FIMBank plc

ANTI-MONEY LAUNDERING
AND
ANTI-TERRORIST FINANCING

POLICY MANUAL

1st July 2010

1 FIMBANK POLICY STATEMENT

It is FIMBank's policy to prevent the misuse of the FIMBank facilities for the laundering of money or for the purpose of financing terrorist activities. FIMBank is committed to full compliance with all applicable laws and regulations regarding the prevention of money laundering and terrorist financing.

For these purposes, money laundering means the conversion, transfer, concealment or retention of any funds or property knowing that the funds or property are derived from any activity that constitutes a criminal offence under Maltese law. The term money laundering should be interpreted as including trade-based money laundering and terrorist financing which refers to the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illegal origins or finance their activities.

If FIMBank, its personnel and/or its facilities are misused for money laundering or terrorist financing, even inadvertently, FIMBank could possibly be subject to penalties. Such activities could also jeopardise the Bank's reputation in local and global markets.

FIMBank places considerable importance in governmental and private sector initiatives to fight financial crime. As an internationally active institution, FIMBank will always co-operate and provide all possible assistance to the Maltese and supranational authorities in this effort.

FIMBank has adopted a Policy Manual and a Procedures Manual which provide the basis for all employees to comply with all relevant requirements in this area and assist employees in preserving the good name and reputation of FIMBank. Employees should be alert to the possibility of FIMBank being unwittingly involved in the activities of third parties who may seek to use FIMBank facilities to hide the source or beneficial ownership of money or other financial property. There could also be serious consequences for directors, officers, managers and employees, as the case may be, namely fines or imprisonment, in respect of offences against the law or regulations.

This Policy Statement sets out the principles that are of universal application within the FIMBank Group, including offices and branches located overseas. Where FIMBank p.l.c. or any of its subsidiaries are involved in associated undertakings, whether in Malta or overseas, it is expected that such undertakings, whilst not falling within the scope of this Policy Statement, should observe together with the applicable laws, the rules and regulations that adhere to these principles at least as a minimum best practice.

The Policy Manual and the Procedures Manual provide the basis for all employees to comply with all relevant requirements in this area and assist employees in preserving the good name and reputation of FIMBank.

2 INTRODUCTION

2.1 What is the Policy Manual

As part of its anti-money laundering and terrorist financing programme, FIMBank has adopted two manuals:

- The Anti-Money Laundering and Terrorist Financing Policy Manual
- The Anti-Money Laundering and Terrorist Financing Procedures Manual

This is the Policy Manual. It sets out the FIMBank policy in relation to money laundering and terrorist financing prevention. It will be a high level guide for all employees and will describe how it affects you as a FIMBank employee in this important area.

The Policy Manual also provides some of the answers to the more common questions in this area. To further assist employees in obtaining a general understanding of the relevant requirements, the Policy Manual contains a general description of the legislation and regulations covering FIMBank's activities.

The Policy Manual is being distributed to all employees to enable all employees to have a general understanding of the requirements in money laundering and terrorist financing prevention. It is not intended to cover all the detailed requirements in this area. Those details appear in the Procedures Manual.

2.2 What is the Procedures Manual

Unlike the Policy Manual which is a high level document, the Procedures Manual will contain the day to day detailed procedure that should be observed in the bank's AML and terrorist financing programme.

The Procedures Manual will be distributed to employees who deal with or who have other contact with customers and/or counterparties. The Procedures Manual will also be given to all business unit managers whether or not the business unit or the business unit manager is in a customer or counterparty facing area.

3 FIMBANK GROUP – ITS STRUCTURE AND ORGANISATION

3.1 FIMBank Group

The FIMBank Group comprises: FIMBank plc, and its subsidiaries London Forfaiting Company Ltd, MENAFACTORS Limited, FIM Property Investments Limited, FIM Business Solutions Limited and FIMFactors BV. This Policy Manual sets out principles that are of universal application within the FIMBank Group, including offices and branches located overseas. Where FIMBank p.l.c. or any of its subsidiaries are involved in associated undertakings, whether in Malta or overseas, it is expected that such undertakings, whilst not falling within the scope of this Policy Manual, should observe the local laws and the rules and regulations that adhere to these principles at least as a minimum best practice.

3.2 FIMBank plc

FIMBank plc is a public limited company registered under the laws of Malta and is listed on the Malta Stock Exchange. It is licensed as a credit institution under the Malta Banking Act 1994. The FIMBank Group, including FIMBank, is supervised on a consolidated basis by the Malta Financial Services Authority.

FIMBank also operates in a number of other countries both inside and outside the European Union. As such it may be subject to the local legislation and rules in the Host Country where such activities take place.

3.3 AML Laws and Regulations – Malta and Overseas

As a credit institution incorporated in Malta, FIMBank is subject to all Maltese laws, regulations and guidance notes in the course of all its activities. As noted above, it is also subject to various AML and terrorist financing laws and regulations in the overseas countries in which it conducts business.

As set out in the Policy Statement, it is FIMBank's policy to observe all applicable requirements wherever it conducts business. The application of overseas laws, regulations and other requirements can raise detailed and complicated issues, including the application of Home State and Host Country legislation. This can lead to other issues concerning compliance with local requirements. In the event there is any uncertainty regarding the application of local requirements employees should contact the FIMBank Group Head of Legal & Compliance.

4 APPLICABLE LEGISLATION AND REGULATORY STRUCTURE

4.1 Brussels Directives and adherence to Supranational Initiatives

Malta is a Member State of the European Union. It is therefore required to implement the EU Directives promulgated in Brussels. Brussels has adopted a number of initiatives in this area. For these purposes the most significant are the Anti-Money Laundering Directives.

The 1st Anti-Money Laundering Directive was adopted in 1991. The 2nd Anti-Money Laundering Directive was adopted in 2001 and the 3rd Directive was adopted in 2005. Among other things, the 3rd Anti-Money Laundering Directive has set out for the first time the EU required measures for the prevention of terrorist financing.

Malta has been one of the first EU Member States to have already adopted legislation implementing the 3rd Anti-Money Laundering Directive. As a result of EU membership, Malta is also a member of the Committee on the Prevention of Money Laundering and Terrorist Financing (CPMLTF) which advises the EU Commission on proposed Directives, and liaises EU positions with the FATF.

Malta also adheres to a number of supranational initiatives and participates at international fora engaged in the fight against money laundering and terrorist financing. Since 2003 Malta is a member of the EGMONT Group, which brings together over 100 Financial Intelligence Units from different jurisdictions. Malta is also a member of the Council of Europe Select Committee of Experts on Anti-Money Laundering Measures (MONEYVAL) – an FATF associate member -- and subject to the mutual evaluation programmes of MONEYVAL.

4.2 Malta Prevention of Money Laundering Act

The Prevention of Money Laundering Act (the 'Act') was initially adopted in 1994 and has since been amended from time to time. The Act makes money laundering a criminal act in the islands of Malta and a person found guilty of the offence is liable on conviction to a fine up to EUR2,329,373.40 and/or to imprisonment up to 14 years.

The Act makes it an offence to acquire, possess or use the proceeds of any criminal act, or to assist anyone else in doing so, knowing that such property is the proceeds of a crime. The proceeds of the criminal activity can include actual funds, electronic money, bookkeeping entries or any other property such as real estate, jewellery, fine arts, etc.

The difficult issue has always been what amounts to criminal activity giving rise to a money laundering suspicion. In the past, the definition of criminal activity for money laundering purposes was limited to robbery, fraud and/or dealing in drugs or other illicit substances. Handling the proceeds from any such activity could be money laundering.

Maltese law in the form of the Prevention of Money Laundering Act has been amended following implementation of the 3rd Anti-Money Laundering Directive. Criminal activity now means any criminal offence or acts of terrorism as defined under the Malta Criminal Code. This means that the offence of money laundering will cover the handling of the proceeds from any activity that would be considered a crime in Malta. Moreover the Prevention of Money Laundering Act was recently amended in 2005 specifically to make the funding of terrorism[1] also a punishable offence under this Act.

This is a particularly sensitive area and if any employee has any question they are encouraged to liaise with the Group Head of Legal & Compliance or the MLRO.

4.3 Malta Prevention of Money Laundering Regulations

The Prevention of Money Laundering Regulations (the 'Regulations') were initially adopted in 1994 to implement the Prevention of Money Laundering Act. However, unlike the Act, the Regulations only target persons and institutions operating in the financial sector.

The Regulations are the second tier of Maltese requirements. They require financial institutions such as FIMBank to maintain systems and procedures to guard (i) its own business and (ii) the financial sector as a whole from being abused for the purposes of money laundering and/or terrorist financing.

Among other things, the Regulations require banks and financial sector institutions to implement systems and procedures in the areas of customer due diligence, suspicious transactions reporting, education and training, management responsibilities as well as requiring them to implement a series of other internal controls.

4.4 Malta Guidance Notes

The Guidance Notes for Credit and Financial Institutions (the 'Guidance Notes') were drafted by a joint committee of representatives from the Malta banking community, law enforcement agencies and the regulatory authorities. The Guidance Notes were then initially issued in August 1996 through the Central Bank of Malta which was then the competent authority. The Notes were periodically revised to take into account changes in the legislation, changes in the regulations and the appointment of the MFSA as the competent authority as well as the establishment of the Financial Intelligence Analysis Unit ('FIAU').

[1] The offence of funding of terrorism is described in Articles 328F and 328I of the Criminal Code.

The Guidance Notes set out what is expected of banks and their staff in relation to the prevention of money laundering and terrorist financing. They also establish standards for communications between the private sector and the authorities regarding the reporting and the investigation of suspicious transactions.

4.5 Financial Services Authority

The Malta Financial Services Authority (MFSA), which in 2002 took over the functions previously carried out by the Malta Financial Services Centre, is an autonomous public institution reporting to Parliament. The MFSA took over supervisory functions previously carried out by the Central Bank of Malta, the Malta Stock Exchange and the Malta Financial Services Centre for offshore activities. It is the single regulator for the financial services sector. MFSA is the primary regulator for FIMBank activities and supervises it on a consolidated basis.

4.6 Financial Intelligence Analysis Unit

The Financial Intelligence Analysis Unit (FIAU) is a governmental agency within the Malta Ministry of Finance and is responsible for the collection, collation, processing and analysis of information to combat money laundering and terrorist financing activities. It is the agency with whom financial institutions such as FIMBank file disclosure reports of suspicious transactions.

4.7 Money Laundering Activity Outside Malta

The Act provides that all FIMBank employees have an obligation to report suspicions of money laundering or terrorist financing arising from any Maltese criminal activity.

A significant new feature of Maltese law is that the reporting obligations under the Prevention of Money Laundering Act could now extend to cover acts that are committed outside Malta. Therefore, if during the course of their employment in Malta, a FIMBank employee has a suspicion that the Bank is being used or might be used to handle proceeds of criminal activity that occurred outside Malta, the employee has a reporting obligation if the activity would have been a criminal offence had it occurred in Malta.

4.8 FIMBank's Own Internal Rules

FIMBank is fully committed to compliance with Maltese as well as with the international legislation, sanctions and guidance issued by international regulatory bodies.

In addition, FIMBank has itself adopted additional internal rules which amplify and extend some of the Maltese requirements. These internal rules are set out in this Policy Manual, in the Anti-Money Laundering and Anti-Terrorist Financing Procedures Manual and from time to time through internal memoranda from FIMBank management.

Employees are expected to observe FIMBank internal requirements as well as the requirements set out in the Malta Prevention of Money Laundering Act, Regulations and Guidance Notes.

5 FREQUENTLY ASKED QUESTIONS

5.1 What is Money Laundering?

Money Laundering is the process by which criminals attempt to conceal the true origin and ownership of proceeds derived from their criminal activities, including but not limited to drugs, terrorism, theft, fraud and forgery. When undertaken successfully it allows the money launderer to maintain control over his proceeds and ultimately to provide a legitimate cover for the source of his income. Basically, money laundering is an exercise to take dirty money and make it clean. It is important to keep in mind that the misuse of the trade system is increasingly becoming one of the main methods by which criminal organisations and terrorist financiers move money for the purpose of disguising its origins and integrating it into the formal economy. Moreover trade-based money laundering may be more difficult to identify and combat.

The Malta Prevention of Money Laundering Act sets out a wide ranging definition of money laundering which includes;

- The conversion or transfer of any property, knowing such property is derived from criminal activity;
- The concealment or disguise of the source or location of such property;
- The acquisition or retention of such property;
- Attempting, even if unsuccessful, to do any of the above
- Assisting anyone else in doing the activities listed above

5.2 What is Terrorist Financing

Terrorist financing is also an international phenomenon. It often differs from money laundering in that the former frequently involves the movement of significant sums whereas terrorist financing frequently involves smaller sums which are often difficult to identify. Terrorist financing can nevertheless have a high impact as even modest amounts can be used to support highly visible and extremely dangerous activities.

The methods used for terrorist financing are quite variable and can involve the entire range from a complex and detailed series of transactions flowing through illegal enterprises to flows originating from legal operations that get siphoned off to fund terrorist events.

In many respects terrorist financing is the mirror image of money laundering. In one there is an effort to take bad money and make it good and in the other there is an effort to use good money for bad purposes.

5.3 Why have These Activities Become So Important

With the increase in criminal activities, particularly drug and fraud related, the amounts of money involved in Money Laundering have now become enormous. Whilst no accurate data exists, it is estimated that the annual world wide value of money being laundered is in excess of USD1 trillion. At some stage all of this money will eventually pass through the global financial systems in one form or another.

5.4 How does Money Laundering affect you?

FIMBank is a major trade finance banking organisation with a presence in many locations throughout the world. FIMBank provides to its Maltese and international clients a wide and diversified range of banking and trade finance services, all of which could potentially attract third parties who may wish to engage in money laundering or terrorist financing activities. Employees should therefore remain alert to all possible money laundering or terrorist financing situations so as to prevent the services of FIMBank being exploited especially in the view of the increasing misuse of the trade system.

Vigilance is required by all employees, particularly those involved in marketing our products and services to new customers; those involved in actual dealings with customers and those providing operational support to customer business.

5.5 Are there different stages to Money Laundering?

Yes, money laundering normally takes place in three distinct stages as follows:

1. Placement - The objective of placement is to get the money out of cash and into the non-cash economy, for example as a cash deposit or by purchase of an investment. The money then proceeds to the next stage.

2. Layering - The objective of this stage is to pass the money through numerous transactions so as to conceal the original source of the money. Once the trail and link are broken the money can then be used for the final stage,

3. Integration - At this stage, the money can be moved into the legitimate economy to purchase all types of assets whereby the origin and persons behind the money are never suspected.

5.6 How does the Prevention of Money Laundering law apply to tax offences?

Tax evasion is generally a criminal offence. Tax evasion is to be distinguished from legitimate tax planning to minimise or even to legitimately avoid taxation. This is often referred to as tax planning or even tax avoidance. Tax planning and tax avoidance are not criminal offences. Tax evasion is. Employees should be diligent to situations in which FIMBank is being used to launder the proceeds from tax evasion schemes.

This is a very technical, complex and sensitive area, as the line between criminal tax evasion and legitimate tax planning can be difficult to establish. Mere suspicion that a customer may be intending to commit tax evasion is not sufficient to trigger the reporting requirements. For the matter to be reportable there would need to be a suspicion that an indictable tax evasion offence had actually been committed and the benefit from that offence formed part of a transaction in which FIMBank was involved. The establishment and use of account relationships with international holding or trading companies that may form part of international tax planning structures shall not, of itself, be grounds of suspicion of a reportable offence.

Employees should be sensitive to this area, should conduct appropriate due diligence in this regard and any questions should be referred to the FIMBank Group Head of Legal & Compliance or the MLRO.

5.7 When and how do you report a Money Laundering suspicion?

Suspicions can take many forms and some examples are contained in Section 9.4 of this Policy Manual. If you have a suspicion you should promptly report it to the Money Laundering Reporting Officer.

6 FIMBANK AML AND TERRORIST FINANCING PROGRAMME

6.1 The FIMBank Programme

FIMBank has implemented an anti-money laundering and terrorist financing prevention programme to meet it responsibilities under the Act, the Regulations and the Guidance Notes. The programme has six (6) main parts:

- Customer Due Diligence
- Ongoing Monitoring
- The Money Laundering Reporting Officer
- Recognition and Reporting of Suspicious Transactions
- Education and Training
- Recordkeeping and Audit Requirements

Details regarding each of the above are set out in the Procedures Manual. The following is an overview of each of the six parts:

7 CUSTOMER DUE DILIGENCE

7.1 Basic Requirement - Identify the Customer

All banks are required to adopt and then regularly follow procedures to identify all customers. Banks need this information to establish to their satisfaction the identity of the customer and the intended nature of the business relationship.

The definition of a customer is very wide and includes any person whether an individual, a company, a bank, a trust, a partnership or any other legal entity. For banks - such as FIMBank - operating mainly in the corporate and wholesale markets rather than as a retail network, anti-money laundering laws cover all business with other banks, financial institutions and market counterparties.

The identification requirement applies to anyone who does business or seeks to do business with the Bank. As a result, it will apply to any individual, company, bank, partnership, special purpose vehicle or any other person (a) who carries out a transaction with FIMBank (b) who seeks to carry out a transaction with FIMBank or (c) any person who applies to establish a business relationship with FIMBank. The requirements also cover (d) occasional transactions as well as ongoing business.

There are no exceptions to this requirement. It must be satisfied in all instances. The precise details covering this requirement are set out in the Procedures Manual.

7.2 Second Requirement - Verify the Customer's Identity

In most cases, information about the customer is obtained directly from the customer. In other situations the information is obtained from other sources. Irrespective of how or where the identification information is obtained, there are some circumstances in which banks are required to take a further step and actually verify the information. Verification for these purposes means the information is verified from reliable, independent third party source(s).

The requirement to verify information does not arise in all circumstances. The Regulations and the Guidance Notes specify when this must occur.

7.3 FIMBank Documentation

The Regulations and the Guidance Notes require each bank to obtain appropriate customer documentation as part of the bank's systems and controls but they do not specify the exact form of that documentation. The choice of documentation is left to the discretion of each bank.

As part of the controls to commercially protect the Bank's interests, FIMBank has adopted a number of forms, notices and agreements which customers are required to sign depending on the particular circumstances of the customer/counterparty and the nature of the business being conducted with FIMBank. It is important to note that these documentation requirements are in addition to any of the requirements in the money laundering laws requiring FIMBank to obtain identification documentation from or about the customer. The requirements in this Policy Manual and the Procedures Manual only relate to anti-money laundering and anti-terrorist financing laws and regulations.

7.4 Simplified Customer Due Diligence

The Regulations recognise that not all situations require full customer due diligence. There are situations in which simplified customer due diligence may be conducted. In these cases, some very minimum customer identification is still required and the Bank may take the position not to verify the information.

Maltese Regulations spell out when simplified due diligence can be used. For FIMBank's purposes, the most frequent situations will be (i) when dealing with overseas credit institutions that are comparably regulated and (ii) companies whose securities are listed on regulated exchanges.

In view of such provisions, decisions whether to apply the simplified approach beyond those spelled out in the Regulations will be made by the Group Head of Legal & Compliance.

7.5 Overseas Credit Institutions that are comparably Regulated Banks

A considerable volume of FIMBank business is conducted with credit institutions in overseas countries, some of which are in the European Union and others are outside the EU. If the credit institution is conducting business from a jurisdiction that has regulatory requirements comparable to Malta, FIMBank can conduct simplified customer due diligence on that bank.

The definition of an equivalent jurisdiction can be quite detailed and further information on this can be found in the Procedures Manual. Other types of customers and/or counterparties may also qualify for simplified customer due diligence treatment.

The fact that an overseas bank is operating as a regulated entity in a comparable jurisdiction will allow simplified treatment but it is emphasised that this is only for anti-money laundering regulatory purposes. When opening a new relationship even for another regulated entity, FIMBank should be comfortable from a Know Your Customer standpoint that the counterparty is a bank that FIMBank is comfortable dealing with – from a credit, liquidity, legal, regulatory, operational and reputational standpoint.

7.6 Enhanced Customer Due Diligence

Equally some situations by their nature present a higher risk of potential money laundering or terrorist financing. The Regulations and the Guidance Notes specify the type of situations that fall into this category, and the steps that must be taken before conducting business with this type of customer/counterparty.

7.7 Correspondent Banks

The Regulations set out specific details regarding business conducted with correspondent banks. This will be particularly relevant to FIMBank. Effectively, the Regulations consider correspondent banking activities as

higher risk business and such business requires enhanced customer due diligence. The various steps that banks must first take before commencing correspondent banking activities are set out in the Regulations and the Guidance Notes.

7.8 Non-Compliant Jurisdictions

Special attention should be given to business relationships and transactions with persons, including companies and other financial institutions, from countries that do not sufficiently adhere to FATF [2] Standards. The FIMBank Counterparty Approval Officer will maintain a list of Non-Compliant Countries. Prior approval from the Group Head of Legal & Compliance or, in absence, the MLRO will be required before conducting business with any person operating from an office located in a non-compliant jurisdiction or whose parent company is located in a non-compliant jurisdiction.

7.9 Politically Exposed Persons (PEPs)

Enhanced customer due diligence is also required when dealing with politically exposed persons (PEPs). The definition of a PEP is set out in the Procedures Manual but in brief we can define it as a person who is in a politically sensitive role and has been entrusted with prominent public functions. It also covers the PEP's family members and business associates. Enhanced due diligence should be conducted before business is conducted with this category of customer. Prior approval by the President, or any other person as may be so designated, is also required. Business with PEPs also requires ongoing monitoring.

7.10 Deposit Business

In the general course of its deposit raising activities, FIMBank will establish relationships with various types of customers, ranging from natural persons to all type of incorporated or unincorporated entities. These may include institutions, companies and partnerships, investment funds, charities, cooperatives and provident societies, clubs, associations, trusts and foundations, and professional intermediaries managing clients' accounts, etc. In all these cases, the FIMBank Relationship Manager will ensure that all the standard due diligence requirements apply but also that FIMBank understands the nature, purpose and scale of the business or activity which generates the funds that flow as deposits

7.11 Shell Banks

FIMBank has a clear policy to the effect that no business should be undertaken with any shell bank. A shell bank is a bank which does not have a physical presence in any country, and therefore particularly susceptible to risk of abuse and money laundering.

7.12 Who is Responsible for Customer Due Diligence

Primary responsibility for conducting customer due diligence lies within the FIMBank Banking Group, more specifically with the FIMBank Relationship Manager who has responsibility for servicing the customer/counterparty in a specific geographic area. In most cases this will be the Officer within the Corporate and Institutions Banking team who retains primary responsibility for the customer relationship.

The task of conducting the customer due diligence shall include but shall not be limited to (i) obtaining all customer identification information (ii) verifying the customer information as required (iii) obtaining all required additional KYC information and (iv) arranging for the customer documentation to be completed. This responsibility shall rest with the FIMBank Banking Group whilst the Relationship Manager will be supported as necessary by the Transaction Management and Control Team.

[2] The Financial Action Task Force on money laundering which is an international organisation that sets key standards for countries to observe in their legislative programme. FATF maintains a list on countries they consider as not compliant with recommendations.

7.13 Reliance on Third Party

In certain circumstances FIMBank may rely on a third party to conduct FIMBank's customer due diligence but the ultimate responsibility for meeting the due diligence requirements remains at all times with the person responsible for conducting the due diligence exercise. Further measures to be observed when relying on third parties are in the Procedures Manual.

7.14 Who Approves New Business Relationships and New Accounts

The new business relationship and new account approval process can be summarised as follows:

(a) the FIMBank Relationship Manager is responsible for ensuring that customer due diligence has been completed;
(b) the Counterparty Approval Officers within the Transaction Management and Control Team (or equivalent position in the case of a subsidiary) are responsible for reviewing the documentation presented as per (a) above, and confirming that it is in order;
(c) where the due diligence process as indicated in (b) has raised no concerns following the performance of all the account opening procedures (e.g. negative WorldCheck results, satisfactory references, no sanctions or similar high risk or PEP associations highlighted, negative check on garnishee orderings, etc) the Counterparty Approval Officers shall pass on the documentation to the Head of TMC for approval of the account relationship as per (e) below.
(d) where the due diligence process has raised concerns, and before the Account Relationship may commence, approvals from the
(i) Head of Risk Management for credit, operational and similar risks, and/or the
(ii) Head of Legal & Compliance for documentation, KYC and legal risk, and/or
(iii) the President or any other person so delegated for unusual, large or high-risk relationships, e.g. PEP[3], shall be requested.
Such approvals shall be provided within 72 hours;
(e) Following from (c) or (d) above the Head of TMC or any other person so delegated by the Head of TMC, after assuring that the above-mentioned approvals are on file, is responsible for approving and the actual opening of the account relationship.

A flow chart illustrating the procedures for approving new business relationships/accounts is attached as an *Annex* to this Manual.

7.15 Timing of Due Diligence

A business relationship shall not commence and the account shall not go into operation until the steps listed in 7.14 above have been completed. Any deviation or exception to this requirement must be approved by the President, or as may be so delegated.

8 ONGOING MONITORING

Banks and their employees are required to monitor transactions to determine if any particular transaction is suspicious in nature and may be related to money laundering or terrorist financing activities. Monitoring does not require looking at every transaction. The extent of the monitoring will be determined on a risk based approach. .Ongoing monitoring is an important part of the Bank's money laundering and terrorist financing prevention program.

[3] Politically Exposed Persons.

9 RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

9.1 Recognition of Suspicious Transactions

Every bank is required to establish suspicious transaction reporting procedures.

There is no clear regulatory pronouncement as to what constitutes a suspicious activity but a suspicious transaction will often be one which is inconsistent with the customer's/counterparty's known legitimate business or personal activities or with the normal business for that type of account, or where trade or financial anomalies or discrepancies surface through analysis of the financial and trade data available. Suspicious activity can occur either in the negotiation stages with a prospective customer in order to commence a business relationship, or at the outset of the client relationship, or even long after the relationship has been initiated.

9.2 Reporting of Suspicious Transactions - The Bank's Responsibilities

The Regulations make clear that each bank is expected to adopt an internal system whereby unusual or suspicious transactions are reported.

To comply with these responsibilities FIMBank has implemented a set of procedures for reporting suspicious activity to the Malta authorities – the Financial Intelligence Analysis Unit (FIAU).

Paragraph 9.3 sets out the requirements for employees to report suspicious transaction to the FIMBank Money Laundering Reporting Officer. The MLRO will conduct such enquiry as he believes appropriate and a decision will then be made whether a report is required to be submitted to the FIAU. All contact with the authorities in respect to these reports, including any required follow up, will be handled by the MLRO

9.3 Reporting of Suspicious Transactions - Employees' Responsibilities

The Regulations also make clear that there is a statutory obligation on all staff in a bank to report suspicions of possible money laundering or terrorist financing activities or any transactions which are particularly likely, by their nature to be related to money laundering.

All employees must accordingly be alert to possible money laundering or terrorist financing activities. Employees are required to make a report in respect to information that comes to their attention during the course of their business where (i) they know or (ii) they have reasonable ground to suspect that a person is engaged in money laundering or terrorist financing.

There is a distinction between knowledge and suspicion. Having *knowledge* means actually knowing it to be true. *Suspicion* is more subjective. For money laundering or terrorist financing purposes suspicion is something beyond mere speculation. It is something less than knowledge but it is something that is based on some foundation.

A transaction which appears unusual is not necessarily suspicious. Even customers with a stable and predictable business profile will conduct occasional business that may appear unusual for them. Unusual is, therefore, in the first instance only a basis for further enquiry.

Employees are not required to actually find out whether suspected funds or property originate through any criminal activities, nor are they required to proactively search out or investigate suspected conduct. They should, however, be sensitive to the importance of this subject and should be aware of the need to report the matter should information come to their attention as a FIMBank employee.

If an employee does have a suspicion that some money laundering or terrorist financing is or has been conducted, the employee should promptly report the information to the MLRO in writing using the forms provided by the MLRO.

Because of the importance attached to suspicious activity reporting FIMBank directors, officers and employees are protected from criminal or civil liability for breach of any banking confidentiality obligation if they report their suspicions to the MLRO in good faith. This protection will apply even if they did not know precisely what the underlying criminal activity was.

9.4 Some Examples of Possible Suspicious Activity

The following are 'red flags' that could indicate suspicious activity. The examples do not necessarily represent reportable events but they do suggest situations that may be indicative of activity that should be followed up and clarified:

General Typologies

- Failure or refusal of a new customer to provide documentation in accordance with FIMBank account procedures.
- Use of an overseas corporate or trust vehicle for which verification of identity can not be established
- A customer with no discernible reason for using the facilities of FIMBank in Malta
- Any business in the name of an overseas bank or financial institution from a country which does not have equivalent anti-money laundering regulations.
- A customer from a country which does not have equivalent anti-money laundering regulations seeking to open an account in Malta.
- Any apparently unnecessary use of an intermediary in a transaction.
- Intermediaries who delay providing confirmation that they hold documents verifying the identity of their principal(s).
- Any departure from the FIMBank account and new counterparty opening procedures demanded by the customer.
- Any customer who is prepared to conduct business at a price which is materially away from the then market price.
- Any transaction which appears to have no commercial justification or is inconsistent with the customer's normal account relationship with FIMBank.
- Large third party cheques endorsed in favour of the customer.
- Use of dormant accounts: large inward credit followed by withdrawals.
- Ready acceptance by customer of unfavourable banking conditions.
- Back-to-back deposits/loans with overseas banks from countries which do not have equivalent anti-money laundering regulations.
- Requests to borrow against assets held by or to the order of the bank, where the origin of the assets is not known or is inconsistent with the known wealth of the customer.

- Receipt of funds from countries which do not have equivalent anti-money laundering regulations.
- Movement of large size funds by banking customers, particularly if it is an unusual movement for that particular customer.
- Regularly changing standing banking instructions, or standing delivery instructions in the case of securities and money market transactions.
- Settlement instructions whereby securities or money market instruments are settled other than by way of cash against delivery through a recognised correspondent bank or settlement system.
- Settlement arrangements which are other than the regular way for that product or instrument.
- Constant and regular small deposits that are not in line with the customer's normal trading activities.
- Misrepresentation of the price, quantity or quality of imports or exports.
- Fictitious trade activities carried out through front companies;
- Mismatch between the import and export countries documentation

Specific typologies that may be suggestive of Terrorist Financing

Moreover, the following relationships/situations may be particularly suggestive of activity that could be related to Terrorist Financing:

- Organisations or entities associated with governments/countries indicated to have assisted or financed terrorist activity.
- Structures, which may often include trusts from unfamiliar jurisdictions, that are promoted by professional firms known or indicated to advise governments, countries or associated entities linked with terrorist activity.
- Alternatively, structures introduced by unknown or obscure professional firms with addresses in highly respectable Western European financial centres.
- Charitable initiatives or programmes, especially if the relationship is of relatively short duration with unusually large flows, which do not emanate from ordinary introductions.
- 'Migrants associations', peculiar 'religious' organisations that come with questionable introductions (especially from countries connected with terrorism) and 'hawala' activity that defeats common sense explanation.

Cash Transactions

- Large cash (USD10,000 or equivalent, or more) deposits or withdrawals
- Regular cash deposits subsequently transferred out of the account within a short period.

- Cash transactions on accounts where one could expect to see more normal modes of commercial financing.

- Outward payment instructions requesting disbursement in cash.

9.5 Tipping Off

The Act provides for the offence of tipping off which is punishable by a prison term up to two (2) years and a fine up to EUR50,000.

Once an external report has been made by the Bank to the Malta authorities (the FIAU) or once an internal report to the MLRO has been made, it is a criminal offence for anyone to release any information which is likely to prejudice the external or the internal investigation.

Reasonable enquiries of a customer, conducted in a tactful manner, regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity is acceptable as it forms an integral part of the KYC program. Such enquiries should not give rise to tipping off.

However, this is a particularly sensitive area as the penalties are severe if the enquiry is for what ever reason thereafter considered by the authorities to have been a tip off. As a result, in the event that an internal suspicious report is submitted to the MLRO employees should consult with the MLRO before having any further conversations with the person that was the subject of the report.

10 MONEY LAUNDERING REPORTING OFFICER

10.1 What is a Money Laundering Reporting Officer (MLRO)

All banks are required to appoint a Money Laundering Reporting Officer who should be responsible for the implementation and maintenance of the suspicious reporting procedures.

10.2 Who is the FIMBank MLRO

The FIMBank MLRO is:

Ivan Fsadni
FIMBank p.l.c.
7th Floor
The Plaza Commercial Centre
Bisazza Street
Sliema SLM15

Telephone: (+ 356) 21322100

10.3 What are the Responsibilities of the MLRO

The function of the MLRO is designated by the Malta Prevention of Money Laundering Regulations and elaborated upon in the Guidance Notes. Because of the high confidentiality and responsibility of the MLRO, he/she should be a person of sufficient seniority to command the necessary authority.

The MLRO is required to determine whether the information or other matters contained in the internal report gives rise to a knowledge or suspicion that a customer/counterparty is or could be engaged in money

laundering or terrorist financing. The MLRO is not expected to investigate a transaction other than internally or to determine whether the funds are the proceeds of a criminal activity.

In making this judgment the MLRO must consider all relevant information available within the bank concerning the person or business to whom the internal report relates. The MLRO shall therefore enjoy reasonable access to information in reaching a decision, however the ultimate decision for filing a report with the FIAU shall rest with the President, or as may be delegated in the President's absence.

11 EDUCATION AND TRAINING

The Regulations require banks to ensure that all employees are aware of the policies and procedures that have been put in place to prevent the bank from being sued for money laundering or terrorist financing purposes. Each bank must also take steps to ensure that all employees are aware of the bank's requirements and their own obligations under the Act and the Regulations, and also to provide the necessary training to its employees in recognising, handling and dealing with potential money laundering and terrorist financing transactions.

This Policy Manual is given to all employees to meet the foregoing requirement. The Procedures Manual with its more detailed provisions is given to employees having dealings with or other contact with customers and counterparties to further support this obligation. It is also given to all business unit managers whether or not they are involved in customer facing activities.

All staff are expected to observe Maltese law requirements as well as FIMBank's own requirements as set out in this Policy Manual and in the Procedures Manual.

Non-compliance with the Policy Manual or the Procedures Manual may result in disciplinary actions. Before a decision with regard to disciplinary action is taken, the seriousness and merits of each case shall be appraised by Management.

12 FURTHER INFORMATION

Many of the provisions in this Policy Manual as well as the Procedures Manual involve detailed and/or technical requirements. Any employee requiring clarification regarding any matter in either Manual or concerning any other money laundering or terrorist financing matter, or wishing to provide feedback or suggestions for updates to the Manual, should contact:

Group Head of Legal & Compliance
Group Legal and Compliance Department
FIMBank p.l.c.
Telephone: (+ 356) 21322100

No parts of this Manual may be reproduced, and no updates or amendments shall have effect, unless with the prior approval of the Group Head of Legal and Compliance.

ANNEX – FLOWCHART ACCOUNT OPENING