ensure that the documents, data or information held are kept up to date in accordance with the ongoing monitoring obligations. Therefore, subject persons are required to have a system in place in order to update CDD documentation whenever the need arises, e.g. to update expired passports (refer to Section 3.1.5).

### 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.

### 3.2.4 Timing of CDD when there is a suspicion of ML/FT

Regardless of any exemption or threshold, 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.

### 3.2.5 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.
3.3 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, where applicable:

(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; and
(d) 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 the verification procedure is due to serious reasons 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 reference number or a passport number. In such 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.

Moreover, in deciding whether to opt for one of the measures 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 specified 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
Consultation Document

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 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 who 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, 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. Subject persons shall ensure that supporting identification documentation is available, or may be made available on request, to the 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).

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.

43 Cap. 345 of the Laws of Malta.
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.

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 and prohibit subject persons from applying the provisions dealing with SDD.

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:

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

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 by producing an identification document containing a photograph. 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 any other third party, as defined in Section 3.6.2, undertaking equivalent activities to such persons.

Generally, such certification is 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 in capitals underneath) and clearly indicate his position 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 considering 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 a relevant financial activity;
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.

(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\(^{44}\) 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. Although not required by the PMLFTR, it would also be appropriate for credit institutions to apply the required measures to cross-border correspondent banking relationships established in a Member State of the Community.

Where a credit institution seeks to establish such correspondent banking relationship it has to ensure that:

(a) it fully understands and documents the nature of the business activities of its respondent institution, including from publicly available information:

   (i) the reputation of the institution;
   (ii) the quality of supervision on that institution; and
   (iii) 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:

\(^{44}\) Cap. 371 of the Laws of Malta.
(i) 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

(ii) 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

(iii) 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;

The senior management of a credit institution is generally the executive body of the credit institution which is at the highest level of the organisational management structure and holds executive powers conferred onto it with and by the authority of the Board of Directors of the credit institution. 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 preferably 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 identify all PEPs. The PMLFTR however require the application of EDD only to those 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:
   (i) joint beneficial ownership of a body corporate or any other form of legal arrangement;
(ii) 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 request such information directly from the applicant for business and consider making use of commercial databases set up for such purposes to confirm the information provided by the applicant for business. The development of 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, could serve as an effective document for identifying PEPs. This questionnaire should be signed by the applicant for business and the beneficial owner, where applicable.

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;

The senior management of a credit institution is generally the executive body of the credit institution which is at the highest level of the organisational management structure and holds executive powers conferred onto it with and by the authority of the Board of Directors of the credit institution. 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 guidance refer 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 guidance on ongoing monitoring refer 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 subject persons should have in place mechanisms and procedures to carry out a risk assessment to identify and establish 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 information obtained by the entity being relied on should be made immediately available to the subject person placing reliance. Therefore, notwithstanding the fact that the subject person is placing reliance on another entity, the subject person must have 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.

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 shall request 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. 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.

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 or in a reputable jurisdiction; 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 persons 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;
- 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 3.6.1 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:

- 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. 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;
- 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.

Furthermore, if 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. Although, the FIAU has adopted the list of equivalent countries agreed upon by the Member States of the European Union, subject persons should however refer to the definition of a ‘reputable jurisdiction’ in the PMLFTR and act accordingly. For further information on the notion of a ‘reputable jurisdiction’ subject persons should refer to Section 8.1.
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.45 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 become exposed to and thereby determine:

(a) whether the application of EDD in accordance with Section 3.5 is necessary; and
(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).

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

45 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\(^{46}\) 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.

\(^{46}\) Ibid, pp. 23-24, paragraph 3.6.
• Customers that are politically exposed persons.

In determining the risk that a customer poses, subject persons should also be aware of the customer’s behaviour. The following situations should be kept 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. 47

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 resources 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 48 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, 49 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.

47 This part of the Implementing Procedures and Guidance is based on Chapter 4 of JMLSG Guidance.
48 FATF RBA Guidance, p. 24, paragraph 3.7.
49 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.
(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 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\(^{50}\) 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.\(^{51}\) 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:

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

\(^{50}\) FATF RBA Guidance, p. 23, paragraph 3.5.
\(^{51}\) Reference should also be made to sanctions, embargoes or similar measures issued by the EU.
4.2 The Risk-Based Approach

While the risk-assessment and risk-management procedures specified in Section 4.1 above are mandatory in order to determine when the application of EDD is necessary and to update CDD in respect of existing customers in accordance with the PMLFTR, 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 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.\(^{52}\)

Subject persons should be aware that where a decision to apply the RBA is taken, a framework should be implemented. The model\(^ {53}\) 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.


\(^{53}\) 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.
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.

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 due diligence. 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.\textsuperscript{54}

\section*{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:

- identifying and assessing risks;
- managing and controlling risks;
- monitoring controls; and
- recording the actions taken.

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

\textsuperscript{54} Ibid, p. 2-3, paragraph 1.12 and 1.13.
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 guidance on the manner in which such procedure should be implemented.

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.55

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.

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

---

55 FATF RBA Guidance p. 22, paragraph 3.2.
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
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**

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

Notwithstanding the fact that the RBA has been adopted, even where a subject person might have a high risk-appetite, the subject person is still required to classify the customers referred to in Regulation 11 as high risk and therefore apply enhanced due diligence measures commensurate with the risk profile of the customer.

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: 56

- implementing a customer identification programme that varies the procedures in respect of customers in accordance with the identified and assessed ML/FT risks;
- requiring adequate standards in relation to the quality of documentary evidence obtained;
- obtaining additional information in accordance with the identified and assessed ML/FT risks; and
- adopting the extent of monitoring customer transactions/activities depending on the outcome of the risk assessment.

A customer identification programme should at least involve: 57

- a standard information dataset to be held in respect of all customers;
- standard verification requirements for all customers;
- the possibility to apply more extensive due diligence on customer acceptance for higher-risk customers;
- the possibility to apply, where appropriate, more limited identity verification measures for specific lower risk customer/product combinations; and
- 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. 58

56 This part of the Procedures and Guidance is based on Chapter 4 of the JMLSG Guidance.
57 Ibid. p. 38, paragraph 4.23.
58 Ibid. p. 38, paragraph 4.27.
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 to review the adequacy of the risk assessment, the internal controls and the compliance arrangements. Such audits 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.

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 PROCEDURE

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:

- records indicating the nature of the evidence of the CDD documents required and obtained, comprising a copy of, or reference to, the evidence required for the identity and providing sufficient information to enable the details as to a person’s identity contained in the relevant evidence to be re-obtained. Such records should be maintained in relation to all business relationships formed and occasional transactions carried out;
- in the course of an established business relationship or occasional transaction, records containing details on the business relationship and all transactions carried out by the customers, including the original documents or other copies which are admissible in court proceedings;
- 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 Section 6.8).

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:
- reports by the MLRO to senior management;
- records of consideration of those reports and of any action taken as a consequence thereof;
- internal audit reports.

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 commencement of this time period depends on the type of records to be retained.

5.3.1 CDD documentation

With respect to CDD documentation, the time period of five (5) years commences from the date on which the business relationship is terminated. This date varies depending on the following circumstances:

- Negotiations: The date of ending the business relationship in respect of whose formation the record was compiled.
- Suspicion: In the case of an occasional transaction, 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: The date of carrying out the occasional transaction, or the last of a series of single large transactions, in respect of which the record was compiled.
- Series of Transactions: The date of carrying out the last occasional transaction in a series of transactions, in respect of which the record was compiled.

The date of carrying out the last transaction also applies if the formalities necessary to end a business relationship were not observed but the five (5) year period elapsed since the date of carrying out the last transaction. However, the business relationship should be immediately formally terminated.

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 on the business relationship and on the transactions carried out in the course of a business relationship 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 with the date on which the occasional transaction or the last of a series of occasional transactions took place.

Transaction records where a suspicious transaction report has been filed with the FIAU 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. However, this five (5) year retention period may be extended by the FIAU as may be required. In any case it is advisable that at the expiry of the five (5) year periods subject persons liaise with the FIAU before destroying these records.

5.3.3 Records in relation to the background and purpose of a complex or large transaction

The time period for the retention of the findings established by the subject person in relation to complex or large transactions, including unusual patterns of transactions, 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

The PMLFTR do not state the manner in which records are to be kept. A hard copy of original documents, however, must always be maintained if authenticated copies are obtained in lieu of the originals. The following are some ways in which records could be retained:

- in physical files;
- on microfiche;
- 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:

- whether they maintain or have maintained a business relationship with a specified natural or legal person/s during the previous five years; and
- 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.\textsuperscript{59}

\textsuperscript{59} 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:

(a) Officer of the subject person

The subject person may not appoint as MLRO any person who is not an official in employment with or the executive director of the subject person and is resident in Malta. This implies that the functions of a MLRO may not be:

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

(b) Sufficient seniority and command

The MLRO must be of 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 senior management 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’s AML/CFT policy.

According to the PMLFTR the MLRO is responsible for:

- receiving reports of knowledge or suspicion of ML/FT;\(^{60}\)
- considering such reports to determine whether a suspicion of ML/FT subsists.\(^{61}\)

\(^{60}\) Regulation 15(4)(a) of the PMLFTR.

\(^{61}\) Regulation 15(4)(b) of the PMLFTR.
The appointment of the MLRO, and any subsequent changes thereto, must be notified to the FIAU and to the relevant supervisory authority.

6.2 The designated employee

A designated employee is an employee of the subject person who is appointed to assist the MLRO in the fulfilment of his AML/CFT duties. The appointment of the designated employee must be approved by the MLRO and shall work under his direction.

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 also be notified to the FIAU and the relevant supervisory authority.

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. Therefore, it is crucial that all employees are informed of the identity of the MLRO and any designated employee(s). Internal reports should be submitted in a written form, preferably on a standard template, accompanied with all related information and documentation. The name of the employee making the report need not be disclosed by the MLRO to the FIAU.

It should be noted that ideally reporting lines should be as short as possible with the minimum number of people between the employee with the suspicion and the MLRO. This ensures speed, confidentiality and accessibility to the MLRO. However, in certain large organisations the reporting lines can be such that an employee has to first submit the report to his superior, who evaluates such report and decides himself if there are sufficient grounds for a suspicion, in which case the report is then 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 subject person should have a system whereby records are kept in writing of internal reports not forwarded to the MLRO and where the reasons for such decisions are recorded. Such records should be made available to the MLRO who shall ensure compliance with the internal procedures and to the internal auditors where applicable.

---

62 Regulation 15(6) of the PMLFTR.
63 Regulation 15(11) of the PMLFTR.
In cases where an internal report is not forwarded to the MLRO and the employee still has a suspicion that ML/FT is occurring, the reporting lines should be such that the employee can 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 vital 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) other connected accounts or relationships, including where the person suspected of ML/FT:
   (i) is a settlor, donor, contributor, protector, trustee or beneficiary of a trust, trust account or other trust relationship with the subject person; or
   (ii) 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
   (iii) 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 6.12, 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, as soon as is reasonably practicable, but not later than five (5) working days from when the suspicion first arose, disclose that information, supported by the relevant identification and documentation, to the FIAU.\(^{64}\)

The FIAU has to be informed about these suspicious transactions through the completion of a Suspicious Transaction Report (STR). A template for this purpose can be found in Appendix II.\(^{65}\) MLROs have to complete this report and should provide as much detail as possible together with the relevant identification and other supporting documentation. This report should then be delivered preferably by hand, to the FIAU premises addressed to the Director at the following address:

<table>
<thead>
<tr>
<th>Financial Intelligence Analysis Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>67/4 South Street</td>
</tr>
<tr>
<td>Valletta VLT 1105</td>
</tr>
</tbody>
</table>

In cases of great urgency an initial disclosure may be made by telephone, but a written report will also be required immediately thereafter:

| 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 other 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 allocating 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.\(^{66}\) 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 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 use

---

\(^{64}\) Regulation 15(6) of the PMLFTR.

\(^{65}\) It is to be noted that a STR which is not submitted in the format provided by the FIAU in Appendix II 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 in Appendix II. An electronic copy of the STR form may be found on http://www.fiumalta.org/library/PDF/STRFORM.doc.

\(^{66}\) The powers of the FIAU to request additional information are broader in terms of Articles 30 and 30A of the PMLA.
this extension provision sparingly as its frequent use could hinder the FIAU in the conduct of its duties.

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 the 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 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.

Upon receipt of such 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 notified to the subject person. The FIAU may authorise the execution of the transaction before the expiry of the twenty-four (24) hour period. Where the FIAU does not oppose the execution of the transaction, the subject person may proceed with the execution of the transaction in question.

Where the execution of the transaction is opposed by the FIAU, the subject person may 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 has 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.

6.7 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.

6.8 Complex or large transactions

Regulation 15(1) requires subject persons to examine with special attention, and to the 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:

- complex transactions that have no apparent economic or visible lawful purpose;
- large transactions that have no apparent economic or visible lawful purpose;
- unusual patterns of transactions that have no apparent economic or visible lawful purpose; and
- 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.

6.9 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). Although, the FIAU has adopted the list of equivalent countries agreed upon by the Member States of the European Union, subject persons should however refer to the definition of a ‘reputable jurisdiction’ in the PMLFTR and act accordingly. For further information on the notion of a ‘reputable jurisdiction’ subject persons should refer to Section 8.1.

If such jurisdictions continue not to apply measures equivalent to the PMLFTR, subject persons are under an obligation to inform the FIAU which, in collaboration with the relevant authority, may 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.

6.10 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. Disclosure of such information would give rise to the offence of tipping off and may prejudice an investigation. The elements of the

---

67 Regulation 16(1) of the PMLFTR.
offence of tipping off and the punishment set out by law are laid out in more detail in Section 8.4.1.6.

A subject person must however still retain the necessary contact with a customer and should enquire, in a tactful manner, 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.

6.11 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. 68 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:
   (i) undertakes equivalent activities;
   (ii) forms part of the same group of companies; and
   (iii) 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:
   (i) undertakes equivalent activities;
   (ii) performs their activities whether as employees or not;
   (iii) 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
   (iv) 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:
   (i) that relate to the same customer;
   (ii) that relate to the same transaction;
   (iii) that involve two or more institutions or persons situated in Malta, within another Member State of the European Community or in a reputable jurisdiction;

68 Regulation 16(2) of the PMLFTR.
such persons are subject to equivalent obligations of professional secrecy and personal data protection; and

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, 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 should also be noted that the fact that a subject person carrying out a relevant activity under paragraphs (a) or (c) is seeking to dissuade a client from engaging in an illegal activity shall not constitute tipping off. This provision envisages those situations where the client seeks advice from the professional on whether a particular transaction or business activity is legal or otherwise. In this case the professional is receiving information in the course of ascertaining the legal position of the client and therefore that professional would not be in breach of the duty of confidentiality. On the other hand, in the event that a client seeks to carry out a transaction with the aim of laundering money, the professional is under an obligation to file a STR with the FIAU without informing the client.

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.

6.12 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 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 competent 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 during that calendar year. 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)

69 Regulation 16(3) of the PMLFTR.
70 Regulation 15(12) of the PMLFTR.
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.

6.12.1 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:

- information on STRs submitted internally and to the FIAU;
- 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;
- an overview of the manner through which the MLRO would have assessed internal compliance, including overall oversight by the internal audit function, highlighting any non-compliance findings that may have been identified and corrective measures taken accordingly; and
- information concerning the AML/CFT training attended by the MLRO and, where applicable, designated employees, and AML/CFT training provided to staff members.

The Report is to be completed by the MLRO and submitted to the FIAU in accordance with the time-frames envisaged in Section 6.12.2 below. Subject persons should ensure that the report is also submitted internally to senior management and the Board of Directors, as applicable.

A soft-copy of the template of the Report is available on the website of the FIAU. The FIAU may review the template Report from time to time but shall allow sufficient time for subject persons to comply with the new format.

6.12.2 The submission period

Subject persons will be required to submit the Report, **covering the previous 12-month period**, in accordance with the time-frames provided below:

28th February of every year:
- Credit Institutions
- Financial Institutions
- Insurance Companies

31st March of every year:
- Investment Services Licensees
- Collective Investment Schemes
30\textsuperscript{th} April of every year:

- Corporate Service Providers
- Real Estate Agents
- Casinos

31\textsuperscript{st} May of every year:

- Other categories of non-financial subject persons

It shall be the MLRO’s responsibility to ensure that the Report is submitted by the designated date.

6.12.3 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. Moreover, the Report will assist the FIAU in planning its on-site monitoring programme on a risk based approach to 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.71

Awareness of the AML/CFT procedures 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,72 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; and
(d) the offences and penalties in relation to any breach of the PMLA or the PMLFTR.

71 Regulation 4(1)(d) and (e) of the PMLFTR.
72 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 an insurance company 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:

- the date on which the training was delivered;
- the nature of the training;
- the names of employees receiving the training; and
- the results of any assessment undertaken by employee.

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 for those employees who would have already received training during previous programmes.

In addition to ongoing refresher training, subject persons must provide training at appropriate intervals as follows:

- to new employees during the induction training upon commencement of work;
- to specific employees where there is a change in the employee's role at some stage after employment;
- to employees in general, on the basis of risk, with more frequent training being conducted where appropriate;
- 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.\(^73\) 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.

\(^73\) Regulation 4(2) of the PMLFTR.
CHAPTER 8 – OTHER ISSUES

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 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; or whether the prohibition laid down in Regulation 6 (cross border branches and subsidiaries) applies to a particular jurisdiction.

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 Equivalent Countries issued by the Member States, 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.

The list in the Common Understanding issued by the EU Member States contains the following countries:
Argentina
Australia
Brazil
Canada
Hong Kong
Japan
Mexico
New Zealand
The Russian Federation
Singapore
Switzerland
South Africa
The United States

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 the Dutch overseas territories (Netherlands Antilles and Aruba). Those overseas 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.

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 revised 2003 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”.

80.
8.2 Branches and subsidiaries

The PMLFTR 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.74

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

- communicate to such branches and majority owned subsidiaries its relevant AML/CFT internal policies and procedures established in accordance with the PMLFTR; and
- 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, who are ultimately responsible for the institution's risk profile.

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.

74 Regulation 6(1) of the PMLFTR.
8.4 Offences and penalties

8.4.1 Offences and contraventions under the PMLFTR

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

8.4.1.1 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.

8.4.1.2 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.
8.4.1.3 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.

8.4.1.4 Contravention of the provisions on customer due diligence

Regulation: 7(12)


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.

8.4.1.5 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).

8.4.1.6 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.

### 8.4.2 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.

#### 8.4.2.1 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.\(^\text{75}\)

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 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).\(^\text{71}\)

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

\(^{75}\) The amounts in Euro correspond to the equivalent sum in Maltese liri at the fixed Maltese lira/Euro exchange rate of 0.4293.
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.

8.4.2.2 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.76

8.4.2.3 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.77

8.4.2.4 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

---

76 The amounts in Euro correspond to the equivalent sum in Maltese liri at the fixed Maltese lira/Euro exchange rate of 0.4293.
77 Ibid.
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.  

8.4.3 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.

---

78 Ibid.
79 Ibid.
APPENDIX I - Open Sources

- CIA World Factbook

- 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 – STR Template**

Company Name

---

**SUSPICIOUS TRANSACTION REPORT**

for Money Laundering and Financing of Terrorism

<table>
<thead>
<tr>
<th>Date</th>
<th>Report Ref. No.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Check appropriate box:  
- Initial Report  
- Supplemental Report

Previous connected reports:  
Ref. No. ___________________  
Ref. No. ___________________

---

**Part 1: Subject of Report** *

<table>
<thead>
<tr>
<th>Full Name of Suspect (including aliases and/or nickname/s):</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

Identification: Type and document number (If available, copy to be attached to this report):

- Identity Card  
- Passport  
- Company Number  
- Other – Specify

No. ___________  
No. ___________  
No. ___________  
No. ___________

Expires: ___________  
Expires: ___________  
Expires: ___________  
Expires: ___________

Address:

Date of Birth / Registration:

Occupation / Nature of Business:

Nationality / Country of Incorporation:

Date when Business Relationship was established:

Type of Products (Accounts, Investments, Policies, Usernames, etc) held with institution, if any:

<table>
<thead>
<tr>
<th>(One product per box)</th>
<th>(One product per box)</th>
<th>(One product per box)</th>
</tr>
</thead>
</table>

Product/Relationship (Accounts, Investments, Policies, Usernames, etc) Number

---

88.
Date of Opening/Closing of Product (Account, Investment, Policy, etc.)

Balance as at report date:

Name of the MLRO (in block letters):

Signature of the MLRO:

* Subject persons submitting STRs dealing with more than one subject should submit multiple copies of this page (Part 1) ensuring that the details of each subject are submitted on a separate page.

**Part 2: Suspicious Transaction/Activity**

<table>
<thead>
<tr>
<th>Details of Sums arousing suspicions indicating source &amp; currency used</th>
<th>Date</th>
<th>Amount</th>
<th>Source</th>
</tr>
</thead>
</table>

**Explanation/description of suspicious transaction/activity**
The STR should be described in a complete and clear manner. All facts should be given in a chronological order including what is unusual, irregular or suspicious about the transaction/activity being reported. All relevant information used by the MLRO supporting documentation that is likely to assist the FIAU in its analysis should be attached to this report. *(Annex additional sheets if required.)*

List of Documents attached:

Name of the MLRO (in block letters)

MLRO’S Signature

This report should be accompanied by a covering letter on the subject person’s letterhead, which must also be signed by the MLRO. Any additional material that may be considered to be relevant and which may be of assistance to the FIAU, including bank statements, copies of cheques, forms, vouchers, telegraphic transfers, policies, details of associated accounts and products, copies of correspondence and agreements, should also be submitted.