



Anti-Money Laundering and Terrorist Financing Manual



Contents

1. Money Laundering Prevention and Combating Terrorist Financing	1
2.1 Introduction.....	1
2.2 Principles of Money Laundering Prevention & Combating Terrorist Financing Policy	1
2.3 PMA Legislation and Regulatory Requirements	2
2.4 AML Policy.....	2
2. Roles and responsibilities at the bank level.....	7
3.1 Defense Lines	7
3.2 Responsibility of the Board of Directors (Compliance Committee)	8
3.3 Responsibility of the executive management.....	8
3.4 Internal audit responsibility.....	9
3. Anti-Money Laundering and Terrorist Financing Unit.....	10
4.1 Organizational Chart.....	10
4.2 The independence of the Anti-Money Laundering and Terrorist Financing Unit	11
4.3 Assigning and terminating the services of the Anti-Money Laundering and Terrorist Financing unit official.....	11
4.4 The responsibilities of the Anti-Money Laundering and Terrorist Financing Unit	12
4. Customer Due Diligence - Know Your Customer	14
5. Suspicious Activity Reporting	35
6.1 Introduction.....	35
6.2 Internal Reports.....	36
6.3 Consideration of Internal Reports and External Disclosures	36
6.4 Exiting a Relationship	37
6.5 Transaction Monitoring.....	37
6.6 Suspicious Transaction – Money Laundering Indicators	37
6.7 Training	39
6.8 Suspicious Transaction /Exception Reports.....	39
6.9 Submission of the STR.....	40
6.10 Procedure for Reporting	40
6.11 Filling up the STR.....	41
6.12 Collation of Documents	42
6.13 Duties of the Reporting branch/office manager	42
6.14 Internal STR template	49
6. Sanctions / Boycott Law	51
7.1 Background.....	51
7.2 The National Bank Policy.....	51
7.3 Dealings with Sanctions Targets	51
7.4 Sanctions Policy.....	52
7.5 Appendix 1: Summary of Sanctions.....	56
7. Record Retention.....	64
8.1 Introduction.....	64
8.2 Retention Period requirement.....	64
8.3 Electronic archiving system.....	65
8. Sanctions in the event of non-compliance with anti money laundering and terrorist financing laws.	65
9.1 Article (38) Exemption from sanctions	65
9.2 Article (39) The penalty for a legal person	65
9.3 Article (43) Penalty for financing terrorism crime	65
9.4 Article (44) Penalty for violating the provisions of the law decree.....	66
9. National Bank companies and financial institutions.....	67
10. Compliance Training	67
11.1 Significance of Compliance Training	67
11.2 Types of Compliance Training.....	67
11.3 Benefits of Compliance Training	68

Definitions

Law (Decree)	Anti-Money Laundering and terrorism financing Decree Law No. (20) of 2015 And Its Amendments Issued By The Decree Law No. (13) of 2016
The unit	The Financial Monitoring Unit in the Palestinian Monetary Authority.
The committee	The National Committee to Combat Money Laundering and Terrorist Financing.
Monetary Authority.	Palestine Monetary Authority.
Politically Exposed Person (PEP)	the person along with his family, relatives, and associate, who are or have been entrusted with prominent public functions or political positions in Palestine or abroad includes political party officials, judges, legislative council members, prosecutors, heads of State-owned Enterprise and the heads of institutions and bodies, charities and NGOs or the authorities of the State of Palestine or of any other foreign state and heads and prominent representatives of international organizations
(Non continues) customer	The customer who does not have a continuous business relationship with the bank.
The real beneficiary	The natural person who has or ultimately controls the customer or account of the person on whose behalf the transaction was performed, or the person exercising effective final control over a legal person.
Business relationship	The relationship that arises between the customer and the bank and relates to the banking activities and services that the bank provides to its clients.
Due diligence	Identifying the customer's identity, legal status, activity, source of funds, the purpose and nature of the business relationship and the real beneficiary (if any), verifying all of that information, and the continuous monitoring of operations that take place in the context of an ongoing business relationship by any of the means specified under the relevant legislation, in addition to identifying the nature of the future relationship between the bank and the customer and the its purpose.
Imaginary bank	A bank that does not have a fixed place of business to receive its customers, does not employ one or more people who practice actual activity and management and does not keep records of its operations, and is not subject to inspection by a competent regulatory or supervisory authority, whether in the country in which it was founded or in another country.
Electronic transfer	Any transfer process made by a bank using electronic means on behalf of the requester to issue the transfer, according to which the money is sent to another bank, where the transferee can receive it regardless of the fact that the person requesting the transfer is the same person who transferred it.
The Board of Directors	The Board of Directors of TNB.
Compliance Committee	It is a committee derived from the Board of Directors of TNB. This committee that oversees the compliance monitoring and combating money laundering and terrorist financing in the bank.
Executive Management (Senior)	It is the executive management (senior management) of TNB.
General Manager	General Manager of TNB.
Business units	Various departments in TNB.
Anti-Money Laundering and Terrorist Financing Unit	It is the unit concerned with combating money laundering and terrorist financing in TNB.
Anti-money laundering and terrorism financing official	The person in charge of the Anti-Money Laundering and Terrorist Financing Unit, who is appointed by the Board of Directors of TNB.

1. Money Laundering Prevention and Combating Terrorist Financing

1.1 Introduction

With the increasing risk of money laundering faced by financial institutions around the world, regulators are focusing on the controls and procedures banks have put in place to prevent money laundering and actively assist law enforcement authorities in detection and in investigation.

To this end, The National Bank has set out the following Principles, policies and procedures on the Money Laundering Prevention and Combating Terrorist Financing.

1.2 Principles of Money Laundering Prevention & Combating Terrorist Financing Policy

The principles set out below form the Bank's policy on the prevention of money laundering (dealing with the proceeds of crime) or the financing of terrorist activity (where the funds may or may not originate from crime). It is a clear statement to our staff and regulators of the Bank's position on this critical risk issue. The policy is essential in order to deter money launderers from targeting TNB and to protect the Bank from regulatory penalties, litigation and reputation risk.

As an organization committed to the prevention of money laundering, The National Bank will:

1. Establish clear lines of internal accountability and responsibility. Primary responsibility for the prevention of money laundering rests with the business, which must ensure that staff are adequately trained and that appropriate internal controls are in place and operating effectively. The business is supported in meeting this responsibility by the Compliance and AML functions and Legal Counsel.
2. Document, implement, and maintain local systems, controls and procedures which interpret this policy for each business.
3. Take all reasonable steps to verify the identity of our clients, including the beneficial owners of corporate entities (including trusts) and the principals behind customers who are acting as agents. We will take all reasonable steps to ensure that information about clients are kept up-to-date.
4. Establish systems to retain adequate records of identification, account opening, and transactions for a minimum of ten years.
5. Refuse any transaction where, based on explanations offered by the client or other information, reasonable grounds exist to suspect that the funds may not be from a legitimate source.
6. Where required or permitted by local legislation, make prompt disclosures of suspicious transactions or proposed transactions to the relevant authorities through the appropriate internal channels.
7. Educate and train our staff on the requirements of local legislation, the Bank's policy on the prevention of money laundering, the recognition of suspicious transactions, the systems, controls and procedures implemented.
8. Co-operate with any lawful request for information made by government agencies during their investigations into money laundering.
9. Support governments, law enforcement agencies and international bodies such as the Financial Action Task Force, in their efforts to combat the use of the financial system for the laundering of the proceeds of crime.
10. Report money laundering issues to the senior management on regular basis. The Money Laundering Reporting Officer (MLRO) will determine and communicate the content, format and frequency of management reporting.

1.3 PMA Legislation and Regulatory Requirements

In general, the PMA regulations stress robust KYC procedures, transaction monitoring, suspicious activity reporting and staff training as the foundation for prevention of money laundering.

Article No (19) and (23) of Decree No (20) for the year 2015 and any amendments thereto, read in addition to Amendments Issued by the Decree Law No. (13) Of 2016 later amendments criminalize money laundering and form the cornerstone of Palestine anti-money laundering requirements and procedures. The Anti Money Laundering established Committee and Financial Follow-up Unit (FFU) is Palestine's Financial Intelligence Unit for investigating fraud and suspicious transactions.

Decree No (20) for the year 2015 and any amendments thereto describes in detail the conduct and activities that constitute "terrorism" within the definition of the law, to whom the law will apply and the penalties, for breaching any of its provisions.

For laws & regulations on specific subject or when in doubt, please refer to the compliance department for guidance, TNB staff can also refer to the PMA –AML/CFT Laws and Regulations link available <http://www.pma.ps/Default.aspx?tabid=856&language=en-US>

1.4 AML Policy

Anti-Money Laundering (AML) and Combating Terrorists Financing (CTF)

1. Introduction

With the increasing risk of money launder faced by financial institutions around the world, regulators are focusing on the controls and procedures banks have put in place to prevent money laundering and actively assist law enforcement authorities in detection and in investigation. To this end, The National Bank has set out the following high-level policy on the prevention of money laundering.

2. Policy Guidelines

The National Bank's (herein referred to as The Bank) anti-money laundering policies will be applicable Bank wide to all business and service units of the bank and its subsidiary companies

3. The National Bank's Policy against Money Laundering & Combating Terrorists Financing

The policy has been produced in accordance with PMA requirements and might extend to international requirements and best practices at certain levels. The guidelines are designed to provide adequate support to the business to minimize the risk of money laundering and comply with legislation and regulations.

The principles set out below on the prevention of money laundering (dealing with the proceeds of crime) or the financing of terrorist activity (where the funds may or may not originate from crime). The policy applies to all countries in which The National Bank operates. It is a clear statement to our staff and regulators of our

position on this critical risk issue. The policy is essential in order to deter money launderers from targeting TNB and to protect us from regulatory penalties, litigation and reputation risk. As an organization committed to the prevention of money laundering, TNB will:

3.1. General principles for combating money laundering and terrorist financing

- The principles outlined below form the Bank's principles for combating money laundering (dealing with the proceeds of crime) or financing terrorist activities (where the funds are first derived from the proceeds of crime). The policy is a clear statement to our employees and regulators about the bank's position on this serious issue. It is necessary to deter money launderers from targeting the bank and protecting it from regulatory penalties, litigation and reputation risks.
- As an institution committed to combating money laundering and terrorist financing, TNB is keen to do the following:
 - Establish clear lines of internal accountability and responsibility. Primary responsibility for the prevention of money launder rests with the business, which must ensure that staff is adequately trained and that appropriate internal controls are in place and operating effectively. The business is supported in meeting this responsibility by the Compliance Department.
 - Document, implement, and maintain local systems, controls and procedures which interpret this policy for each business in the context of local regulations.
 - Take all reasonable steps to verify the identity of our clients including the beneficial owners of corporate (including trusts) and the principles behind customers who are acting as agents. We will take all reasonable steps to ensure that information about clients is kept up-to-date.
 - Establish systems to retain adequate records of identification, account opening, and transactions for a minimum of ten years.
 - Refuse any transaction where, based on explanations offered by the client or other information, reasonable grounds exist to suspect that the funds may not be from a legitimate source.
 - Where required, make prompt disclosures of suspicious transactions or proposed transactions to the relevant authorities, through the Compliance Department.
 - Educate and train our staff in the recognition of suspicious transactions, the requirement of local legislation, TNB policy on prevention of money laundering and the systems, controls and procedures implemented in each jurisdiction.
 - Co-operate with any lawful request for information made by government agencies during their investigations into money laundering.
 - Support governments, law enforcement agencies and international bodies such as the Financial Action Task Force, in their efforts to combat the use of the financial system for the laundering of the proceeds of crime.
 - Report money laundering issues to local management and on regular basis. TNB Money laundering Reporting Officer (Head of AML/CFT department) will determine and communicate the content, format and frequency of management reporting.

3.2. Local Legislation and Regulatory Requirements

In general, local regulations stress robust KYC procedures, transaction monitoring, suspicious activity reporting and staff training as the foundation for prevention of money laundering.

Decree No (20) for the year 2015 read in addition to Amendments Issued by the Decree Law No. (13) Of 2016 later amendments criminalize money laundering and form the cornerstone of Palestine anti-money laundering requirements and procedures. The following offences are examples of serious crimes covered under this law:

1. Participation in a criminal group or an organized fraud group.
2. Human trafficking and alien smuggling.
3. Sexual exploitation of children and women.
4. Illegal trafficking in narcotics and psychoactive substances.
5. Illegal trafficking in arms and ammunition.
6. Illegal trafficking in stolen and other goods.
7. Bribery and embezzlement.
8. Fraud.
9. Counterfeiting currency
10. Counterfeiting and piracy of products.
11. Crimes in violation of the Environment Law.
12. Killing or serious harm.
13. Abduction, holding captive, or taking hostages.
14. Burglary and theft.
15. Smuggling.
16. Extortion, threat, or intimidation.
17. Forgery.
18. Piracy on marine and air navigation.
19. Offences provided for in articles (99,89,88,87) of securities law in force
20. Corruption offences
21. Tax crimes
22. Illegal sale or conversion of land by the applicable regulations in Palestine, including mediation or any act aims to illegally alienate land or part of the land to be annexed to a foreign country.
23. Offences provided for in Antiquities Law operating in Palestine
24. Breach of trust
25. Financing of terrorism and terrorist acts
26. Electronic piracy of all kinds

The Financial Follow-up Unit (FFU) is Palestine's financial Intelligence Unit for analyzing and investigating Fraud and suspicious transactions.

The Palestinian Capital Market Authority has issued AML regulations applicable to the securities markets and institution subject to its authority.

Decree No (20) for the year 2015 read in addition to Amendment Issued by the Decree Law No. (13) Of 2016 describes in detail the conduct and activities that constitute "terrorism" within the definition of the law, to whom the law will apply and the penalties, for breaching any of its provisions.

3.3. Responsibility of Reporting

Under the current regulations, each bank has reporting obligations to the Financial Follow-up Unit (FFU) of the PMA. Each Bank has a designated Money Laundering Reporting Officer who is responsible for reporting any suspicious transactions to the respective FFU. There is an established process for internal review and reporting to the MLRO (See below).

The business raises Suspicious Transaction Reports (STRs) to the MLRO who reviews these STRs and engages in more detailed investigation and may in turn report the STR to the FFU. The National Bank recognizes the importance of properly identifying customers and their transactions and is committed to prevent Money Laundering and Combat Terrorism Financing.

The main elements of the Bank's money laundering prevention policy are as follows:

- Obtaining full information/identification of customers, beneficial owners of companies in order to understand the ownership and control structure of all legal entities. In the event of any person claiming to be acting on behalf of another, such a person must have proper legal authority to do so. The same applies on customers activities through comprehensive Know Your Customer and Customer due Diligence process. It is our policy that transactions will not be executed, nor business relationships entered into, with customers who fail to provide sufficient and accurate evidence of their identity. (Source: Article 6.2 from the AML-CFT manual for Banks issued by the PMA and Decree Law No. (13) Of 2016 - Article 6).
- Branches and/or business units will not open anonymous accounts, nor accounts in obviously fictitious names or numbers. The bank should always rely on the account holder's name as in the passport or the trade license in case of juridical persons. (Source: Decree Law No. (13) Of 2016 - Article 6- Identification of Customers).
- If a branch and /or business unit suspects that the funds or transactions derive from or contribute to money laundering, they will promptly report their suspicions in the required manner. (Source: Decree Law No. (13) Of 2016 - Article 13- Duties of the Supervisory Authorities).
- Where transactions have no apparent economic or visible lawful purpose or are suspected of money laundering, their background and purpose will, as far as possible, be established, recorded and reported in the required manner.
- Branches and/or business units are to treat with caution, business relationships and transactions with persons, companies and financial institutions from countries which do not apply adequate controls against money laundering .(Source: Decision No. (1) of 2017 and its amendments to Decision No. (3) of 2019 of the FFU - Related to High-risk and other monitored jurisdictions).
- Where the soundness or legitimacy of the source of funds cannot be established, such transactions will be reported. (Source: Decree Law No. (13) Of 2016 - Article 14- Reporting).
- Where it is suspected that a customer is conducting transactions on behalf of non- mandated parties, branches and/or business units will take all prudent and reasonable measures to verify and record information about the true identity of the principal or beneficiary of such transactions.(Source: AML/CFT instructions number 2 for the year 2016 Sections 5).

- The National Bank will comply with all lawful instructions of competent authorities with respect to reports made under Anti Money Laundering legislation. (Source: Decree No (20) for the year 2015 –Article 11).
- Spreading Money Laundering awareness and prevention culture to all staff via specific training activities and periodic bulletins.
- Regular review of the above elements by the Banks compliance officers/AML Head of department/ internal auditors and/or external examiners from local and international regulatory authorities.
- Maintenance and Retention of Records i.e. maintaining and keep the physical records pertaining to customer identification and transactions for a minimum period of 10 years.
- The policy of The National Bank is to follow sound banking practices by complying with legal and professional responsibilities. Our policy against Money Laundering and Terrorism Financing is to keep an eye on any possible effort made by any person to use the bank as a channel to move funds as part of any criminal activity.
- We closely monitor unusual transactions carried out by our customers or any other person through our banking operations. We also carry out an inspection of our customers' accounts periodically to ascertain whether the transaction in the account reflect their business activity.
- Reporting suspected cases of following proper procedures and rules, gives the bank and employees protection against lawsuits and procedures for violating bank secrecy or criminal lawsuits regarding the implementation of a suspicious transaction in accordance with Articles No. (14, 15) of the Anti-Money Laundering and Terrorist Financing Law.

3.4. Screening

All new accounts are scrutinized against the PMA, FFU listing, OFAC and United Nations Lists.

All additions to the listings issued by FFU are reviewed and updated in our local listing for confirmation of no activity or otherwise with these individuals and/or organizations is FFU of AML/CFT Committee.

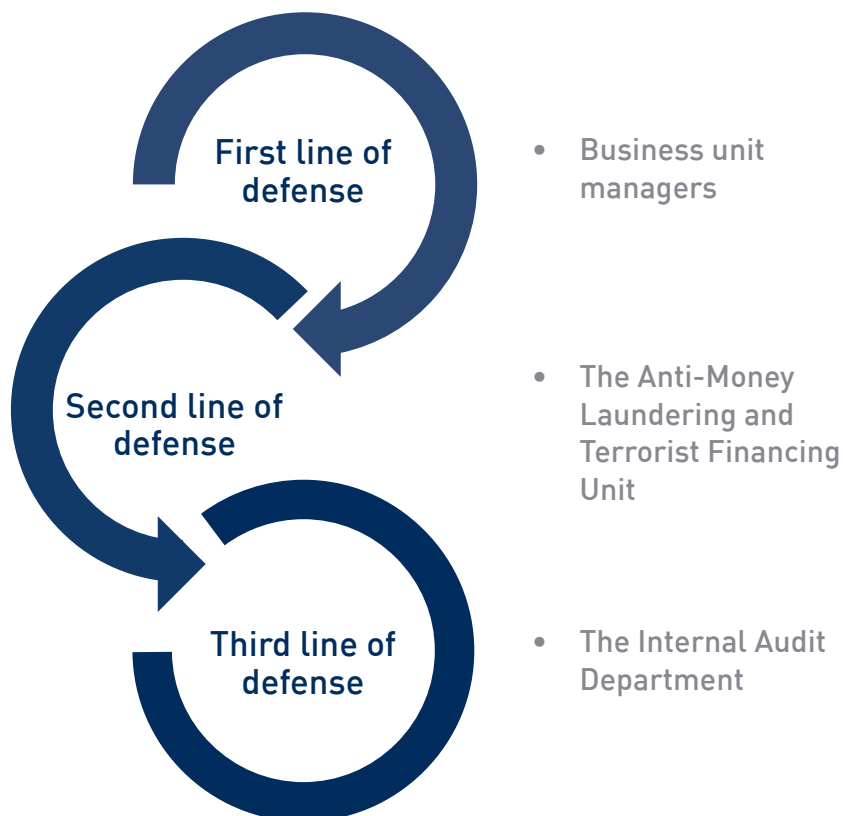
3.5. Training

We at The National Bank will provide ongoing training to our employees on Money laundering prevention and Combating Terrorist Financing to ensure that they are aware of:

- a Ways to identify signs of money laundering that arise during the course of the employees' duties.
- b Steps to be taken once any suspicion is identified.
- c Roles of the employees in the Bank's compliance efforts.
- d Staff should NOT tip-off any person, including the customer that the said customer's transaction is being scrutinized for possible involvement in suspicious money laundering operations and/or terrorist financing.
- e The bank's record maintenance procedure for suspicious transactions.
- f Disciplinary consequences for non-compliance with the AML policy or non-reporting of any suspicious transactions.

2. Roles and responsibilities at the bank level

2.1 Defense Lines



- 1) First line of defense: The responsibility to combat money laundering and terrorist financing lies primarily with business unit managers, where managers and employees of business units must ensure compliance with all applicable laws and regulations related to their departments by ensuring the establishment of policies and procedures and providing adequate training and awareness to unit employees .
- 2) The second line of defense: The Anti-Money Laundering and Terrorist Financing Unit should provide guidance and support to the business unit managers to ensure that those units comply with the bank's laws, regulations, policies and procedures. The Anti-Money Laundering and Terrorist Financing Unit assesses the risks of money laundering and terrorist financing at the bank level and establishes internal policies and procedures to prevent or reduce those risks. Reporting periodically to the Compliance Committee of the Board of Directors. In addition, the Anti-Money Laundering and Terrorist Financing Unit will report cases of suspected money laundering and terrorist financing to the Financial Monitoring Unit in the Palestinian Monetary Authority.
- 3) The third defense line: The Internal Audit Department performs periodic audits of the Anti-Money Laundering and Combating the Financing of Terrorism Unit to ensure that it is operating effectively and reporting to the Audit Committee.

2.2 Responsibility of the Board of Directors (Compliance Committee)

The Board of Directors must:

- 1) Establishing a function for combating money laundering and terrorist financing to follow up on compliance with the provisions of the decision in the law on combating money laundering and terrorist financing, this function should be assigned to an independent employee with proper ranking (holding a manager title) as “Anti-Money Laundering and Terrorist Financing Officer”.
- 2) Supervising the anti-money laundering and terrorist financing function in the bank and ratifying the charter or any other official document according to which this function is created.
- 3) Adopting a clear organizational structure for the function of combating money laundering and terrorist financing, provided that the organizational structure is appropriate with the size of the bank, its branches, the complexity of its operations and its database.
- 4) Adopting job descriptions for anti-money laundering and terrorist financing function that include tasks and responsibilities, qualifications and specifications for the occupants of those jobs.
- 5) Adopting a working procedures guide for the anti-money laundering and terrorist financing function based on risks (RBA), in accordance with Financial Action Task Force (FATF) recommendations, best international practices, basic principles and guidelines issued by the Basel Committee for Effective Banking Supervision, the guide should clearly set the priorities and responsibilities of the AML function, methods of work and mechanisms for reporting and presenting the results of the work and mechanism for taking corrective actions in the event of any violations.
- 6) Ensuring the independence of the AML function and adopting a fair salaries, rewards, incentives system for anti-money laundering and terrorist financing employees at the bank as well as accountability policies in the event of default or breach of job duties.
- 7) Make available adequate financial budget to ensure that the function operate in a manner that achieves the purpose of their creation and raises the ability of employees to manage the risks of money laundering and terrorist financing and reduce them, with budget provisions for training of qualified human cadres, automated systems and applications for combating money laundering, terrorist financing and inquiries on International and Local Sanctions and freezing lists.

2.3 Responsibility of the executive management

Procedures by executive management and business unit managers should include the following:

- 1) Providing adequate controls, systems and programs to identify and prevent any potential misuse of financial and banking services, products and technologies, and reporting on potential violations, provided that the following are guaranteed:
 - A. Electronic systems and programs for combating money laundering and terrorist financing, to be able to classify customer risks, control and track financial operations according to specific scenarios and indicators, and monitor unusual and suspicious operations and movements.
 - B. Electronic systems and programs to inquire about the customer base periodically on the International and Local sanctions and freezing lists and to inquire about parties to external financial operations before they are implemented.
- 2) Ensure that the subsidiary companies of the bank implement the requirements and standards for combating money laundering and terrorist financing policies and procedures.
- 3) Monitoring and auditing the bank’s employees’ accounts to ensure that they are not misused for the benefit of others and / or not in accordance with their nature and purpose or in criminal activities and work to monitor the employee’s unusual financial activity, and to check the suitability of these operations with the nature of the accounts and monthly income, and work to verify the extent of the safety of operations and the adequacy of due

diligence measures.

- 4) Promoting administrative and disciplinary measures against violating employees who are proven to have committed incidents that harm the integrity and reputation of the bank as a result of misusing their accounts or committing financial crimes such as fraud and embezzlement, and that includes informing the Monetary Authority and the competent authorities of any breaches or violations of laws, regulations, instructions, policies and operating procedures in effect.
- 5) Prepare a policy to combat money laundering and terrorist financing and prepare work procedures to implement the requirements and measures to combat money laundering and terrorist financing and the principles of due diligence with the aim of strengthening ethical and professional standards and preventing the financing of terrorist activities.
- 6) Strengthening controls of entry to the bank, including inquiring about the names of persons intended to be employed by banks and / or contracting with them and / or attracting new strategic shareholders and verifying the sources of their money intended to be used to purchase bank shares, with the aim of limiting entry to any persons listed or suspected of having committed Money laundering or terrorist financing crimes or any of the original crimes.
- 7) Keeping abreast of developments related to the risks of money laundering and terrorist financing inherent in the business units for which they are responsible.
- 8) Ensure that business units for which they are responsible comply with all relevant laws, rules and regulations in addition to the bank's internal policies and procedures.
- 9) Ensure that the Anti-Money Laundering and Terrorist Financing Unit is properly equipped with the resources / structure and has the appropriate authority.
- 10) Effective participation in strengthening the fight against money laundering and terrorist financing within the policies and procedures of the National Bank and the Code of Ethics, through:
 - A. Being present and participating in activities related to combating money laundering and terrorist financing, such as seminars and training.
 - B. Approving the proposed initiatives by the Anti-Money Laundering and Terrorist Financing Unit.
 - C. Providing the necessary resources for training courses and ensuring the attendance of employees in these courses.
 - D. Dealing strictly with cases of money laundering and terrorism financing discovered or cases that are discovered.
 - E. Encourage employees to inform the anti-money laundering and terrorist financing unit official of any suspected cases.
 - F. Ensure employee performance evaluation in light of compliance responsibilities and goals as part of the performance measurement process.

2.4 Internal audit responsibility

- 1) The adequacy and sufficiency of anti-money laundering and terrorist financing work program policies and procedures.
- 2) Enhanced due diligence and due diligence procedures, with the focus on high risk clients and operations.
- 3) The efficacy of applying the risk-based approach.
- 4) The effectiveness of bank employees in implementing policies and procedures.
- 5) The adequacy and effectiveness of the AML standards and scenarios defined on the banking programs and systems, including their ability to identify risk, unusual activity and suspicious cases.
- 6) The suitability of keeping records and providing relevant statistics.

7) The extent to which the bank has addressed deficiencies that were discovered during previous audits.

3. Anti-Money Laundering and Terrorist Financing Unit

3.1 Organizational Chart



3.2 The independence of the Anti-Money Laundering and Terrorist Financing Unit

The Anti-Money Laundering and Terrorist Financing Unit and all its employees enjoy independence from any commercial, administrative, or control-related position within the bank in order to allow them to carry out their work freely and objectively. Independence is achieved through organizational and objective status:

1. From an organizational point of view, the Anti-Money Laundering and Terrorist Financing Unit is hierarchically linked and reports directly to the Compliance Committee and is empowered to perform its roles and responsibilities on its own initiative. It is indirectly linked and reports to the General Manager (Executive Management).
2. In order to ensure objectivity, employees of the Anti-Money Laundering and Terrorist Financing Unit are not permitted to assume commercial or operational responsibilities. Moreover, as a guideline, objectivity is presumed to fade when AML / CTF staff control the operations or activities for which they have had authority or responsibility in the past.

The Anti-Money Laundering and Terrorist Financing Unit official reports directly to the Compliance Committee, where he submits semi-annual reports on activities related to anti-money laundering and terrorist financing. These include statistical data reports, challenges and threats that exist regarding money laundering and terrorist financing, the risks of money laundering and terrorist financing. The anti-money laundering and terrorist financing unit official meets at least once a year with the Compliance Committee and has the right to direct access to the Compliance Committee on anti-money laundering and terrorist financing issues. It is not permissible to place employees and officials of the Anti-Money Laundering and Combating the Financing of Terrorism in a position that entails a potential conflict between the unit's responsibilities and any other responsibilities they may have.

3.3 Assigning and terminating the services of the Anti-Money Laundering and Terrorist Financing unit official

1. The official of the Anti-Money Laundering and Terrorist Financing Unit and his deputy shall be appointed by the Board of Directors (the Compliance Committee that emerged from the Board members), provided that the prior approval of the Monetary Authority is obtained on the appointment.
2. The bank submits the curriculum vitae of the candidate to fill the position, with a copy of the passport and the

identity of the candidate, and the necessary documents and certificates according to the requirements of the instructions issued by the Monetary Authority regarding appointment, transfer, disciplinary procedures and resignation.

3. The bank will inform the Palestinian Monetary Authority immediately if the position of the Anti-Money-Laundering and Terrorist Financing Unit official or his deputy, and the person assigned to carry out his duties within the permitted mandate period according to the applicable instructions, becomes vacant.
4. The bank will be provided to the Palestinian Monetary Authority with the reasons that led to the termination of services or removal of the anti-money laundering and terrorist financing unit official or his deputy.

3.4 The responsibilities of the Anti-Money Laundering and Terrorist Financing Unit

The Anti-Money Laundering and Terrorist Financing Unit official shall perform the following tasks and responsibilities:

1. Ensure that the bank meets and complies with the requirements and duties of combating money laundering and terrorist financing stipulated in the Anti-Money Laundering and Combating the Financing of Terrorism Law and the instructions of the Monetary Authority and the National Committee to Combat Money Laundering and Terrorist Financing and the bank's approved policies and work procedures, including:
 - A. Take samples of opened accounts and executed operations and perform compliance checks on them.
 - B. Reporting on the environment and effectiveness of combating money laundering and terrorist financing with the bank, cases of failure to implement anti-money laundering and terrorist financing measures, instances of non-compliance of bank employees with the application of identification and customer verification procedures, due diligence and support, and recommendations for treatment and correction.
 - C. Follow-up on the immediate implementation of the Security Council resolutions and stop the execution of financial operations decisions issued based on the UN Security Council resolutions in accordance with the legislation in force in the State of Palestine.
 - D. Maintaining the internal documents and reports received and referred to the Monetary Authority and the Financial Follow-up Unit.
 - E. Apply the risk-based approach (RBA) and classify the bank's customers according to their degree of exposure to the risks of money laundering and terrorist financing (high, medium, and low), and take into consideration the risk assessment targeting the facility, customers, products, distribution channels and the geographical dimension.
 - F. Review the classification of the degree of exposure of bank's customers to the risks of money laundering and terrorist financing periodically, and in the light of unusual operations and the information and data available to the bank.
 - G. Examining the bank's customer base against the international and local sanctions embargo and freeze lists in a manner commensurate with the size of the database and financial operations, along with documenting them.
 - H. Participation and / or supervision of preparing a self-assessment of the risks of money laundering and terrorist financing in the bank, including the identification of those risks according to the four main categories (clients, products and services, distribution channels, geographical dimension).
 - I. Participate in assessing the risks of money laundering and terrorist financing in new financial and banking products, services and technologies before launch and when developing and modifying previous products, services and technologies, and participate in setting and strengthening the controls and measures necessary to reduce and manage those risks and document that.
2. Raise recommendations on financial budgets, the adequacy of anti-money laundering and terrorist financing programs and systems, and their need for development and modernization.
3. Answer requests and inquiries related to financial operations, money laundering operations and terrorist financing received from the concerned authorities in a manner that does not conflict with the laws in force, and to provide those entities with data, records and documents quickly without delay or procrastination.

4. Monitor and control ongoing financial operations using automated programs and systems to combat money laundering and terrorist financing, monitor and review unusual financial movements and operations and suspicious operations, and maintain records, studies and information on all data for all suspicious and unusual operations.
5. Receive and investigate all communications received from any of the bank's employees in case the employee has doubts that the operation to be executed is a process suspected of being linked to money laundering or terrorist financing or from the original crimes and documenting the results of that investigation.
6. Immediately inform the Financial Follow-up Unit of suspected operations that include the crime of money laundering or terrorist financing or any of the original crimes, whether these crimes were committed, so that suspicious reports are reported according to the approved reporting mechanisms.
7. Inform the Money Laundering and Terrorist Financing Section of the Monetary Authority about suspicious activities and fraud cases that affect the bank's safety, security and reputation.
8. Contribute to setting and coordinating training programs for combating money laundering and terrorist financing, training the bank's employees and informing them of the requirements and developments related to combating money laundering and terrorist financing, in a way that contributes to enhancing their capabilities to discover money laundering and terrorist financing operations.
9. Continuous communication with the bank's departments and departments to address the shortcomings and weaknesses resulting from the national assessment of the risks of money laundering and terrorist financing (NRA), and to ensure that the requirements for strengthening the anti-money laundering and terrorist financing environment are met.
10. Provide statistics related to the following:
 - A. The number of instances of receiving and answering the information request.
 - B. The number of suspected cases that were referred to the unit according to the type of suspected crime.
 - C. Number of suspected instances where not enough suspicion indicators were identified.
 - D. regular screening of the names in the customer base against the lists of international and local sanctions embargo and freezes lists.
 - E. Verify the number of cases in which the names of the Bank's customers were similar to the names of the persons and entities included in the lists of international and local sanctions embargo and freezing lists and the number of cases in which it was verified that the names of the clients were not identical to the names of these persons and entities included in the lists.
 - F. The courses and training programs granted to the bank's employees on the developments and requirements of combating money laundering and terrorist financing.
 - G. The number of cases of currency seizures, checks, and documents suspected of counterfeiting or forging.

4. Customer Due Diligence - Know Your Customer

4.1 Introduction

The National Bank is committed to conducting all its myriad business activities in accordance with the highest ethical standards. The principal source of reputational risk to banking is an inadvertent association with customers involved in criminal activity. Laundering money derived from criminal activity and terrorist financing (which may or may not originate from proceeds of crime) is an area of concern to The National Bank. The Bank has adopted policies and procedures designed to protect it from doing business with these types of customers.

These policies are also consistent with the Bank's desire to have all necessary information to meet customers' needs, deliver excellent service and satisfy all related legal, regulatory and best practice requirements.

The Bank's policy is that no banking business should be carried out unless we know the Customer. Precisely how much information is required to fulfill this requirement, beyond the basic identification and account opening procedures required by the Bank and laws depends on the type of customer, business, services and products involved. It should be explained to the customer that the information is required to allow the Bank to provide the best possible service and make available the most suitable products, whilst at the same time satisfying any applicable laws.

4.2 Purpose of Know Your Customer

Complying with this Know Your Customer policy will help the Bank build effective relationships with its customers. It will also lead to compliance with relevant laws and regulations and adherence to sound and recognized banking practices. It will also help reduce the risk of the Bank being used by criminals in furtherance of illegal activities e.g. money laundering. Finally, it will also safeguard the Bank's name and reputation.

4.3 Rule of Thumb on Account Opening

It is important that senior managers are aware of their responsibility for ensuring that staff involved in opening accounts is fully conversant with the internal policies, procedures, regulations and prudent requirements pertaining to such activities. The following is a brief overview of some of the more important requirements:

- The National Bank Know Your Customer (KYC) Standards are designed to deter and detect attempts to use the Bank to place, layer or integrate proceeds of criminal activity through any of its products or services.
- An account must never be opened until the identity of the customer and the true ownership has been satisfactorily established.
- It is imperative that all account opening procedures are followed, and documentation completed. If a potential customer refuses to produce any of the requested information or documentation or, information is not forthcoming, any relationship which has already begun must be terminated.

4.4 CDD & KYC Policies

The National Bank staff will take all necessary steps to verify the identity of our customers, including the beneficial owners of corporate entities (including trusts) and the principals behind customers who are acting as agents. We will take all reasonable steps to ensure that Know Your Customer ("KYC") information is collected and kept up-to-date, and that identification information is updated when changes occur in the parties involved in a relationship.

In support of this principle, these standards cover:

1. General KYC standards for opening new accounts;
2. Specific KYC standards for certain types of new accounts;

3. Exceptions to normal KYC standards for new accounts; and
4. Sanctions and warning lists

General

Effective KYC procedures form a fundamental part of any anti-money laundering internal control regime. They can reduce the risk of accounts being used for money laundering or terrorist financing and can help identify suspicious transactions. They can also protect The National Bank against fraud and other reputational risks. KYC always includes customer identification (evidence of identity and address), but depending on the risk associated with an account, it can also extend to more detailed due diligence about the customer and their business. KYC is an ongoing process - it does not end when account opening is completed.

These Risk based KYC standards apply to all TNB's branches and subsidiaries, from retail services to commercial trade transactions and correspondent banking. Although most references below are to "accounts", this term should be taken to include all types of relationships with customers including one-off transactions for non-account holders.

Transferring of opening balances from an account held by the potential customer in another bank will be subjected to the same KYC standards. A status opinion of the customer standing maybe requested from the other bank if required but will not be considered as a substitute to The National Bank's due diligence procedures.

For any reason if it is found that an applicant is being refused banking facilities by another bank, enhanced diligence procedures will be applied prior to commencing a business relationship. As a general rule the Bank will not open accounts for customers who request anonymity or who wish to operate the account under an assumed name or use a number as reference. The only exception will be when the customer provides a request from the Ministry of Interior. In such cases the opening of the account should be authorized by the Branch Manager.

The Bank will exercise special care when offering finance facilities to persons holding 2nd Nationality passports issued by a country other than the country of their birth. Further background screening of potential customers will be required prior to opening the account or granting finance facilities to these individuals or to business entities owned by such individuals.

For students (>18 years), evidence of identity and address verification should be obtained in the normal & address verification can be obtained through a parent or the prospective customer's college or university.

For minors & people without full legal capacity only Savings and fixed deposit accounts can be opened and should be opened in the presence of a guardian and all transactions should be executed only in the presence of the guardian. Hence the guardian will be subjected to the same KYC standards. (All parties' passport copies should be obtained). Enhanced due diligence procedures will be applied prior to commencing a business relationship.

The designated staff opening the account will be responsible for their diligent completion and to maintain strict confidentiality in respect of customer information provided therein.

4.5 General KYC Standards for Opening New Accounts

The level of KYC information obtained when opening a new account, and the subsequent management of the account, must be aligned to the potential money laundering risk it presents. This approach enables effort to be more effectively focused on higher risk accounts and reduces The National Bank's overall exposure to money laundering risk. To achieve this risk-based approach businesses must:

- A. Comply with local legislation or regulation on AML/CTF Procedure under TNB's AML policy.
- B. Comply with the laid down procedures to risk assess new relationships or accounts in terms of the potential money laundering risk they present.
- C. Obtain KYC information appropriate to the level of money laundering risk assigned to the account.
- D. Monitor and manage new & existing accounts that reflect the level of money laundering risk assigned to them.
- E. Comply with the identification process of any potential or existing customer who is the subject of a sanction or on a recognized warning list.

4.6 The Risk Assessment of New Accounts

The category of risk assigned to an account will determine the KYC information required and the subsequent intensity of management and monitoring of the account.

A business must have a risk assessment process in place to enable new accounts or relationships to be divided into three categories for anti-money laundering purposes:

- lower risk (**LR**) (refer to Appendix **A**)
- medium risk (**MR**) (refer to Appendix **B**)
- High Risk (**HR**) (refer to Appendix **C**)

All accounts must be assigned to one of these three categories. This will enable us to effectively manage particular exposure to money laundering risk.

The risk assessment process used must incorporate:

- An assessment of the risk associated with the product or service and its potential vulnerability to being used for money laundering purposes.
- An assessment of the risk associated with the type of customer and the nature of their business or source of wealth.
- An assessment of the anticipated volume of activity (e.g. thresholds).
- A review of the relevant KYC information for all customers against PEP / FPEP / Warning list databases.
- Official findings on non-compliant or high-risk countries (see Appendix **D** List).
- Local assessment criteria to reflect any money laundering risks specific to the operating environment in the country concerned.

As stated above, the risk assessment procedures adopted by a business must consider the level of risk associated with the country(s) that the customer resides in, operates from or sources funds from. Extra care and due diligence is required for higher risk countries. For the purposes of these KYC/CDD standards, **High Risk Countries are listed in Appendix D**. This list considers official information concerning the adequacy of anti-money laundering regimes in different countries (e.g. Financial Action Task Force - FATF) and other country risk information (e.g. Transparency International).

Head of Compliance may add/remove countries to/from this list, considering local issues. The rationale behind these should be explained to CEO and business heads.

It is recognized that for some types of account it will not be possible to establish, at the point of account opening, whether the financial thresholds will be exceeded. While such an account may initially be designated as lower risk based on other criteria, it should be flagged for review and re-designation/classification as medium or special risk as required.

4.7 Risks of new products and services

In order to reduce the risks of money laundering and terrorist financing in financial and banking services and products and in line with the requirements of the Palestinian Monetary Authority and the recommendation of Financial Action Task force No. (15), it:

1. All risks associated with the new service, product or technology, including the risks of money laundering and terrorist financing, must be identified and evaluated before launching any new financial or banking product or service and / or using any new technologies.
2. Work to establish policies and procedures to manage these risks effectively.

4.8 KYC Requirements for Each Risk Category of New Account

The type of KYC information obtained for a new account must be aligned with the risk categorization to which it has been assigned.

- For Lower risk accounts, only basic identification information, using reliable evidence, is required.
- For medium risk accounts, enhanced KYC requirements apply such that the basic identification information is supplemented with more detailed data on the customer and their business / source of funds.
- Special risk accounts must be subject to the most comprehensive levels of KYC. They would be expected to represent only a very small proportion of a typical portfolio.

For the avoidance of doubt, KYC data obtained and retained must meet PMA's regulatory requirements, and legal requirements and evidence of identification information (identity and address) must be obtained for all customers.

The most common form of reliable identification evidence for an individual is a passport or national identity card, both of which are normally signed, numbered, bear a photograph, and contain additional information such as date of birth and nationality. All this information can be vital to the Authorities in the course of a money laundering investigation. Whenever possible, identification evidence should be provided by the customer at a face to face meeting with Bank staff, or the Bank's appointed direct sales agents, before an account is opened. Where verification of identity cannot be completed face to face (e.g. operating accounts through the internet or by emerging technologies) as for those customers who open accounts at The National Bank. The potential customer will be required to present themselves at the nearest branch to sign and hand over necessary documents after initial login via electronic means except for incremental accounts that have been opened on face to face basis.

Where the customer is based in a high-risk country, copies of all relevant pages of identification documents must be certified as "originals sighted" with the certifiers name and contact details (e.g. branch, staff number, telephone etc.) annotated. Copies must be clear and legible, details of any verification checks undertaken must be made available and retained on file. Customers should not be asked to send important identification documentation such as Passports, Identity Cards, and Drivers Licenses etc. via the mail because of the risk of loss or interception.

For corporate and institutional customers (and subsidiaries of such customers) whose capital (both equity and debt) is traded on a recognized, local and international stock exchange, there is no need to identify individual shareholders or directors beyond what might form part of normal commercial due diligence. Evidence of this special "exchange listed" status must be recorded and retained on file.

For private, unquoted entities (i.e. companies, partnerships and institutions), in addition to verifying the legal existence of the business, including its registered and operating addresses, it is essential to identify those who have control over the entity and its assets. Therefore, a risk-based approach should be adopted to identify persons with significant control over the entity's assets (e.g. persons or beneficial owners holding more than 10% interest in the company). This includes the verification of the directors (including the managing director) and all signatories with a significant level of authority (e.g. CEO, Finance Head etc. where not already included above) in line with the requirements for personal customers (above). In addition, for individuals who have authority to act on behalf of the entity, suitable evidence of such authority (e.g. Board Resolutions) should be obtained.

The verification of entity addresses, and the addresses of the directors and beneficial owners of the entity, can be supported by sight of official documentation issued by the company registrar, company searches or certified documents received from banks in non-high risk countries (copies of which should be countersigned by the Bank and retained). For addresses outside Palestine, or an address different to that on the official documentation, must be separately verified. However, the verification of the identity of the relevant directors/beneficial owners as required by this chapter, must be undertaken in the same way as for personal customers as set out above.

A) Personal Accounts

1. Full name, date of birth, and nationality (Name of the customer as appearing in the passport. Refrain from using abbreviations);
2. Current residential / business address, telephone/fax numbers and email address (P.O. Box addresses is not sufficient);
3. Occupation or Nature of Business;
4. Passport Copy and Residence Visa;
5. Purpose of the account where this is not clearly implicit in the product or service being offered. (While the use of a mortgage or auto loan account may be clear, a savings account could for example, be used for several different purposes and a record should be retained of its intended use);
6. Period of service with present and previous employers;
7. Estimated monthly income and expenditure;
8. Estimated monthly turnover on the account and # of Transactions (Dr & Cr);
9. Number of dependents;
10. Other activities of the customer;

B) Juridical Accounts

1. Full legal name and, if applicable, registration number;
2. Registered and operating addresses;
3. Nature of business;
4. Full name, date of birth, and nationality of beneficial owner, directors;
5. Passport Copy and Residence Visa for all parties;
6. Purpose of account if not clearly implicit in the product or service being offered;
7. A certified copy of the company's registration certificate issued by a valid Palestinian company observer (with a renewal date of no more than one year).
8. Memorandum & Articles of Association;

9. The approval of the board of directors of the company in question or the authorized signatory on behalf of the company, according to the registration certificate, to open the account by bank stating the type and currency of the account to be opened and the purpose of opening the account.
10. Valid power of attorney in favor of the person(s) authorized to sign on behalf of the business entity and their delegator powers;
11. A form bearing the company's name in Arabic and English, and its address and official stamp.
12. A written commitment by the company's board of directors to inform the bank of any future material changes that occur in the company or those authorized to sign for the company.
13. Identification of the legal representative of the company. (Basic data)
14. Regarding non-profit companies, the approval of the Prime Minister must be met to accept donations, aid, and financing, and explain the purpose thereof.
15. Description of the customer's primary trade area, and whether international;
16. Transactions are expected to be routine;
17. Description of the business operations, the anticipated volume of cash and total sales, and a list of major customers and suppliers;
18. Information in relation to those individuals controlling the account (beneficial ownership should clearly be understood). When identifying beneficial ownership and control of companies we should first try to identify the natural persons who ultimately have a controlling ownership interest; but if there is doubt over whether such persons hold the beneficial ownership, or when no such natural persons can be identified, any other natural persons that may exercise control over the customer through means other than shareholding should be identified. If these measures fail to identify a natural person exercising such controls, we should then take reasonable steps to identify the natural person holding a senior management position. If a company is controlled by other companies, then we need to identify controlling beneficial owners, regardless of the number of levels;
19. In all cases true copies of the original passport should be obtained from business owners, partners, Power of Attorney holder and all other signatories.

At the time of opening an account an assessment must be made to determine whether it is likely, perhaps when combined with existing accounts for the same customer, that the account activity will exceed the financial threshold value limits (see Appendix A). This assessment should be documented as part of the account approval process. If necessary, the additional KYC data required for Medium or Special Risk at account opening should be obtained to avoid the need to revert to customers within a short period of time to seek further KYC information.

KYC information must be obtained and retained for all parties to an account, including any directors, beneficial owners or controllers of funds who may not be signatories to the account (unless the exception for listed and significant entities, Governments). Identity information for all relevant parties must also be recorded on the relevant account management systems to facilitate future searches against sanctioned names etc. Guidance on acceptable types of identification evidence is set out below.

Where the customer is, or appears to be, acting on behalf of a third party, identification evidence must be obtained in respect of both parties and proper legal authority should be verified.

Here are the guidelines for the types of acceptable identification guides:

1. KYC Requirements for Lower Risk Accounts (LR)

For **LR** accounts, subject to any of the specific exceptions below (i.e MR and HR), reasonable steps must be taken to verify that the customer is who they claim to be by obtaining, assessing, and retaining sufficient evidence of their identity and their residential and, where appropriate, operating address. This must be done as soon as reasonably practicable after contact is first made with the customer or potential customer and, subject to the exception below before the account is operational.

As a minimum, the KYC information that must be obtained include: The full legal name and residential / registered or operating address must be verified separately using reliable evidence.

2. KYC Requirements for Medium Risk Accounts (MR)

The basic identification KYC outlined above must also be obtained for all **MR** accounts, but this must be supplemented by additional information to provide for a fuller understanding of the customer, their business, and their proposed use of the account.

This “**enhanced**” KYC information should be documented on a Risk Assessment Profile Forms, as a minimum it should include:

- An understanding of purpose of the account or relationship.
- An understanding of the source of funds likely to pass through the account - based on information about the nature of the customer’s business, employment or other income generating activities (for Private and Offshore Banking customers, it will also be appropriate to record the underlying source of wealth and estimated networth);
- An indication of the anticipated volume and type of activity to be conducted across the account; and
- Where relevant, an understanding of the relationship between the various signatories and underlying beneficial owners

3. KYC Requirements for High Risk Accounts (HR)

HR accounts are those that represent a particularly high potential risk in relation to money laundering. A list of mandatory **HR** accounts is at (**Appendix C**), but a business must designate any additional types of account that, in its judgment, could represent a particularly high potential vulnerability to money laundering or, for example, are known to be of particular concern to local regulators. Nevertheless, **HR** accounts would be expected to represent only a very small proportion of a typical country portfolio.

The way in which **HR** accounts are treated compared with **MR** accounts will focus primarily on the management and monitoring of the account once it is opened (see below). Any additional KYC data appropriate at **HR** will be determined by the exact nature of the account itself, but could include, for example:

- A full understanding of the purpose of any trust or corporate structures involved in the relationship, particularly for complex arrangements. In these circumstances documentation explaining why the structure was put in place should be obtained; trustees have to obtain and maintain adequate and accurate beneficial ownership information, including information on the identity of the settler, the trustee(s), and the protector (if any), as well as disclose their status as trustees.
- A full understanding of the source of wealth and estimated net worth of an individual;
- The purpose and source of funding for specific transactions; or in the case of services provided for another financial institution, an understanding of their anti-money laundering policies and procedures

Identify the real beneficiary

1. A “real beneficiary” is a natural person who has or ultimately controls the customer or account of the person on whose behalf he conducted the transaction, or the person exercising effective final control over a legal person and its management.
2. The real beneficiary is usually the person who basically owns or controls the client or is acting on his or her behalf in conducting a specific transaction or activity. As for the individual customer, he himself is usually considered the real beneficiary unless it is proven otherwise, and the bank must make the necessary inquiries when there is evidence that the customer He does not act on his own behalf.
3. When an individual (the natural person) is identified as the real beneficiary, the bank must obtain the same information that helps to identify and verify his identity as a natural person as stated in the requirements to identify (the natural person).
4. If the customer is a legal person, the bank must identify and verify the identity of the real beneficiaries who own 10% or more of the shares or voting rights in the legal person (a partnership, or a company, for example).
5. The bank must obtain the temporary and permanent addresses of the real beneficiaries, and the risk-based approach can also be applied in this by defining reasonable measures to verify the address, taking into account the number of the real beneficiaries, the nature of their business, the proportions of their shares in the legal personality and the extent of family interdependence among them.

Address Verification

Certified copies of address documents, or a record of the manner, in which address verification was achieved, must be retained. Acceptable address evidence to be retained on file can take various forms, for example:

- 1) documented record of a home visit;
- 2) confirmation from locally approved and reliable electronic verification methods (e.g. copy of utility bill or Etisalat bill; or letter from employer)
- 3) Copy of an original official document issued by a central or local government body.
- 4) P.O. Box addresses are not acceptable, For all risks, customers should provide their residential address by way of a recorded description or other means.

Ongoing Account Management

Ensure that the account opened is not used as a vehicle to facilitate transactions which are beyond the scope of its primary operating objectives. The National Bank risk based approach to KYC is based partly on differentiating between the KYC data required for each risk category of account when opened, and partly on differentiating between the way in which each category of account is subsequently managed and monitored.

Once opened, the ongoing management of an account for money laundering prevention purposes needs to ensure that KYC data is complete and kept up to date and that material changes in the account profile / account activity are identified. Such monitoring of accounts is a critical part of the risk-based approach – it determines whether the account should remain in the same risk category. Review procedures must therefore identify two types of change.

1. Any change in KYC data (normally notified by the customer) that results in a change of risk category e.g. a change to an overseas address, or a relationship with a Politically Exposed Person (P.E.P or EPEP) is identified.
2. Any change in the activity profile of the account that exceeds LR thresholds or change is inconsistent with the KYC data on file and our understanding of the customer’s business, such changes must be identified and reviewed and, where necessary, the account risk level reclassified. In line with any reclassification, the required KYC information

must be obtained and assessed to ensure the appropriate risk classification.

While the primary purpose of the review process is not only to undertake a detailed analysis of individual transactions but to observe any activity across the account that is considered suspicious and must be reported in line with local procedures.

Dormant Accounts

Where accounts have been classified as “dormant”, are reactivated, the customer should be contacted, and their identity verified (or re-verified if identification evidence is already held) to the required guidelines for new accounts.

Account Review Procedures

All staff will need to be vigilant in preventing the account/s of individual and corporate business entities from being used as a vehicle to facilitate transactions which are beyond the scope of its primary operating objectives.

The Bank will adopt periodical monitoring mechanism (both manual and system application based) to assess its customer’s transactions against the customers’ profiles and update its records as and when required.

LR Accounts: there is no fixed review period. Exception reporting procedures is in place such that they can highlight when account data relevant to the risk criteria set out in **Appendices A** have changed. For LR Corporate Bank’s borrowing accounts, monitoring should be supplemented by considering changes to money laundering risk as part of the normal Credit Application review cycle.

MR & HR Accounts: in addition to the normal exception reporting procedures established for LR , MR & HR accounts must be subject to an overall account review at least once every year. Reviews should be undertaken by the account relationship manager or equivalent, Changes to KYC data including beneficial owners, principal shareholders, or authorized signatories must be supported by appropriate verification evidence. The review should also determine whether an account should be re-graded/reclassified to LR, MR or High Risk. Procedures should be in place to provide monthly reporting of overdue reviews by age.

Direct contact with the customer is not a mandatory part of the account review process. Such contact would only be appropriate if, for example, a deficiency in KYC is identified, or further information is needed in order to understand fully the customer’s business or use of the account.

The review should be undertaken by the relationship manager or equivalent and independently checked by their line supervisor.

Fast remittances (Western Union)

The National Bank adopts the policies and procedures for combating money laundering and terrorist financing of the global agent and the sub-agent of Western Union and all of its contents as part of the Western Union agreement on all transactions executed through the National Bank and its network of branches and sub-agents. Where the following is adhered to:

1. Comply with all the contents of the policies and procedures in relation to combating money laundering, terrorist financing, combating fraud, and the special requirements mentioned.
2. Entering all the required data on the fast money transfer system in its correct form, in order to complete the KYC procedures.
3. Exercising due diligence to get to know the customer, his activity, and the real beneficiary between the parties to the transfer and verify that in appropriate ways.
4. Ensure that the customer appears in person to disburse the transfer, and that agencies or authorizations are not accepted to disburse quick transfers.
5. Not to exchange or send remittances except in the case of presenting official valid identity documents.

6. Dealing with unknown persons or those with pseudonym, fictitious or abbreviated names is prohibited in any case. (At least the first and last name are mentioned without abbreviations).
7. For WU operators the bank publishes awareness and appropriate culture regarding anti-money laundering, terrorist financing and anti-fraud on an annual basis or when there is a fundamental change in policies and instructions.
8. In the event that there is any kind of suspicion regarding the rapid remittances of a specific customer, coordination with the concerned authorities shall be made to assess the risks of dealing with the customer and take the appropriate decision according to the risk assessment study.
9. The results of the examination of incoming and outgoing movements, and any suspected cases examined in the department or reported, are included as part of the STR.

Specific KYC Standards for Certain Types of Account

For most types of account, the general KYC standards above should be applied. However, regulators and international bodies recognize that more specific KYC procedures apply to certain types of account e.g.:

A. Private Banking Customers

There has been several high-profile money laundering cases in the media involving high net worth individuals. The potential vulnerability of Private and Offshore Banking accounts to abuse by money launderers has been recognized and addressed by banks through the Wolfsberg Principles (available at www.wolfsberg-principles.com) and these should be reflected in the Private and Offshore Banking when we launch this business.

All new Private and Offshore Banking relationships are treated as MR and These types of relationships should normally be established through face to face meetings, however where this is not possible references to corroborate the applicant's reputation should be obtained. This is in addition to the further identification steps above. Under no circumstances must numbered or alternate name accounts be used, even where the identity of the underlying customer has been established and recorded.

B. Trusts

Money launderers may view the anonymity and complex structures associated with some types of Trust arrangements or fiduciary relationships as providing an opportunity to avoid identification procedures and conceal the origin of funds. It is therefore essential to verify the identity of the settlor of the Trust or fiduciary relationship (i.e. the person supplying the funds), those who have control over the funds (e.g. Trustees), beneficiaries, and any person who has authority to remove the Trustees.

Exceptionally, identification requirements may be waived for any Trustee who does not operate an account or give instructions relating to fund transfers. Whenever a Trustee is replaced, the identity of the new Trustee should be verified (in line with personal customers above) before they are allowed to exercise control over the funds. All this relevant information is usually available on the Trust Deed and this therefore should be sighted and evidenced accordingly

Whenever funds are received on behalf of a Trust or fiduciary relationship, the source of the funds must be properly identified, and the nature of the transaction understood (reasonable exceptions may be allowed in the case of regular receipts from the same, previously identified source).

For discretionary and offshore Trusts or fiduciary relationships, the nature and purpose of the relationship as well as the original source of funding must be ascertained

Care must be taken when fiduciary relationships are set up in offshore locations where strict banking secrecy prevails. Relationships set up in jurisdictions where no money laundering legislation or regulation exists will also warrant additional enquiries and measures. Written confirmation from the trustees or managers of the Trust that there are no anonymous principals should be obtained. The original source of the funding should also be

established.

Any application to open an account or undertake a transaction on behalf of another without the applicant identifying their Trust or nominee capacity should be regarded as suspicious and treated accordingly (see section on Reporting Suspicious Transaction)

Where customers are represented by non-financial business persons (e.g. lawyers), take reasonable measures to obtain information about the true identity of the person on whose behalf the account is opened or a transaction is conducted (beneficial owner) and ensure that the appointment of trustees are as per the trust deed which specifies:

- Name of the Trust and mailing address
- Jurisdiction of establishment
- Residential address (P.O. Box addresses is not sufficient).
- Certified True Copy of the trust deed/agreement; information concerning the nature & purpose of the trust and beneficiaries.
- Occupation or Nature of Business.
- Passport Copy and Residence Visa
- Full name, date of birth, and nationality of all parties on the account
- Name/addresses of principal owners /trustees

C. Powers of Attorney and Third-Party Mandates

The authority to deal with assets under a Power of Attorney or Third-Party Mandate constitutes a business relationship and therefore any person in that role must be identified in the same manner as the primary customer.

All Powers of Attorney accepted for individuals, corporate accounts, institutions or Trust businesses should always be verified (e.g. sight relevant POA agreements) and it is important that the reason for granting the Power of Attorney is understood and recorded and proper identification is met.

D. Financial Institutions

Financial Institutions are defined as any Bank, Finance Company, Brokerages, Money Changing Establishment, Financial or Monetary Intermediary or any other Establishment licensed by the PMA, whether publicly or privately owned.

The Bank will refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence, and which is unaffiliated with a regulated financial group (i.e. shell banks).

The National Bank will not open and maintain any account with Wire Transfer Traders / Dealers, who are not registered and licensed by the PMA.

It is essential to gain assurance that a financial institution, with which a relationship is proposed, is properly constituted, is supervised by an acceptable financial regulatory authority. Where they are responsible for financial regulation and, in addition to normal business considerations, is an institution with which we would wish to be associated from a reputational perspective. In support of this, KYC documentation to be sought could include:

- Obtain true copy of the institution's license.
- Receive request from FI to open Vostro Account and commence correspondent banking operation with the bank (proceed as per policy and procedure for opening Vostro Accounts).
- copy of the Certificate of Incorporation;
- copy of relevant internet page published by the institution's regulator;

- copy of the FI's KYC-MLP procedures
- Response to our AML Questionnaire

Discretion should be exercised as to whether these documents should be notarized. Consideration should also be given as to whether it is necessary to undertake further checks of the institution with the relevant regulator, a known correspondent in a suitably regulated country.

Given that the adequacy of anti-money laundering procedures may differ from one financial institution to another, the level of KYC due diligence can be determined as follows:

- For financial institutions in equivalent countries, it can be assumed that the institution will have in place appropriate anti- money laundering KYC controls in relation to its own customers.
- For branches or subsidiaries of financial institutions outside the equivalent countries, that have their Head Office in an equivalent country, a declaration must be sought from the Head Office that the branch or subsidiary in question follows money laundering prevention and KYC procedures equivalent to FATF standards.
- for all other financial institutions, reasonable steps must be taken to establish that they conduct sufficient due diligence on their customers and on the origin of funds passing through their account in line with FATF equivalent standards
- Relationships must not be established with "Shell Banks" that have no physical presence in any country, or with correspondents that allow their accounts to be used by such institutions
- Accounts should be terminated or not opened where the financial institution is unable or unwilling to confirm that they have adequate procedures to verify the identity of their customers. Accounts for financial institutions that fail to provide satisfactory answers to reasonable questions, including, where appropriate, confirming the identity of customers featuring in unusual or suspicious transactions, should also be referred to the head of the business unit and terminated.
- Relationship managers are responsible for regular reviews, on a risk-weighted basis, of relevant institutions' KYC procedures. Customer visits may provide an opportunity to achieve this. The results of the review should be recorded.

1. Financial Institutions acting as Correspondent Banks

In addition to the requirements for financial institutions (see above), greater due diligence should be taken where a correspondent banking relationship is created, particularly for higher risk financial institutions. These may include those from higher risk jurisdictions, ones that are privately owned or are managed by PEP's or FPEPs or have had regulatory problems historically (refer Wolfsberg Principles for Correspondent Banks "www.wolfsberg-principles.com" for more examples). Our correspondents should have internal anti-money laundering standards that are as robust as ours and it is particularly important to determine whether they take steps to thoroughly identify their own customers on whose behalf we may conduct transactions. Where their customers are other financial institutions or correspondents (i.e. downstream correspondent banks), our correspondent's due diligence procedures on these downstream correspondents should be questioned. This may require their AML procedures being reviewed. It is also essential, in order to identify any potentially suspicious activity, to understand the type of business undertaken by the correspondent itself and therefore the normal or expected use of the account.

2. Financial Institutions subject to Equivalent AML Regulations Acting as Agents

Where a financial institution acts as an agent for an underlying customer, the identity of the underlying customer must also be verified in accordance with these KYC Standards. Evidence of the underlying customer's identity is not required where the financial institution has been deemed to have FATF equivalent standards in place.

Financial Institutions outside of equivalent countries must also give written assurance that they have verified the underlying customer's identity to FATF standards. Where the Financial Institution is from a high-risk country, evidence of the underlying customer's identity must be verified as if they were a direct customer of The National Bank.

E. Bearer Shares

Bearer shares are negotiable instruments that accord ownership of a corporation to the person who possesses the bearer share certificate and are common in some parts of the world. As a result, it can be extremely difficult to verify the identity of the holders and therefore the owners of companies. Even where this can be confirmed at account opening, the ease with which they can be transferred means that this information can become out of date very quickly and the risk of dealing with undesirable individuals is significantly increased. This risk may be mitigated in some circumstances where detailed records of all holdings and transfers are maintained by a reliable authority.

Bearer Shares are vulnerable to abuse by money launderers and relationships involving Bearer shares require the highest level of due diligence (Special Risk).

F. Account Opening before Obtaining Full KYC Evidence

Under exceptional circumstances (Lower and Medium Risk customers only), where it is essential to conduct business before full documentary evidence of identity has been obtained, the reasons for the exception must be recorded in the customer's file and the exception resolved as a matter of urgency. However:

- Payments to third parties should not be allowed under such circumstances so that, in the event of subsequent decline and account closure, all funds can be returned to the customer.
- To avoid the risk of a customer using such a situation to legitimize funds by passing them through the Bank, cash or traveler's cheques above USD 5,000 should not be accepted onto the account
- Exceptions to these rules can only be authorized by the CEO and Head of Compliance or managers formally delegated by them.
- Accounts opened under this exception must be carefully monitored by management and by the Business (RM, Sales Officer) or Compliance Officer until all outstanding information has been obtained.
- Business must not be continued with customers who fail to produce satisfactory evidence of their identity within 30 days and maximum up to 50 days.
- An undue delay by a customer in providing satisfactory proof of identity, without adequate explanation, might be viewed as grounds for suspicion that the person concerned is involved in money laundering and consideration should be given to making a report to the Head of Compliance

Sanctions and Warning Lists

A formal sanction is a legally binding instruction to exit, report or freeze an account or category of accounts. Depending on local regulatory procedures, warning lists may or may not have a legally binding effect on the Bank's actions.

Local procedures for opening new accounts, must incorporate adequate controls to ensure that individuals, organizations, and corporate entities who are identified in accordance with all the above, are not subject to official sanctions and do not appear on warning lists of suspect names, such as those suspected to be linked to terrorism, circulated by governments and law enforcement agencies.

It is the responsibility of the Head of Compliance to be aware of sanctions and warning lists relevant to their jurisdiction; and to inform the businesses accordingly. These should be cross-checked against the Bank's customer database regularly.

Sanctioned countries are decided by Compliance Department from time to time.

Suspicious Transactions

Suspicious transactions are often those that are inconsistent with a customer's business and banking activities. Transactions which do not appear to be in keeping with the purpose and usual activity of an

account, or the business conducted by an account holder, may be considered suspicious and must be examined and reported if necessary.

Similarly, transactions which fail to adequately identify or attempt to disguise the origin of funds of the beneficiary of transferred funds may be considered suspicious.

Obviously, the key to recognition of suspicious transactions is by knowing enough about the customer and his/her/their business to identify transactions that may be unusual or suspicious. Possible money laundering and suspicious transactions, including:

1. Cash Transactions;
2. Customer Accounts;
3. Investment Related Transactions;
4. International Transactions;
5. Letters of Credit – Trade Finance;
6. Loans; and
7. Electronic Banking;

Staff should make themselves familiar with the “indicators” as to possible money laundering and suspicious transactions.

Appendix A – Lower Risk Accounts

Risk assessment procedures must be implemented within the bank at the level of customer risk, products and services, geographical area and delivery channels. The following transactions may be considered low risk:

- 1) Clients who work in jobs with a relatively stable source of income and this source is legitimate and well-known and justify the nature of the work carried out by the customer within the responsibilities of his job (Palestinian citizens and those with salaries who have one or more products related to the assets).
- 2) Clients with a good reputation and known as private companies that have a long and documented history in the activities they carry out and the sources of their funds are known in addition to a good knowledge of the owners and controlling the company.
- 3) Relationships with regulated financial institutions, or that have a headquarters in Palestine or countries that implement FATF-compliant standards or have adopted anti-money laundering standards equivalent to that of FATF. (When relying on the fact that the headquarters is in a country that adopts FATF standards or equivalent standards, its policies and procedures must be binding on the relevant subsidiary and subsidiary).
- 4) Relationships with Palestinian government departments or their agencies (including their own legal firms).
- 5) Relationships with registered public companies and their subsidiaries listed on a local or internationally recognized stock exchange.

Appendix B – Medium Risk Accounts

For any customer that does not meet the risk rating factors mentioned in the low and high-risk accounts, the customer's rating is of medium risk.

Appendix C – HR Accounts

The following customer's accounts must be classified as HR for Retail, Corporate & FI:

- i. All relationships involving Politically Exposed Persons (P.E.P's and Foreign PEPs). See **Appendix I**, below for clarification.
- ii. All relationships with overseas customers residing or operating in or any customer where the bank has evidence that the funds are sourced from high risk countries. **(See Appendix D for HRC)**.
- iii. Relationships involving offshore trust structures.
- iv. Financial Institutions in high risk countries where the bank concerned is not a FATF jurisdiction or has not adopted the equivalent standards.
- v. The complexity of relationships and connections in the structural structure of the company or institution and in cases where it is not possible to find reasonable legitimate business relationships or ties.
- vi. All relationships with businesses involved in activities considered to be particularly vulnerable to money laundering risk such as defense, money services bureau, exchange houses, dealers in high value commodities (e.g. traders in precious metals) jewelers, auction houses, antique dealers, real estate brokers/dealers.
- vii. Charities, religious bodies, and non-profit companies.
- viii. Sanctioned Entities and Individuals.
- ix. Engaging in businesses where cash is used extensively in lieu of other means.
- x. The nature and scope of the customer's commercial activities and their geographical location indicate more sensitive levels of risk.
- xi. Correspondent banking relationships where the bank concerned is not in an equivalent jurisdiction or has not adopted the equivalent standards.

Appendix D – High Risk Countries

The circulation of high-risk countries is relied upon by the Monetary Authority circulars.

Appendix H - Note on Politically Exposed Persons (P.E.P's)

Accounts for PEP's and Foreign PEPs should always be treated as **HR**.

There is no internationally recognized legal definition of a Politically Exposed Person. However, they would normally be considered to include senior present and former political figures, their immediate family and close associates:

1. Senior political figure is a senior figure in the executive, legislative, administrative, military or judicial branches of a government (elected or non- elected), a senior figure of a major political party, or a senior executive of a government owned corporation. Corporate entities, partnerships or trust relationships that have been established by, or on behalf of, a senior political figure are also included.
2. Immediate family typically includes the person's parents, brothers and sisters, spouse, children, in-laws, grandparents and grandchildren where this can be ascertained.
3. Close associate typically includes a person who is widely and publicly known to maintain a close relationship with the senior political figure and includes a person in a position to conduct substantial domestic and international transactions on his or her behalf.

TIPS for Sales and Service Officer/ Customer Service Manager/ Branch Manager

Ensure that the following are adhered to when opening an account:

1. On receipt of a customer's requests to open an account and keeping in line with knowing the customer under "Know Your Customer", enquire and verify the identity of the person prior to adhering to such request.
2. Avoid establishing relationship with those customers who do not provide satisfactory information required by the bank.
3. It is prohibited to open current accounts (with cheque book) to non- residents.
4. The original passport should be available at the time of opening the account. The Account opening officer should make a copy of the passport (including the page with the valid residential visa) and the copy should be stamped "a true copy of the original" and must diarize for renewal of passport as well as residence visa
5. All necessary information and documents on juridical persons especially the trade license must also be diarized for renewals in order to keep a copy of the valid license on bank's files at all times.
6. Accounts should not be opened for "Associations/ Non-Profit Organizations", except for those associations that present a true "declaration decision" issued and signed by H.E. the Minister of Social Affairs.
7. Verify the identities of all parties to the account (i.e. joint account holders), and signatories to the mandate where the person/s with whom the bank has contact is/appears to be acting on behalf of another person/s; i.e. minor.
8. In relation to customer's residential address, ensure that the applicant's residential address can be physically located by way of prominent landmark, or street & district name or other means, as a P.O. Box number alone is not sufficient evidence of address.

In the course of conversation with the customer either at the time of opening the account or thereafter, attempt to establish the following:

- Consider the proximity of the customer's residence or place of business to the bank office or branch location. If it is inconvenient, the bank should determine why the customer is opening an account at that location.
- Call the customer's residence or place of employment to thank him or her for opening the account. Discovery of disconnected phone service or no record of employment warrant further investigation.

- Consider the source of funds used to open the account. For example, large cash deposits at the time of opening the account and subsequent deposits.

If the customer cites vague terms (such as: a sales employee, businessman, or company manager), inquire about the nature of the business or the name of the company and its activities.

- Ensure that the validity of customer's ID is checked before opening additional new account or granting any new facilities.
- After opening the account obtain details in order to establish the sound knowledge of the customer and account conduct.
- Check the name of the business enterprise through external search engines and bank references.
- If appropriate, visit the customer's business to verify its existence and its Ability to engage in the business it described.
- Consider the source of funds used to open the account. Large deposits, especially cash.
- Pay attention to corporate entities, international business corporations or nominee officers, especially if such organizations are based in countries or jurisdictions considered to be secrecy or money laundering havens.

Cooperative Societies / Charitable / Social or Professional Societies

Verify the information required hereunder:

- Constitution/By- Laws of the society, association/club;
- Certified True Copy of the minutes of the meeting at which the current office bearers were elected;
- Resolution of the governing body authorizing the opening of the account. Name and addresses of the authorized signatories and Certified True Copies of their passport;
- Identify all signatories and their authority to exercise significant influence over the organization's assets; i.e. members of governing body, the president, board member, the treasurer, PEPs etc.
- Verify independently the persons involved ensuring that they are true representatives of the institution and independent confirmation of the purpose of the institution.

Embassies and Diplomatic Missions

Where the account to be opened is for an Embassy or Diplomatic Missions, inquire the following information and obtain the required certificates as follows:

- Letter of authority to open an account, bearing the original signature of the Head of the Diplomatic Mission;
- Certified True Copy of the Ministry of Foreign Affairs letter permitting the establishment of the Diplomatic Mission;
- Foreign Country letter appointing the Consul/Ambassador, duly attested by the Ministry of Foreign Affairs; and
- Certified True Copies of passports of the Ambassador/Consul and other authorized signatories.

Safe Deposit Lockers

- Where facilities such as safe custody and safety deposit boxes are provided, the identification procedures set out above must be followed (unless, as in the case of existing customers, the information has already been obtained).
- Ensure to lease locker facilities to only those accounts holders with the bank and who are well known to the

branch staff and managers approval obtained.

- Vigilantly monitor frequent movements/ usage of the vault.
- Enquire further instances where customer requires additional lockers or requires a bigger locker.

KYC/CDD for Customer Remittances and Third-Party Banking Transactions Branch Teller Cash / Cheque Credits

While accepting cash/ cheque deposits to a customer's account from a non-account holding third party

- Ensure to request from the depositor a valid identification document (passport/ ID (for both nationals and expats).
- Make a copy of the ID provided by the depositor and attach with the deposit slip after due verification with the original
- Obtain the depositors contact number/s and note it beside the signature on the deposit slip.
- Input the name of the depositor in the transaction description in the banking system.
- Where the depositor is an account holder, ensure that depositor's name in the credit slip is same as per the title in the depositor's account.
- Where the depositor is unable to provide and establish a valid identity, forward the matter to designated Compliance officer at the Bank.

In the case of a suspicious transaction, complete the form specified by the Palestinian Monetary Authority and state the source of the funds and the purpose of the deposit and send it to the bank's money laundering official.

Outward Cashiers orders/Demand Drafts / Telegraphic Transfers (amounts =or>USD 5,000.)

- Any transaction from a non-customer must be restricted and shall require approval from the Branch Manager.
- The remitter shall provide the bank with a valid identification document (passport, ID and address (not PO Box only).
- The purpose of remittances will also be subjected to scrutiny and should be noted on the application.
- The full name, address and contact telephone numbers of the remitter as well of the beneficiary mentioned on the request /application.
- The purpose of the transfer and all other standard information required in the transfer shall be written on the application form by the remitter.

The failure of the employees concerned to comply with these standards of know-your-customer is subject to disciplinary action in accordance with local law and internal HR policy

4.9 Politically Exposed Persons

1. Introduction

Politically Exposed Person (PEP) is a term defined by the Financial Action Task Force (FATF) as an “individuals who are or have been entrusted with prominent public functions in a foreign country, for example: Heads of State or of the government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials, ministers and deputy or assistant ministers, members of parliaments, central banks governors, ambassadors etc.”

As per PMA definition Politically Exposed Person (PEP) are

“Individuals who are or have been entrusted with any of the following functions wither they were foreign or local including their family members and any related party to them:

- 1) Persons in public political or senior positions:
 - a) Country president, his consultants, and presidents of origination that are reporting directly to presidency office;
 - b) Prime Minister and Members Ministers Counsel and the like;
 - c) Ministries Secretaries and the like;
 - d) Managers and general managers in government, public office and the like;
 - e) Managers and heads of public bodies and institutions and the like.
 - f) President and members of the Legislative Council;
 - g) President and members of the Judicial Council;
 - h) Judges of courts at various degrees;
 - i) Members of the Public Prosecution;
 - j) Managers and leaders of security agencies officials and directors of departments in public administrations and governorates;

- k) Managers, leaders and officials of the Palestinian Public Security, and directors of public security departments in public administrations and governorates; and
 - l) Leaders and senior positions in Palestinian political parties and factions and those with important positions in these parties and factions.
- 2) Presidents, deputies, board members and directors of charitable institutions or associations, local and foreign NGOs.
 - 3) Ambassadors, consuls and members of the diplomatic corps.
 - 4) Presidents and directors of international organizations, their deputies and their representatives.
 - 5) Executives in state-owned entities.”

Immediate family members of the persons referred to above include:

- a. The spouse
- b. Any partner considered by national law as equivalent to a spouse
- c. Children and their spouses or partners,
- d. Parents; grandparents and grandchildren and close relations through marriage.
- e. Persons known to be close associates’ of the persons referred to at (a) above including:
 - 1. Any natural person who is known to have joint beneficial ownership of legal entities and legal arrangements, or any other close business relationship, with a person referred to at (a) above. and
 - 2. Any legal entity or legal arrangement whose beneficial owner is that natural person and which legal entity or legal arrangement is known to have been set up for the benefit of a person referred to at (a) above.
 - 3. Persons who are widely known to maintain an unusually close relationship with the PEPs and will include those persons who conduct business on their behalf.

Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. Hence, the PEP, their family members and close associates are considered to be High risk persons.

Given the nature of the risks and the fact that PEPs covers a very broad range of individuals, implementation of this policy requires careful consideration and the use of judgment. It is not the intention to undermine acceptable low risk business opportunities

e.g. the provision of normal credit facilities/finance to PEPs of modest wealth living within their means or indeed to prevent accounts being opened offshore for higher risk categories. What is needed is that any higher risk accounts are only opened after enhanced due diligence has been undertaken and there has been appropriate sign off and that there is ongoing monitoring of the account to prevent any change in the nature of the operations of an account going unnoticed.

2. General Guidelines

Enhanced due diligence will be observed at all times when opening accounts for Politically Exposed Persons (PEPs) since they potentially represent higher risk as they either are in a position to exert undue influence on decisions regarding the conduct of business by private sector parties, or have access to state accounts and funds. The very reason for PEP screening is to fight (high level) bribery, illegal kickbacks, corruption, tax fraud, embezzlement or outright theft of State assets or funds....etc, not simply establishing the fact that an individual is a PEP.

FATF encourages Financial Institutions (FIs) to consider the geo-political conditions of a country and region when dealing with PEPs. By using industry recognized and accepted third party standards for the risk ranking of countries, one might consider either reducing or extending the period a person remains Politically Exposed as part of a risk based approach.

PEPs pose a potential risk. They are not terrorists, money launderers, narcotics traffickers or necessarily high risk to institution. They are to be identified and their account activities monitored for any form of bribery or corruption, but they remain bankable as long as the procedures for PEPs are followed. Corrupt PEPs with money to hide will evolve their tactics and will be forced underground, they hide their identities and manage their wealth through trusts, corporations and even charities.

3. Policy Guidelines

Businesses have to complete an enhanced customer due diligence in particular areas of:

- 3.1 The decision to open an account for a PEP will be taken at a senior management level with consultation of the Head of Compliance.
- 3.2 The National Bank will not open an account for a PEP or their immediate families without prior approval of a senior management level with consultation of the Head of Compliance.
- 3.3 Sufficient information will be gathered from any new customer, which will require to be checked from reliable information available publicly or through respected intelligence sources, in order to establish whether or not the customer is PEP.
- 3.4 Considerable precautions will be taken by Business units to thoroughly assess the customer' profile and will be required to diligently complete the "Know your customer" (KYC) form for the specific type of account opened, as PEPs (or rather their family members and close associates) would not necessarily present themselves in that capacity, but disguise themselves as ordinary business people, masking the fact they owe their high position due to illegitimate means.
- 3.5 The sources of funds will be thoroughly investigated prior to accepting such funds into the PEP account as under certain circumstances, the bank and/or its officers and employees themselves could be exposed to charges of money laundering, if they know or should have known that the funds stemmed from corruption or other financial crimes
- 3.6 The Bank will be through and vigilant regarding high profile individuals or with persons and companies that are clearly related to or associated in having business relationships with PEPs.
- 3.7 Business units will be compelled to re-establish/ reconsider the banker- customer relationship with a person (as well as people and companies that are clearly related to him/her) whom it suspects of subsequently being a PEP.
- 3.8 As all PEPs may not be identified initially and since existing customers may subsequently acquire PEP status, such business relationships should be subjected to additional scrutiny, enhanced due diligence and an ongoing review.
- 3.9 All Politically Exposed persons (PEPs) or Foreign Politically Exposed persons (FPEP) account/s will be flagged on the Banking System **(Development should be made with IT for future MIS and queries).**

4. Opening an Account for a PEP

4.1 Customer Service Officer/ Manager

- 4.11 When handling the request to open an account, perform an Enhanced Due Diligence before establishing a relationship with Politically Exposed Persons (PEPs).
- 4.12 Determine and identify PEP customers according to the above mentioned definitions.
- 4.13 Identify the accountholder and beneficial owner and/or signatories.
- 4.14 Matching their names against the Watch List.
- 4.15 Obtain relevant information directly from the account holder, such as:
 - a. Official responsibilities of the individual's office;
 - b. The nature of the title (e.g., honorary or salaried);
 - c. Level of authority over government activities or other officials;
 - d. Access to significant government assets or funds;
 - e. Identify the accountholder's country of residence;
 - f. Customer's source of wealth, including the activities that generate that wealth;
 - g. The source of funds for any initial investment as well as subsequent major additions is identified;
 - h. Ongoing monitoring of accounts for sizeable and unusual activity is undertaken with greater frequencies.
- 4.16 Determine the purpose of the account and the expected volume and nature of account activity.
- 4.17 Make reasonable efforts to review public sources of information.
- 4.18 Take reasonable measures to establish the source of wealth and source of funds of such customers; [such details shall be obtained from the potential customer when completing the Know Your Customer (KYC) form and before activating the account].
- 4.19 Coordinate with Compliance department to obtain information on immediate family members or close associates having transaction authority over the account.
- 4.110 Obtain approval from Senior Management (CEO or his Delegate) for establishing or maintaining business relationships with such customers by forwarding the account opening request (customer details) to Compliance department through the designated compliance officer in the branch/ business unit. Attach the obtained approval to the account opening documents.
- 4.111 Flag all PEP or FPEP account/s in the Banking System at the time of Account Opening.

1.2 Compliance Officer

- 1.2.1 On receiving approval to open the account for politically exposed person, forward the necessary approval to the designated account opening staff ensure that information obtained is precisely filled in the "Know your customer" form.
- 1.2.2 Seek approval from Head of Compliance in case the account opening request is from a foreigner nationality identified as a PEP. On receipt of approval, forward the approval to the account opening staff.
- 1.2.3 Monitor the business relationship and transactions performed on the account and subject the account to a more detailed review at least once a year.

1.2.4 Closely monitor and properly identify the source of funds and immediately report any un-identified source of fund to Money Laundering Reporting Officer in Compliance Department for their scrutiny and onward investigation

1.3 Head of Compliance - MLRO

1.3.1 Verify the potential customer's name against the internal as well as external database sources to ascertain further details of the customer.

1.3.2 Ascertain the gravity to which the customer is politically exposed and probably linked to money laundering sources.

1.3.3 Depending on the exposure as revealed through the search engines, approve/or decline the account sighting the exposure and risks associated in establishing banking relationships with the potential PEP customer and inform the business accordingly.

1.3.4 Seek approval from CEO /his authorized designate to commence banking relationship.

1.3.5 On receiving the approval, instruct the compliance officer and business unit to;

- a Conduct enhanced ongoing monitoring of the business relationship and transactions in their account.
- b Closely monitor and properly identify the source of funds.
- c Report any un-identified source of fund to the MLRO in Compliance Department

1.3.6 In case the account was declined, immediately arrange to inform the concerned compliance officer and business unit to communicate the management's decision to decline the relationship.

1.3.7 On receiving satisfactory evidence of customer misconduct or violations as per relevant Anti Money Laundering regulatory, keep the senior management informed and take the following course of actions:

- a Maintain strict confidentiality.
- b Fill Suspicious Transaction Report highlighting and indicating reason and escalate to the MLRO.
- c MLRO in turn will report the unusual transaction to "AML Suspicious Case Unit" at PMA along with the duly required completed forms after completing the necessary investigation.
- d Handle the customer account with utmost discretion without "tipping off" the customer.
- e Assist PMA's Officials in their investigation and if required freeze the account as per PAM written request.
- f Retain all records pertaining to the customer and make them available for further reference of PMA examiners / Investigating authorities until they declare the investigation as completed and closed.

5. Suspicious Activity Reporting

5.1 Introduction

The National Bank (TNB) will refuse any transaction where, based on explanations offered by the customer or other information, reasonable grounds to exist to suspect that the funds may not be from a legitimate source or are to be used for an illegal activity such as terrorism.

"Suspicious Transaction" is often used in the context of money laundering prevention. Suspicious transactions are often those that are inconsistent with a customer's business and banking activities. Transactions which do not appear to be in keeping with the purpose and usual activity of an account or the business conducted by an account holder, may be considered suspicious and must be examined and reported if necessary.

Similarly, transactions which fail to adequately identify or attempt to disguise the origin of funds of the beneficiary of transferred funds may be considered suspicious. (AML/CFT manual issued as part of the PMA instruction-section 3 point 1.8).

Obviously, the key to recognition of suspicious transactions is by knowing enough about the customer and his/her/their business to identify transactions that may be unusual.

The National Bank will make prompt reports of suspicious activity, or proposed activity through the appropriate internal channels

We will cooperate with any lawful request for information made by government agencies during their investigations into money laundering.

5.2 Internal Reports

Internal reporting requirement for TNB and the disclosure requirements extend to cover all forms of suspicious activity e.g. knowledge or suspicion of a link to money laundering may arise where a new or existing customer, or a person acting on behalf of a customer, simply sets out a proposal for business, whether or not a subsequent transaction takes place. It can also arise where the Bank is acting in an advisory capacity only.

All businesses must have clearly documented procedures in place that require all relevant members of staff to report knowledge of money laundering or suspicious activity as quickly as possible. The procedures must provide for the escalation of reports to Money Laundering Reporting Officer (MLRO). They must be documented. The standard STR form should be adopted in each business and support function.

Internal reporting procedures may allow staff to consult with line management, who may wish to comment on any proposed report before escalating it to MLRO. However, the procedures must enable all staff to make a report directly to MLRO if they so wish.

The procedures must provide for disciplinary action to be taken against any member of staff who fails, without reasonable excuse, to make a report or who blocks, or attempts to block a report by another member of staff.

5.3 Consideration of Internal Reports and External Disclosures

Businesses must have procedures in place to ensure that all internal reports are properly reviewed by the MLRO. The MLRO determines if a disclosure is required and ensure it is made promptly to the authorities.

It is essential that the MLRO has access to all information in relation to the account(s) under review in order to make a reasoned judgment on the need for further action including external disclosure. MLRO must therefore be given access to all available KYC information for the customer, or any person on whose behalf the customer has been acting, and the transaction history of the relationship.

The MLRO decision on external disclosure must not be the subject of consent or approval of any other person (this does not prohibit the MLRO from consulting with other managers in the process of arriving at a final decision).

The bank will maintain records of all Suspicious Activity Reports filed and the original or business record equivalent of any supporting documentation for a period of 10 years from the date account closure, unless it is held for investigation where, it will be retained until the PMA's Anti Money Laundering committee and FFU and/or other investigating state authorities declare that the investigation has been completed.

Following the making of a disclosure, full and prompt co-operation must be given to all legal requests to provide further information to the authorities to assist their investigations into money laundering.

Under no circumstances should a customer be informed that a disclosure has been made, as such notification (often referred to as "Tipping Off") could prejudice an existing or potential investigation by the authorities which might expose us to financial penalty and considerable reputational damage.

Where, following a disclosure, the PMA allows the relationship to continue and management decides to retain the account, subsequent activity must be subject to particularly close vigilance. Any new activity that adds to the original suspicion must be disclosed.

5.4 Exiting a Relationship

It is The National Bank's policy not to enter into or maintain relationships that we believe may be used, or are being used, for money laundering. Where a suspicion arises, therefore, management must introduce an intensified account monitoring regime and carefully consider, with advice from the Business and/or MLRO whether to continue with the relationship. Where an external disclosure has been, or is being, made, guidance should be sought from the AML/CFT committee and related FFU before exiting as such action may alert the customer and prejudice official investigations.

5.5 Transaction Monitoring

- Employees of the Bank and their authorized legal representatives will have the right to closely monitor unusual account operations carried out by the customer or their agents.
- All customer transactions will be screened on an ongoing basis to satisfy that the account is not used for any activities other than what the account was intended for and to identify any suspicious transactions.
- The Bank has the right to reveal, without notifying the applicant or seeking prior approval, the applicant's personal or financial information, including any suspected money laundering transactions, to the Financial Follow-up Unit of the AML/CFT committee or to any government, regulatory or legal authorities through the PMA.
- The Bank also has the right to release such information to their legal advisors in order to safeguard the bank against probable penalizations imposed by international regulatory authorities conducting routine investigations.
- The bank will review daily/periodical records, exception reports and other management information should be used to support the identification of suspicious transactions. Records of all transactions reviewed by the business will be maintained for a period of 10 years from the date of processing the transaction or account closure.

It is recognized that a business, supported by a specialist detection system provides the most effective way to meet legal and regulatory obligations and manage associated reputational risk.

It should be noted that standards in relation to the use of specialist systems for the detection of potentially suspicious transactions are quite separate from the requirements to review the overall profile of an account in order to comply with The National Bank KYC policy

Linked Transactions: a recognized technique used by non-account holders seeking to launder money is to undertake a series of transactions, each one of which is small enough to avoid normal KYC requirements or is just below local cash reporting limits. Where such linked transactions are identified, the circumstances should normally give rise to a suspicious activity report. Where feasible, relevant branch records should be periodically reviewed to identify possible linked transactions cases.

Dormant Accounts: In addition to the requirement of the KYC Section, transactions undertaken when a dormant account is re-activated should be subject to particular scrutiny and an internal report made to the MLRO if the re-activated activity is considered suspicious.

5.6 Suspicious Transaction – Money Laundering Indicators

Suspicion is personal and subjective and falls far short of proof based on firm evidence. Suspicion has been defined by the courts as to whether an event has occurred or not. Although the creation of suspicion requires lesser factual basis than the creation of belief, it must nonetheless be built upon some foundation.

In respect of these procedures a suspicious transaction, series of transactions or account behavior in general can be defined as:

“Where a business relationship exists (or is proposed) a suspicious transaction (or series of transactions or account behavior) will often be one that is inconsistent with a customer's know profile, legitimate activities or with the normal business for that type of account”.

Articles 2 and 8 of sections 6 of the AML/CFT manual for banks issued by the PMA contain a comprehensive list of indicators as to possible money laundering and suspicious transactions, including Cash Transactions\Customer Accounts\Investment Related Transactions\Letter of Credit – Trade Finance\ Loans i.e. Finance\Electronic Banking & Miscellaneous.

Staff should make themselves familiar with the contents of these articles and “indicators” as to possible money laundering and suspicious transactions, any other law, circular, notice, declaration, instructions issued by the PMA and related committees and units. Or any other relevant regulatory authority on this subject. These requirements and international standards for money laundering control and reporting, as contained in the following laws, Instructions, statutes and their corresponding regulations will be complied with:

- a. Decree No. (20) of 2015 and (13) of 2016: Anti-Money Laundering and Terrorism Financing And Its Amendments;
- b. Decree No. (14) of 2015: [Concerning the Enforcement of Security Council Resolutions](#);
- c. AML/CFT Committee Instruction No. (2-G) of 2017: [Related to Dealing with Money Exchangers in Israel](#);
- d. AML/CFT Committee Instruction No. (5) of 2016: [Related on Reporting Express Remittance Transactions](#);
- e. AML/CFT Committee Instruction No. (3) of 2016: [Related to Measures for the Importing of Used Car from outside Palestine](#);
- f. AML/CFT Committee Instruction No. (2) of 2016: [Related AML-CFT for Banks](#);
- g. AML/CFT Committee Instruction No. (1) of 2014: [Related to Political Exposure Persons PEPs](#);
- h. AML/CFT Committee through the Financial Follow-up Unit Decision No. (3) of 2019: [Related to High-risk and other monitored jurisdictions](#);
- i. AML/CFT Committee Decision No. (2) of 2019: [Related to High-risk and other monitored jurisdictions](#);
- j. AML/CFT Committee Decision No. (1) of 2019: [Related to High-risk and other monitored jurisdictions](#);
- k. AML/CFT Committee through the Financial Follow-up Unit [List of high-risk and non-binding countries](#) on AML / CFT standards by FATF;
- l. AML PMA instructions relating to the [AML-CFT Manual for Banks](#);
- m. AML PMA instructions relating to the [Anti-Money Laundering and Terrorism Financing Risk](#);
- n. AML PMA instructions Circular No. 253 of 2019: [Related to the Internal Audit on Banks AML-CFT Environment](#);
- o. AML PMA instructions Instruction No. (10) of 2019: [Related to AML-CFT Function](#);
- p. AML PMA instructions Circular No. 158 of 2017: [Assuring the update of Legal Entity and Natural Persons data](#);
- q. AML PMA instructions Circular no. 121 of 2017: [Related to Publicized Remedial Actions](#);
- r. AML PMA instructions Circular No. 29 of 2017: [Updating Legal Entity and Natural Persons data](#);
- s. UN security council Press release <https://www.un.org/press/en/content/security-council/press-release>;
- t. PMA AML/CFT local freezing lists <http://www.pma.ps/Default.aspx?tabid=866&language=en-US>
- u. The Forty (40) Recommendations relating to Combating Money Laundering as well as the Nine (9) Special Recommendations relating to Combating Terrorist Financing issued by the FATF.
- v. Other International Guidance on the subject of Anti-Money Laundering and Terrorist Financing including (but not limited to) Basel Committee publication No. 85 – Customer Due Diligence for banks, United Nations Resolutions and Guidance on the suppression of Terrorist Financing, Wolfsburg Principles etc.

It's the responsibility of the head of compliance and AML officer to follow up and keep the bank up to date with

the newly issued instructions and circulars by the AML/CFT committee, PMA and international best practices in relation to compliance.

5.7 Training

Staff should be trained and made aware of the importance of reporting STR requirements. All staff has personal responsibility to report suspicious activity. In case of breach of such responsibility staff will be subjected to internal disciplinary action and prosecution.

- The Compliance Department of the Bank will train and update its employees on the provisions of relevant anti-money laundering legislation and internal/international standards applicable for reporting of suspicious and/or unusual transactions.
- Important information received in between training sessions will be communicated through internal memorandums.

5.8 Suspicious Transaction /Exception Reports

This helps clarify what is expected from businesses relating to Suspicious Transaction Monitoring. While the below is not exhaustive, it describes some of the key controls/procedures that are expected to be followed:

- Follow the documented process that sets out what staff must do when they identify suspicious activity and to whom they must report it.
- The Branch Manager/ Unit Head is responsible for ensuring that his/her staff are aware of the AML-CFT Manual and its instructions No 2 for the year 2016, special care is taken in respect of the following:
 - **Article 4-2** should a non-account holder wish to pay, by cash, for a transfer/drat with **USD 5,000** or equivalent in other **currencies** (or more), the identity of the individual should be verified (name and full address of beneficiary, physical check of original **passport** or Labor Card). These details should be entered on required by the AML/CFT department as shown below and initiated by the customer and the bank officer and then forwarded to the Compliance Department. (Copy to be retained by the branch).
 - **Article 4-3,4&7** That in case of receiving a transfer/draft to be paid in cash or in the form of traveler's checks to non-account holders (note that in such situation, no monetary threshold is applicable). The form should be completed and forwarded to Compliance Department. (Copy to be retained by the branch).
 - **Article 9** states that the bank shall apply special attention and consider reporting any of the following situations, if deemed necessary:
 1. When renting safe deposit boxes;
 2. When requesting facilities against deposits;
 3. When depositing cash or travelers' checks in an existing account by persons not representing the owner of the account;
 4. When collecting international checks of unknown third parties;
 5. When requesting the execution of complex or large transactions specifically those that have no clear financial purpose and those related to offshore activity;
 6. Large cash foreign exchange operations (purchase and sale of currencies);
 7. Exchange large amounts of cash denominated in small amounts;
 8. Deposits of large amounts or recurring deposits of amounts summing up to large portions that are not with the

nature of the client's apparent activities and the usual volume of its operations;

9. Operate an account primarily for transferring large amounts to foreign countries or for receiving large-scale transfers such that it appears to be unjustified;
 10. Exchange of checks issued from abroad or nominal checks in large amounts that are not compatible with nature and the volume of the customer's usual activity, or claims to be, for example, gambling gains;
 11. Large or recurring transactions related to external activity, which the Bank considers to be disproportionate with the size of the activity.
- **Article 3** of AML/CFT Instructions No. (5) of 2016 requires the bank to provide the Financial Follow-up Unit with daily reports on all incoming or outgoing express remittances of a value equal to or exceeding USD 500 or the equivalent in other currencies, including all data related to the Remittance, whether it is conducted through the bank itself or by its banking or financial agents.
 - **Article 12** of AML/CFT Instructions No. (2) Of 2016 states that the bank shall provide the Financial Follow-up Unit with daily reports on the financial transactions carried out through it Including the parties to the financial transaction and their values according to the following:
 - All external electronic remittances incoming or outgoing from or to Palestine that are equal to or their value exceeds USD 5,000 or its equivalent in other currencies.
 - All internal electronic transfers between banks equal to or greater than the amount of USD 5,000 or its equivalent in other currencies.
 - All checks of any kind equal to or greater than USD 5000 or its equivalent to that of other currencies.
 - Deposits or withdrawals equal to or greater than USD 5,000 and its equivalent to that of other currencies.
 - Letter of credits and collection policies equivalent to or greater than USD 5,000 or its equivalent of that of other currencies, including transfers related to the execution of those credits.

5.9 Submission of the STR

On observing any suspicions customers transaction (as listed), or have doubt about a transaction, immediately notify the designated compliance officer in the Branch / Business Unit through the prescribed "**Internal STR template**" (use the enclosed template).

Do not indicate to the customer that the concerned transaction is subjective to a suspicious transaction. **DO NOT TIP OFF THE CUSTOMER.**

Discreetly obtain any additional information as and when escalated to the Compliance Department.

5.10 Procedure for Reporting

Step 1:

Filling up the STR by the Reporting Officer ('RO') and the collation of all relevant supporting documents log in the In-house STR excel sheet of the Branch/Unit;

Step 2:

Review of the STR by Branch Manager/Heads of Department to ensure that the STR is properly filled up and all relevant supporting documents collated and enclosed;

Step 3:

**STR to be sent AML/CFT Department & receive an acknowledgement;
Reference for future use and branch/Unit's records;**

Step 4:

Enlist in STR Log, Acknowledge receipt, Review of the STR by Compliance Department;

Step 5:

External ST Report preparation by MLRO - AML/CFT Department (a refer marker flag is placed on the account for ongoing monitoring).

Refer to the attached template "external STR report " to be submitted to the Financial Follow-up Unit of the AML/CFT committee of the PMA;

Step 6:

Submission of the STR by MLRO – AML/CFT Department to the Financial Follow-up Unit (FFU) of the AML/CFT committee.

Step 7:

Await the FFU to provide a response (acknowledgement/directive).

Step 8:

Notify the business of the FFU decision to the business to execute where applicable.

5.11 Filling up the STR

- All sections of the STR have to be filled in. If any section is not applicable, please state 'N/A'.
- Information to be provided under the heading "Brief Description of Customer's Relationship with Bank (Past & Present]"

Example:

The date the account(s) was opened

The purpose for which the account was opened

The name of the account-holders and whether the account was in joint- names

If the purpose is to receive company funds when the account is a personal account, the reason for such discrepancy

Any previous accounts which may have been closed and the dates they were closed.

The account profile: i.e. what are the normal transactions on the account and the average account balance?

Information to be provided under the heading "**Reasons for Suspicion**". The information should be set out in a chronological order.

All information which may be helpful in assisting the authorities in their investigations are relevant

What aroused the staff's suspicion (i.e. deviation from the standard operation of the account, forgery of documents etc.)?

State the actual reason for the suspicion

The date of any meetings which the staff had with the Customer

What was discussed?

What transaction(s) did the customer want to undertake?

Why did the customer want to undertake the transaction(s)?

Information to be provided under the heading **“Reasons Given By Customer for Transactions / On Making Further Enquiries”**

What questions did the staff ask the customer in relation to the transaction?

What was the customer’s response?

Did the customer display any emotion e.g. was the customer agitated, evasive etc?

Did the staff ask any further questions and what was the Customer’s response?

Information to be provided under the heading **“Other Relevant Information”**

- . Any company searches done if it is a corporate account or if the company is related to the account.
- . Any other related accounts? (In the case of an individual, check to see if he is an authorized signatory or director of any other corporate customer of the Bank).

5.12 Collation of Documents

The documents that should accompany an STR are as follows:

- All account opening forms
- All customer identification documents
- 6 months bank account statement showing the recent transactions on the account(s) etc.
- Documents evidencing the suspicious transaction(s).
- This would include all relevant correspondences, invoices, agreements etc if any.
- Other relevant documents such as company searches etc.

5.13 Duties of the Reporting branch/office manager

- Investigate the past history of customer’s account to determine whether the customer made the same kind of transactions previously;
- Obtain accurate evidences of the doubtful transactions to justify suspicions;
- Forward all relevant documents together with the detail of doubtful transaction to the AML/CFT Department officer and head of compliance.
- Keep the Branch Manager / Customer Service Manager informed of such suspicious transactions and course of follow-up with Compliance Department
- Keep custody of the following files:

File Number Purpose of file

- 1. To stay abreast of MLP & CTF Circulars, Regulations, Guidelines and Procedures;**
- 2. To keep daily reports after reviewing and initials;**
- 3. To keep records of cases under investigation & not yet reported to AML/CFT Department;**
- 4. To keep records of cases investigated and reported to AML/CFT Department;**
- 5. To keep PMA and AML/CFT committee templates formats that are filled in by customers (copy of this format should be maintained for review by the Compliance Department periodically).**

1) Customer Service Officer

Exercise caution and report to the Branch AML Compliance Officer where:

- a The customer is reluctant to provide complete information about the nature and purpose of its business, anticipated account activity, prior banking relationships, the names of its officers and directors, or information on its business location.
- b A customer's home or business telephone/mobile is disconnected and cannot be contacted.
- c The customer is reluctant to furnish identification when purchasing negotiable instruments in considerable amounts.
- d A customer is a trust, or Private Investment Company that is reluctant to provide information on controlling parties and underlying beneficiaries. It is strictly prohibited to have any relationship directly or indirectly with institutions that have no physical presence (Shell banks and Companies).

2) Branch/office Manager

Be aware of any of the following unusual account conduct of the customer;

- a Maintains a number of accounts or margin account that is not in agreement with the nature of business activities.
- b Maintains various accounts without any accepted reasons to deposit small amounts in each account to veil large cash deposit.
- c Maintains accounts with various banks in the same area and collects the balances in one consolidated account for further transfer.
- d Depositing endorsed cheques (third party Cheques) of significant amount when it does not seem to be relevant to the nature of account holder's business.
- e Activation of dormant account after a lapse of time.
- f Deposits being made to one account by a large number of depositors without an adequate explanation.
- g The customer's background differs from that which would be expected on the basis of his or her business activities.
- h A customer makes frequent or large transactions and has no record of past or present employment/ business experience.

3) Teller and Account Transactions

Teller / Customer Service Officer

Exercise caution when the following **cash transactions** take place at the counter:

- a. The customer uses unusual or suspicious identification documents that cannot be readily verified.
- b. A customer frequently exchanges small denominations for large denominations.
- c. Frequent deposit of currency wrapped in currency straps or currency wrapped in rubber bands that is disorganized and does not balance when counted.
- d. Unusual large cash deposit made by customer whose previous activities were usually conducted by negotiable instruments.
- e. Significant increase in cash deposit, without any justification.
- f. Splitting a large sum of money in small deposit, where the sum total reaches or exceeds the indicated amount of USD 5,000 or its equivalent.
- g. Business / Corporate entities transact in cash rather than negotiable instruments.
- h. Continuous deposit of cash to cover DD's, TT or other negotiable instruments.
- i. Transferring a significant amount of funds to or from outside the country with the instruction to pay cash.
- j. A person customarily uses the automated teller machine to make several bank deposits below a specified threshold.
- k. Customer accesses the safe deposit box frequently before making currency deposits structured at or just under USD 5,000, to evade the Transaction Reports.
- l. Depositing endorsed cheques (third party Cheques) of significant amount when it does not seem to be relevant to the nature of account holder business.
- m. Activation of dormant account after a lapse of time.
- n. Deposits being made to one account by a large number of depositors without an adequate explanation.

4) Funds Transfer Transactions

Teller / Customer Service Officer

Be vigilant in respect of **fund transfers** where;

- a. Funds transfer activity occurs to or from a financial secrecy haven, or to or from a high-risk country (ies) (as per list provided and updated by Head of Compliance) without an apparent business reason or when the activity is inconsistent with the customer's business or history.
- b. Many small, incoming transfers of funds are received, or deposits are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer's business or history.
- c. Large, incoming funds transfers are received on behalf of a foreign client, with little or no explicit reason.
- d. Funds transfer activity is unexplained, repetitive, or shows unusual patterns.
- e. Payments or receipts with no apparent links to legitimate contracts, goods, or services are received.
- f. Funds transfers are sent or received from the same person to or from different accounts.

- g. Funds transfers contain limited content and lack related party information.
- h. A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves high-risk countries.
- i. Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- j. Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
- k. Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- l. Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to high-risk countries.
- m. Movements of funds from one bank to another and then funds are moved back to the account.

5) Finance Facilities

Consumer Finance Service Officer

Exercise caution and report to the AML Officer where following conduct is observed in the finance facility;

- a. Repeated early payment of loans unexpectedly.
- b. Loan requisitions guaranteed by third party assets, where the origins of such assets are unknown.
- c. Loan transactions secured by deposit held in high risk countries.

6) Trade Finance Transactions

Trade Finance Officer

Look into the following Trade Finance methods which may possibly implicate money laundering transactions and report to the AML Officer;

- a. The exported or imported merchandise is not suitable for the customer's activity.
- b. The customer has opened one or more letter of credits in a manner that is not commensurate with the customer's activity.
- c. The customer changes the beneficiary's name shortly before the payment process or changes the place of payment to countries other than the recipient's country.
- d. The difference between the value of the goods shown in the letter of credit and the value of the real goods.
- e. Goods are received in the name of a non-issuing party.
- f. The financial guarantee submitted for approval is not appropriate with the size of the customer's financial activity and the date of his dealings with the company.
- g. The existence of payment terms in favor of external parties that have no clear relationship with the letter of credit.
- h. Mismatch of the amounts stated in the letter of credit document presented by the client with the original documents.

- i The beneficiary must be from the letter of credit of a company owned by the customer.
- j The shipping company must be owned by the same customer.
- k None existence of the shipping agent in Palestine. (Documents should be checked on selective and regular basis with the competent authorities).
- l Sudden and unexplained increases in a customer's normal trade transactions.
- m Customers are conducting business in high-risk countries and/or shipping goods through high-risk countries.
- n Customers involved in potentially high-risk activities (e.g. dealers in weapons, nuclear materials, chemicals, real estate, precious gems; antique dealers, Auction Houses, Jewelers, Exchange houses, traders in certain natural resources such as metals, etc).
- o Obvious over pricing or underpricing of goods and services.
- p Transactions evidently designed to evade legal restrictions, including evasion of necessary government licensing requirements.

7) Other Customer Activities

Customer Service Officer

1. Pay due diligence to the following investment related transactions done by the customer and report to the AML Officer:
 - a. Purchase and lodgment of securities in the bank at a time that seems unreasonable with customer's position.
 - b. Back to back loans/deposits with subsidiaries or affiliates of financial establishments working in and located at areas notorious for money laundering or drug trafficking.
 - c. Buying and selling of big quantities of foreign currencies /securities in cash inconsistent with the income of the customer.
 - d. Buying and selling of securities which purposes is not clear or where done in unusual circumstances.
 - e. Using financial advisors or intermediaries where the actual investor is unknown.
 - f. Account to be of a dummy / shell company with delays in their audit & financial statements or does not publish their accounts at all.
2. Look into the following International Banking & Financial Transaction which may implicate money laundering transactions;
 - a. Introduction of a customer to the bank through external organizations, which are working in or located at areas notorious for money laundering or drug trafficking
 - b. Having a large balance in customer's account or movements far exceeding a company's normal sales that are subsequently transferred to account(s) maintained outside the country, especially in the areas that enforce strict banking secrecy laws.
 - c. Regular and recurring, paying or buying and selling of traveler's Cheques or issuance of drafts or banker's Cheques in large amounts.
3. When the customer uses electronic channels to conduct banking transactions, be mindful of the following transactions:
 - a. Deposit/s of number of small fund transfers via Swift, Telex and/or any other electronic methods, whereby the consolidated large balance/s is transferred to another country.

- b. Regular and large deposits using electronic payments that are identified as bonafide transactions received from notorious money laundering areas.
 - c. Inward payment orders received from outside the country and instructed to be transferred abroad without touching the customer accounts (such transfers must be reflected in the account statement prior to re-routing).
 - d. Increased usage of the ATM and other cash deposit machines.
4. Where the activity is inconsistent with that of their business;
- a. The currency transaction patterns of a business show a sudden change inconsistent with normal activities:
 - b. A large volume of cashier's checks, money orders, or funds transfers is deposited into, or purchased through, an account when the nature of the account holder's business would not appear to justify such activity.
 - c. A retail business has dramatically different patterns of currency deposits from similar businesses in the same general location.
 - d. Unusual transfers of funds occur among related accounts or among accounts that involve the same or related principals.
 - e. Goods or services purchased by the business do not match the customer's stated line of business.
5. Other Suspicious Customer Activities to be looked into are:
- a. Deposits are structured through multiple branches of the same bank or by groups of people who enter a single branch at the same time.
 - b. Currency is deposited in amounts just below identification or reporting thresholds.
 - c. Visit to the safe deposit box or use of safe custody account on an unusually frequent basis.
 - d. Safe deposit boxes or safe custody accounts opened by individuals who do not reside or work in the institution's service area despite the availability of such services at a branch closer to them.
 - e. Unusual traffic patterns in the safe deposit box area or unusual use of safe custody accounts, where more individuals enter/ frequently enter/ carry bags or other containers that could conceal large amounts of currency, monetary instruments, or small valuable items.
 - f. Rental of multiple safe deposit boxes (where the aggregate size is bigger than (70cmX70cmX70cm)).

8) Function of the MLRO Head of the AML/CFT department

- a. AML/CFT Department will receive and review any reports of suspicious activity from Branches/ Business Units.
- b. Analyze the facts presented through the documents and perform an individual evaluation of the customer account and collect additional information through the branch if required.
- c. On failure to obtain satisfactory clarification, determine whether the suspicious activity warrants reporting to Financial Follow-up Unit.
- d. AML/CFT Department are required to investigate the background and purpose of transactions deemed to be 'unusual' and to set forth their findings in writing, even in the event, it is not considered necessary to report the transaction to the FFU as suspicious. As in the case of other documents these findings should also be maintained for inspection by the competent authorities for a period of at least 10 years.
- e. The AML/CFT Department will be responsible for maintaining records of all STRs reported to them and any action taken by them, including reason for reporting or not to the external regulator or the relevant authorities.

- f. The AML/CFT Department shall formalize an Annual Report covering the MLP & CTF policies, procedures, systems and controls and when necessary make appropriate recommendations for improvement in the ongoing management of the firm's AML/CFT risks.

All Staff should ensure strict confidentiality and do not let the customer be aware of any suspicion/s being made by customer or transactions on the account.

5.14 Internal STR template

Date: STR Ref Nr.	No of Pages: 2 (including this page)
--	---

REPORTING OFFICER

Name _____ Tel _____ Fax _____
 Position _____ Branch/Dept _____





CUSTOMER/CLIENT DETAILS AND BACKGROUND

Customer Name _____ ID/Passport No. _____
 Nationality _____ Address _____
 Telephone No _____ Occupation _____
 Employer's Name _____ Local Address _____
 _____ /Tel No _____

Existing Accounts (Nos)	Type of Accounts	Credit Balance	Date	Date Account Opened

BRIEF **DESCRIPTION** OF CUSTOMER'S RELATIONSHIP WITH BANK (PRESENT AND PAST) CONSUMER BANKING RELATIONSHIP

NATURE OF TRANSACTION

-  Reactivated dormant account
-  Large/unusual cash deposits/withdrawals
-  Activity inconsistent with customer
-  Regular/unusual off-shore activity

DETAILS OF TRANSACTIONS A	ROUSING SUSPICION	N
Amount (Dr/Cr)/Value date	Account No(S)	Details of Remitting Bank(incoming funds)/ Destination (outgoing funds)
REASONS FOR SUSPICION		
Review of account statements shows no major activity other than deposit of cash in round sums and from their to immediate Telex Transfers. Appears individual account being used for business purpose.		
REASONS GIVEN BY CUSTOMER FOR TRANSACTIONS/ON MAKING FURTHER ENQUIRIES		
OTHER RELEVANT INFORMATION-		
<u>IMPORTANT:</u> Please attach copies of (1) <u>Account opening form</u> , (2) <u>Recent account history</u> (3) <u>Suspicious transaction documents</u> AND (4) <u>Customer identification documents</u> .		
NOTE: You should not inform customer/client of your suspicion and report.		
REPORTER'S SIGNATURE		

6. Sanctions / Boycott Law

7.1 Background

Economic sanctions are measures designed to deprive a sanctions target of its financial and economic assets and to deny the sanctions target the benefits of trade or economic interaction with the country or countries imposing or implementing sanctions. They are also designed to counteract and attempt to curtail behavior that threatens national or international security or contravenes international law. Sanctions may be multilateral (i.e. mandated by the United Nations or other similar organizations) or unilateral (e.g. the US, UK or EU against a specific target).

The National Bank fully complies with Palestine laws and PMA regulations related to sanctions and embargoes restricting individuals, corporations and, in some cases, foreign subsidiaries from doing business with countries, groups and individuals associated with terrorist activity, narcotics trafficking and illegal activities. The United States of America imposes economic sanctions upon certain countries, governments, entities, individuals and groups in order to further foreign policy goals and national security of the USA. These sanctions may be upon economic, trade, or may apply to assets held in the USA.

In the US, the Office of Foreign Assets Control (OFAC) of the US Department of Treasury is responsible for the administration of sanctions, which are actively and strictly enforced. Penalties imposed can be severe including imprisonment and fine for each violation for individuals and corporations.

The United Kingdom and European Union also impose similar sanctions.

Under the Palestine law, The National Bank will comply with all the United Nations mandated Sanctions. The Head of Compliance & Operational Risk will advise through the Sanction Policies & Procedures and in periodic bulletins the sanctions that impact The National Bank.

Boycott Laws: The Bank shall follow boycott laws and other similar acts under PMA laws as applicable, that prohibit taking actions or entering into agreements that support the boycotted countries or specific territories.

7.2 The National Bank Policy

Where applicable, the Bank's policy is to strictly comply with the prohibitions, restrictions and blocking/freezing local listing requirements, in particular of UN, US or others.

The degree and nature of restrictions, and of exceptions and exemptions to the restrictions, differs widely between different countries. It is therefore essential for the Bank to carefully consider whether the sanctions will affect a particular transaction and to obtain full details of the proposed transaction before entering into the transaction. Breaches of sanctions may result in customer funds being impounded, and fines being imposed on the Bank and its employees.

The Bank Sanctions Policy and supplements thereto can be found in Section 22.5 of this Chapter. Frequent checks and follow ups with the AML/CFT and compliance departments in addition to the Legal Department for any revisions or additions to the Policy shall be made.

7.3 Dealings with Sanctions Targets

In case any of our branches have customers who deal with countries which are the subject of UN, US or other sanctions. In these circumstances, it is imperative that appropriate advice is taken in respect of transactions, particularly where there may be doubts as to whether the transaction can be processed.

7.4 Sanctions Policy

The National Bank Economic Sanctions Policy & Procedures

Scope

This policy & procedures and any supplement to it apply to The National Bank, all its branches and subsidiaries, within Palestine.

1. Introduction

Economic sanctions are measures designed to deprive a sanctions target of its financial and economic assets and to deny the sanctions target the benefits of trade or economic interaction with the country or countries imposing or implementing sanctions. Sanctions are also designed to counteract and attempt to curtail behaviors that threaten national or international security or contravene international laws. Sanctions may be multilateral (i.e. mandated by the United Nations or other similar organizations) or unilateral (e.g. the US, UK or EU against specific targets).

Failure to comply with sanctions can have serious consequences for the Bank and/or its staff. These may range from censure to fines and/or imprisonment, all of which have the potential to cause reputational and regulatory damage.

2. The Banks Policy

The National Bank branches and subsidiaries will comply with Palestine laws and PMA regulations related to sanctions and embargoes restricting individuals, corporations and, in some cases, foreign subsidiaries from doing business with countries, groups and individuals associated with terrorist activity, narcotics trafficking and illegal activities.

Each Branch/ office shall comply with all sanctions that are legally binding on The Bank office and shall maintain controls designed to ensure compliance with such sanctions and with this policy. Even where UK / EU, US or other countries sanctions are not expressed to be legally binding on The bank and its branches and offices (e.g. incorporated outside the UK or US), doing business with sanctioned parties such as suspected terrorists presents significant money laundering and reputational risk. For example, dealing outside the US with parties and/or countries designated under US sanctions could have serious consequences to The National Bank due to its relationship with US correspondent banks. More broadly, The National Bank will seek to identify and avoid transactions that would expose it and any of the transaction participants, including our customers, employees and counterparties, to compliance risk due to sanctions, including transaction(s) that would either directly or indirectly involve or benefit any sanctions target, irrespective of the currency.

3. Definitions

3.1. Economic sanctions

These are measures imposed by United Nations and other governmental authorities designed to deprive a sanctions target of its financial and economic assets and/or to deny the sanctions target the benefits of trade or economic interaction with the country or countries imposing or implementing sanctions.

3.2. UN sanctions

These are economic sanctions imposed by, or that create binding and directly applicable obligations on the member countries of the United Nations. See [Appendix 1](#) for a further summary.

3.3. EU sanctions

These are economic sanctions imposed by, or binding in member states of the European Union. See [Appendix 1](#) for a further summary.

3.4. US sanctions

These are economic sanctions imposed by the United States. See [Appendix 1](#) for a summary.

3.5. Boycott of Israeli Settlements

This is a mandatory boycott applicable to all Israeli settlements established on Palestinian land on or after the year of 1967.

3.6. Local sanctions

These are legally effective sanctions imposed by the governmental authorities of a country in which The National Bank HQ, Branches and offices is located, the PMA Local Sanctions list is attached in See [Appendix 1](#) for a summary.

4. The National Bank Adherence to international Sanctions

4.1. UN Sanctions

The National Bank, its branches and subsidiaries will comply with sanctions and embargoes mandated by the United Nations:

- a. Designed to counteract and attempt to curtail behaviors that threaten national or international security or contravene international laws.
- b. Restricting individuals, corporations and, in some cases, foreign subsidiaries from doing business with countries, groups and individuals associated with terrorist activity, narcotics trafficking and illegal activities.

4.2. US Sanctions

The US Treasury Department's Office of Foreign Assets Control ("**OFAC**") administers and enforces laws and regulations that impose economic and trade sanctions based on US law enforcement, foreign policy and national security goals. For certain target countries, presently including Cuba, Iran, and Sudan, OFAC's prohibitions extend to essentially all unlicensed economic or trade contact with the country, its government, and associated OFAC sanctions targets.

In addition, at present, most financial transactions with and investment in Burma (Myanmar) are prohibited as are transactions involving the Government of Libya. Along with these comprehensive sanctions, OFAC also maintains lists of individuals and entities designated as Specially Designated Nationals ("**SDNs**") with whom transactions are prohibited. The National Bank, branches and subsidiaries must not engage in transactions that breach the OFAC sanctions in any manner or that would cause a US correspondent bank or other US counterparty to be in a breach of an OFAC sanction.

The National Bank Staff - US citizens and Resident Aliens and all Persons in the US:

The National Bank, branches and subsidiaries' staff who are US citizens and US resident aliens employed by or working for The Bank or its subsidiaries wherever located shall comply with OFAC sanctions, as shall all The Bank personnel when visiting the United States. OFAC sanctions prohibit any US person from approving, assisting, financing, or facilitating any transaction entered into by a third party (for example, a non-US office or branch) if the applicable sanctions prohibit a US person from engaging directly in such a transaction. US person employees therefore are exempted and barred from approving, assisting, financing, or facilitating any transaction entered by a third party that OFAC sanctions would prohibit US persons from directly undertaking. Non-US bank offices and branches must not involve US person employees or any US counterparty or the US financial system in any such transaction.

a) New Business

The National Bank, branches and subsidiaries shall not open an account for, enter into any business relationship with, or knowingly process a transaction related to any SDN or other target of OFAC sanctions, including terrorist, narcotics, or proliferation of weapons of mass destruction SDNs or any other party known by The Bank to be the subject of an OFAC sanction. Providing support to SDNs could expose The Bank to legal and reputational censure.

Apart from avoidance of transactions with SDNs, The National Bank, branches and subsidiaries also shall endeavor to comply with the OFAC sanctions directed to sanctioned countries to the extent that The National Bank can legally do so under applicable local law.

In any event, The National Bank, branches and subsidiaries shall not involve US persons, the US financial system or any US-origin goods in any transactions involving an OFAC sanctioned country or other target of OFAC sanctions unless the OFAC regulations would permit the direct involvement of US persons in such transactions.

b) Existing Business

Where any The National Bank, branches and subsidiaries has an account for, or business relationship with, a person, entity or organization ("**Person**") that The Bank identifies as a target of OFAC sanctions, , immediately it is noticed, the respective office shall submit details of the case to the Head of the AML/CFT department , who will submit the case to the Executive Operational Risk Committee, which will review the risks and decide on the appropriateness of continuing with the account or other relationship and also on the external reporting, where applicable. Immediate action must also be taken upon identification of The National Bank's exposure to such Person to prevent any account activity or other transaction by or through the bank on behalf of that Person involving the US financial system, US persons or other prohibited US elements.

4.3. EU (and UK) Sanctions

EU sanctions are imposed principally in order to implement UN Security Council resolutions (which are generally implemented by many other countries) as well as EU foreign policy objectives. In the UK, they are administered by HM Treasury. EU sanctions do not apply to The National Bank entities and branches that are incorporated or operating outside of the EU.

Staff – citizens and nationals of EU Member States:

EU sanctions are applicable to all EU persons. Citizens and nationals of EU Member States (including the UK) employed by The National Bank, branches and subsidiaries, wherever located shall comply with EU sanctions requirements. They are exempted and barred from approving, assisting, financing, or facilitating any transaction entered into by a third party where it would be prohibited for them to do so under applicable EU sanctions laws and regulations.

4.4. Local Sanctions in Countries Where The National Bank, Branches and Subsidiaries are Located

In the case of sanctions imposed by governmental entities in countries where The National Bank, subsidiaries and branches operate, other than the UN, EU, US or other foreign country (“**Local Sanctions**”), The National Bank, branches and subsidiaries bound by such sanctions shall comply with them, in the case where a bank foreign subsidiary and any other entity related to The National Bank not bound by them, they shall consider the risks of conducting business involving the relevant Person, entity or country, before commencing or continuing business with the sanctioned entities / parties.

4.5. Boycott of Israeli Settlements

Article 3 of Instructions No (2) for the year 2018 issued by the AML/CFT committee of the PMA clearly prohibits any transaction of any sort whatsoever with the Israeli settlements established on the Palestinian land on or after the year 1967. Accordingly TNB must not conduct any transaction with financial institutions or its branches or offices which are established in the Israeli settlements.

5. Procedures within The National Bank

5.1. Account Opening

a. UN, US, EU, UK & other countries’ Sanctions operate principally at two levels:

1. Sanctions against SDNs under US Sanctions or against other listed sanctions targets under EU or other country sanctions programs
 2. Sanctions against countries and governments
- b. In The National Bank, the filtering of the sanctioned names and countries is done at:
1. Account Opening – through **Dow Jones** watch lists and internal lists;
 2. Periodic matching of The National Bank client database against the sanctioned individuals and entities;
 3. SWIFT remittances, both inward and outward are filtered through the Financial Crime Management system (FCM) watch lists;
 4. Trade Services – All entities and geographic references in Trade Transaction documents should be screened against the FCM system. Any matching names or references to any sanctioned countries and entities should be referred to AML/CFT department for further guidance.

All perfect positive matches against the FCM watch lists will be rejected. Any match that is not a perfect positive but that potentially represents a true hit will be referred to Compliance for vetting before a final decision is taken.

5.2. Periodic Matching of TNB’s Client Database against international Watch Lists

Each Branch/ office of The National Bank shall run the periodic matching of its customer database against the Dow Jones watch lists (OFAC/UN/US/EU and French lists), on the incremental names as well as the whole database at frequencies prescribed in the AML manual.

Where any of The National Bank, branches and subsidiaries has an account for, or a business relationship with, a Person that it identifies as a target of OFAC sanctions, at the time it comes to the knowledge of The National Bank, the respective office shall submit details of the case to the Head of AML/CFT Departments, who will submit the case to the Compliance Committee (Head of Compliance, Legal Counsel, Chief Risk Officer, CEO & the respective Business Head) , which will review the risks and decide on the appropriateness of continuing the account or other relationship. Immediate action must also be taken upon identification of the exposure to such Person to prevent any account activity or other transaction by or through The Bank on behalf of that Person involving the US financial system, US persons or other prohibited US elements.

The cases will be presented to the Compliance Committee in a paper with the customer details, details of the sanctions being breached, the risk / implication to The Bank and recommendations. The committee will give its verdict and the paper updated and signed by the Head of Compliance and AML/CFT departments and the CEO.

5.3. Filtering of SWIFT Remittances - Inward and Outward

All incoming and outgoing SWIFT messages will be filtered against the Dow Jones Watch Lists. The National Bank will reject or block any transactions as necessary and appropriate that it determines to implicate a prohibition under applicable sanctions laws or regulations or this Policy. The National Bank employees must never seek to circumvent sanctions requirements or assist customers to do so by removing information relevant to sanctions compliance from SWIFT messages or other transaction documents. Any effort by a customer to circumvent sanctions must be reported immediately to the Head of AML/CFT departments.

5.4. Filtering of Parties in Trade Related Instruments

The parties being favored in Letters of Credit and Guarantees, and relevant geographic references should be filtered against the Dow Jones watch list, similar to the account opening process. Any potential true matches should be escalated to the Head of AML/CFT Departments for a decision. Guarantees and Letters of Credit originating from The National Bank should be physically examined to ensure that none of the parties to them are for or in favor of Israeli settlement or the addresses or incorporation of the entities, party to the instruments are not incorporated in Israeli settlements. Business with Israeli settlements and related Israeli entities should be declined, in line with the Boycott requirements.

6. Responsibilities

- 6.1 This policy is owned by the Head of AML/CFT Departments.
- 6.2 The Head of AML/CFT department may mandate that The National Bank will not engage in certain categories of transactions even where the type of transaction concerned may not be in breach of sanctions requirements.
- 6.3 Head of the AML/CFT Departments and Subsidiary Risk Managers are responsible for coordination of sanctions advice to the businesses in their respective countries, with the Head of AML/CFT Department. The Head of AML/CFT department will guide offices/branches on significant points of principle.
- 6.4 All employees are responsible for compliance with this Policy. Any sanctions breach which comes to the attention of any employee shall immediately be reported to their Head AML/CFT department / Subsidiary Risk Manager and escalated to the Head of AML/CFT department.

7. Dispensation

Dispensation for any aspect of this policy should be channeled to the Head of AML/CFT, through Heads of business for each branch/office and Subsidiary Risk Manager, subject to the endorsement of the respective Branch/office / Subsidiary heads.

7.5 Appendix 1: Summary of Sanctions

Certain major jurisdictions in which (or using whose currencies) The National Bank or its clients engage in business, including the United States, European Union ("EU") and United Kingdom, apply economic sanctions laws and regulations, including lists of blocked persons, entities and other targets with whom it is illegal to conduct business and/or for whom transactions must be blocked and relationships reported to the appropriate authorities. In addition, Export Control Measures prohibit unauthorized or unlicensed exports, transfers and sales of certain specified commodities, technology and technical data to certain countries, companies and individuals,

as well as (in some cases) re-exports from one third country to another.

Below is a summary of some of the principal such laws and regulations applicable to transactions that might involve The National Bank. In addition to those described below, other sanctions laws and regulations may apply, depending on the jurisdiction(s) in which The National Bank and its clients are operating.

a. United Nations (UN)

The United Nations (UN) Security Council has the authority to call for the imposition of economic sanctions by UN members against governments, persons and entities that have attracted UN censure. As a UN member, The AML/CFT committee of the Palestinian Monetary Authority (PMA) generally aligns its sanctions policies with the decisions of the UN Security Council. This alignment is enacted in regulation by virtue of circulars issued by the PMA.

Among other targets of UN sanctions, the UN Security Council has issued a series of resolutions directed against nuclear proliferation and other illicit activity by certain Iranian entities. The AML/CFT Department of the PMA is referencing the UN Council site as part of its circulars in this regard. Details of the requirements of these circulars and any other similar circulars issued by PMA from time to time are available on its website at <http://www.pma.ps/Default.aspx?tabid=854&language=en-US>.

b. US Economic Sanctions

The US Treasury Department's Office of Foreign Assets Control ("OFAC") administers and enforces laws and regulations that impose economic and trade sanctions based on US law enforcement, foreign policy and national security goals. For certain target countries, OFAC's prohibitions extend to essentially all unlicensed economic or trade contact with the country, its government, and associated OFAC sanctions targets.

Along with these comprehensive sanctions, OFAC also maintains lists of individuals and entities designated as Specially Designated Nationals ("SDNs") with whom transactions are prohibited. The list of SDNs includes, for example, Specially Designated Narcotics Traffickers and Trafficking Kingpins, Specially Designated Terrorists, Specially Designated Global Terrorists, and Foreign Terrorist Organizations and SDNs listed for purposes of Non Proliferation of Weapons of Mass Destruction.

OFAC continuously updates its designations of Sanctions Targets in response to US law enforcement, foreign policy and national security objectives. Summaries of the OFAC sanctions programmes and related programme information are available at OFAC's website: <https://www.treasury.gov/resource-center/sanctions/programs/pages/programs.aspx>.

1. *Given the complexity of the different Sanctions rules, employees must not attempt to interpret or apply any of the relevant laws or regulations to a contemplated transaction without first consulting with and obtaining guidance from the Head of the AML/CFT and Compliance Departments.*

c. CISADA/IFSR

On May 2, 2011, the US Treasury Department ("US Treasury") published a proposal for implementing the US correspondent account provision of the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 ("CISADA"). The proposal would substantially increase US Treasury's extraterritorial ability to access and respond to information regarding the Iran-related activity of non-US banks that maintain US correspondent accounts.

Under the proposal, US Treasury can direct US banks to request certifications ("Certifications") from specified non-US banks for which they maintain correspondent accounts. In response to a Certification request, the non-US bank would have to indicate whether it:

- (i) Maintains any correspondent accounts in any currency with Iranian-linked financial institutions designated by OFAC under its counter-proliferation and anti-terrorism sanctions (i.e., financial institutions designated under OFAC's Iranian Financial Sanctions Regulations or "IFSR");
- (ii) Processed any funds transfers in any currency within the preceding 90 calendar days related to an IFSR designated

financial institution, whether or not such funds transfer involved a correspondent account;

- (iii) Processed any transfers of funds in any currency within the preceding 90 calendar days related to a person or entity designated by OFAC as linked to Iran's Islamic Revolutionary Guard Corps ("IRGC").

The disclosure / refusal to disclose incriminating information in response to a Certification request could result in the US correspondent bank restricting or terminating a correspondent account relationship with a non-US bank, or filing a suspicious activity report, based on the US bank's risk-based assessment of the facts and bank policy. In this context, OFAC could also impose sanctions against the non-US bank under the IFSR. Further, any non-US bank that intentionally submits misleading or incorrect information to their US correspondent banks for onward transmission to US Treasury risks liability under US criminal law.

The National Bank, branches and subsidiaries must not engage in transactions that breach the US sanctions as above in any manner or that would cause a US correspondent bank or other US counterparty to be in a breach of a US sanction.

d. European Union (EU) Economic Sanctions

The EU applies sanctions and restrictive measures to third countries, entities and individuals in pursuit of its Common Foreign and Security Policy. EU sanctions comprise measures that both implement binding UN Security Council Regulations across the EU, and which give effect to autonomous EU actions (i.e., that go beyond the scope of UN resolutions).

EU Regulations imposing and/or implementing economic sanctions are directly applicable in and have direct effect in all EU Member States. The measures apply to all nationals of EU Member States and entities incorporated or constituted under the law of an EU Member State, as well as all persons and entities doing business in the EU, including nationals of non-EU countries.

The application, enforcement and setting of penalties with respect to EU sanctions is the responsibility of the competent authority in each EU Member State. In the UK, this is achieved through a series of statutory instruments, and responsibility for administration and enforcement rests with HM Treasury. The UK also adopts its own autonomous sanctions, which are administered by HM Treasury. HM Treasury publishes a consolidated list of financial sanctions targets listed by the United Nations, the European Union and the UK. This list includes all individuals and entities noted on current EU and UK sanctions lists, and is available online: http://www.hm-treasury.gov.uk/fin_sanctions_index.htm².

2. United Kingdom (UK) HMT list

In general terms, it is a criminal offence to make any funds, "economic resources" or, in some circumstances, financial (or related) services available directly or indirectly to or for the benefit of designated sanctions targets (as listed by HM Treasury). The term "economic resources" is defined widely, and includes assets of every kind which can be used to obtain funds, goods or services.

In addition to the prohibition against making funds and economic resources available to listed targets, there are related EU (and UK) arms and other export embargos imposed against certain countries and an investment bank in relation to entities and/or economic sectors in certain jurisdictions.

e. PMA Local listing of Sanctions and Local Freezing lists

The Palestinian Monetary Authority (PMA) and its legally formulated committees and units has the authority to call for the imposition of economic sanctions against governments, persons and entities that have attracted Palestinian/international censure. As a UN member, Palestine generally aligns its sanctions policies with the

decisions of the UN Security Council. This alignment is enacted in regulation by virtue of circulars issued by the AML/CFT Committee of the PMA.

Among other targets of UN sanctions, the UN Security Council has issued a series of resolutions directed against nuclear proliferation and other illicit activity by certain countries. The Decisions circulated by the Financial Follow-up Unit (FFU) of the Palestinian Monetary Authority and has issued certain in this regard. Details of the requirements of these circulars and any other similar circulars issued by (FFU) from time to time are available with the Compliance and AML/CFT departments of The National Bank.

The National Bank shall also comply with the local freezing list issued by The AML/CFT committee of the PMA, the current freezing list is attached as an annex below.

This list shall be periodically updated by the AML/CFT department of the bank to ensure an up to date.

Current Local freezing list of the Palestinian AML/CFT committee of the PMA

December 2019 Source: <http://www.pma.ps/Default.aspx?tabid=866&language=en-US>

Economic Sanctions Policy & Procedures

Supplement 1: The National Bank Staff Who Are US Persons

1. Policy

Staff of The National Bank, branches and subsidiaries, who are US citizens and US resident aliens employed by or working for The Bank wherever located shall comply with OFAC (Office of Foreign Assets Control) sanctions, as shall all personnel when visiting the US. OFAC sanctions prohibit any US person from approving, assisting, financing, or facilitating any transaction entered into by a third party (for example, a non-US office/branch) if the applicable sanctions prohibit a US person from engaging directly in such a transaction. US person employees therefore are exempted and barred from approving, assisting, financing, or facilitating any transaction entered into by a third party that OFAC sanctions would prohibit US persons from directly undertaking. Branches/ offices must not involve US citizens and US resident alien employees or any US counterparty or the US financial system in any such transaction.

2. Definition

US Citizens and Resident Aliens and all Persons in the US are defined as:

- a. Any person present (permanently or temporarily) in the United States who works for any of The National Bank, branch or subsidiary.
- b. Any person who works for The National Bank, branch or subsidiary office and holds US nationality (including dual nationality) or a US resident alien 'green' card.

3. Adoption of the Policy

The following rules apply to staff of The National Bank, branches and subsidiaries who are US Citizens and Resident Aliens and all Persons in the US:

- a. They must not make, advise on, support, endorse, authorize or facilitate any decision or recommendation relating to an OFAC sanctioned activity or participate in any discussion, analysis or planning that involves an OFAC sanctioned activity.
- b. They must not carry out any processing or administrative function in relation to the OFAC sanctioned activity.
- c. They must not refer any OFAC sanctioned activity to a US or non-US person.
- d. Written communications relating to an Affected Activity must not be addressed or copied to any U.S. Staff.

4. Prohibition on US Citizens and Resident Aliens staff involvement in OFAC Sanctioned Activity

- 4.1. Where staff of The National Bank, branches and subsidiaries who are US Citizens or Resident Aliens would be required to make, advise on, support, endorse, authorize or facilitate any decision or recommendation relating to an OFAC sanctioned activity, or participate in any discussion, analysis, or planning that involves an OFAC sanctioned activity, he or she should immediately **abstain** and inform his or her direct manager of the reason for abstaining.
- 4.2. Where a US Citizen or Resident Alien staff member is a member of a committee that may make, advise on, support, endorse, authorize, or facilitate any decision or recommendation relating to an OFAC sanctioned

activity or participate in any discussion, analysis, or planning that involves any OFAC sanctioned activity, he or she should abstain from participating in any of the above activities as well as voting at the meeting. Where the US Citizens and Resident Aliens staff member is physically present at the meeting he or she should leave the room. Where the US Citizens and Resident Aliens staff is attending by video link he or she should leave the room when it comes to the discussion of the OFAC sanctioned activity. The minutes of any meeting that deals with the OFAC sanctioned activity should record that the US Citizens and Resident Aliens staff has abstained and absented himself or herself for the duration of the discussion and vote.

- 4.3. Where a US Citizens or Resident Aliens staff has a management responsibility for a division, department, or unit whose responsibilities may include an OFAC sanctioned activity:
 - a. All responsibilities related to an OFAC sanctioned activity shall be performed by other members of such division, department, or unit that are not US Citizens or Resident Alien staff;
 - b. Subordinates of US Citizens or Resident Alien who deal with an OFAC sanctioned activity shall report to and take directions in relation to the OFAC sanctioned activity from the next senior person in the reporting line above the US Citizen or Resident Alien staff, that is not a US Citizen or Resident Alien staff (or from such other non-US Person Staff member as such next senior person shall appoint);
 - c. In setting objectives to the subordinates, US Citizen or Resident Alien staff shall not include any objective that relates specifically to an OFAC sanctioned activities, **but may take** into account retro-respect performance of subordinates that are not US Citizen or Resident Alien staff in relation to OFAC sanctioned activities in conducting performance reviews.
- 4.4. Written communications relating to any OFAC sanctioned activities should not be addressed or copied to any US Citizen or Resident Alien staff.

5. Prohibition on Referring OFAC Sanctioned Activity to Any Non- US Citizen or Resident Alien Staff

If a US Citizen or Resident Alien staff receives any communication concerning an OFAC sanctioned activity, he or she must not direct the communication, its subject matter or the person making the communication to any other person, but should inform the next senior person in the reporting line above him or her that is not a US Citizen or Resident Alien staff member of the communication, without making any recommendation or qualitative comment regarding the communication.

6. Dispensations

Dispensations may be granted to staff of The National Bank, branches and subsidiaries who are US Citizens and Resident Aliens in relation to certain US sanctioned countries subject to the written approval of the Compliance Risk Committee.

The Head of Compliance will maintain a record of dispensations and copies of written approvals of any such dispensations.

Economic Sanctions Policy & Procedures

Supplement 2: The National Bank Staff Who Are EU Persons

1. Policy

Staff of The National Bank, branches and subsidiaries, who are EU Person employed by or working for The National Bank wherever located shall comply with EU sanctions, as shall all The Bank personnel when visiting the EU member countries. EU sanctions prohibit any EU person from approving, assisting, financing, or facilitating any transaction entered into by a third party (for example, a non-EU office / branch) if the applicable sanctions prohibit an EU Person from engaging directly in such a transaction. EU Person employees therefore are exempted and barred from approving, assisting, financing, or facilitating any transaction entered into by a third party that EU sanctions would prohibit EU persons from directly undertaking. The Bank branches/ offices must not involve EU Person employees or any EU counterparty or the EU financial system in any such transaction.

2. Definition

EU Person is defined as:

- a. any person within the territory of the European Union;
- b. any person inside or outside the territory of the Union who is a national of a Member State;
- c. Any legal person, entity or body which is incorporated or constituted under the law of an EU Member State;
- d. Any legal person, entity or body in respect of any business done in whole or in part within the EU.

3. Adoption of the Policy

The following rules apply to staff of The National Bank, branches and subsidiaries who are EU Persons:

- a. They must not make, advise on, support, endorse, authorize or facilitate any decision or recommendation relating to an EU sanctioned activity or participate in any discussion, analysis or planning that involves an EU sanctioned activity.
- b. They must not carry out any processing or administrative function in relation to an EU sanctioned activity.
- c. They must not refer any EU sanctioned activity to a non-EU Person.
- d. Written communications relating to a sanctioned activity must not be addressed or copied to any EU Person.

4. Prohibition on EU Persons staff involvement in EU Sanctioned Activity

- 1.1 Where staff of The National Bank, branches and subsidiaries who are EU Persons would be required to make, advise on, support, endorse, authorize or facilitate any decision or recommendation relating to an EU sanctioned activity, or participate in any discussion, analysis, or planning that involves an EU sanctioned activity, he or she should immediately **abstain** and inform his or her direct manager of the reason for abstaining
- 1.2 Where an EU Person staff member is a member of a committee that may make, advise on, support, endorse, authorize, or facilitate any decision or recommendation relating to an EU sanctioned activity or participate in any discussion, analysis, or planning that involves any EU sanctioned activity, he or she should abstain from participating in any of the above activities as well as voting at the meeting. Where the EU Person staff member is physically present at the meeting he or she should leave the room. Where the EU Person staff is attending by

video link he or she should leave the room when it comes to the discussion of the EU sanctioned activity. The minutes of any meeting that deals with the EU sanctioned activity should record that the EU Person staff has abstained and absented himself or herself for the duration of the discussion and vote.

- 1.3 Where an EU Person staff has a management responsibility for a division, department, or unit whose responsibilities may include EU sanctioned activities:
 - a. All responsibilities related to the EU sanctioned activities shall be performed by other members of such division, department, or unit that are not EU Persons staff;
 - b. Subordinates of an EU Person who deal with EU sanctioned activities shall report to and take directions in relation to the EU sanctioned activities from the next senior person in the reporting line above the EU Person staff, that is not an EU Person staff (or from such other non- EU Person Staff member as such next senior person shall appoint);
 - c. In setting objectives to the subordinates, EU Person staff shall not include any objective that relates specifically to EU sanctioned activities, but may take into account retro-respect performance of subordinates that are not EU Persons staff in relation to EU sanctioned activities in conducting performance reviews.
- 1.4 Written communications relating to any EU sanctioned activities should not be addressed or copied to any EU Person.

5. **Prohibition on Referring EU Sanctioned Activity to Any Non- EU Person Staff**

If an EU Person staff receives any communication concerning an EU sanctioned activity, he or she must not re-direct the communication, its subject matter or the person making the communication to any other person, but should inform the next senior person in the reporting line above him or her that is not an EU Person staff member of the communication, without making any recommendation or qualitative comment regarding the communication.

6. **Dispensations**

Dispensations may be granted to staff of The National Bank, branches and subsidiaries who are EU Persons in relation to certain EU sanctioned countries subject to the written approval of the Compliance Risk Committee. The Head of the AML/CFT & Risk manager will maintain a record of dispensations and copies of written approvals of any such dispensations.

7. Record Retention

8.1 Introduction

We must maintain our records accurately and retain them in accordance with the applicable law (e.g. Commercial Law and PMA requirement to retain records for at least 10 years from account closure etc.) The records, data and information owned, collected, used and managed by The National Bank must be accurate and complete. Each employee is personally responsible for the integrity of the information, reports and records under his control. Records must be maintained in sufficient detail as to reflect accurately all Banks' transactions. Financial statements must always be prepared in accordance with International Financial Reporting Standards and PMA requirements and fairly represent, in all material respects, The National Bank's financial conditions and results in accordance with those standards.

The retention of records and documents is an important area of compliance which is relevant to all The National Bank businesses and functions. A wide range of documents and records must be held for certain periods in order to:

- Comply with minimum legal requirements;
- Be available for use in the event of future litigation.

8.2 Retention Period requirement

Palestinian Decree No (20) for the year 2015 defines the minimum standards for retention of records for all financial institutions. In particular, Articles 10 specify the requirement for maintaining records. All Bank records must be retained for a period not less than ten years from the date when such records are treated as closed.

Individual business units have policies relevant to the retention of records; records should be retained in accordance with those policies. In addition, it is prohibited to destroy any records that are potentially relevant to a violation of law or any litigation or any pending, threatened or foreseeable government investigation or proceeding.

The following are the most important documents and records that must be kept for a period of not less than 10 years from the date of the end of the business relationship:

- 1) The original copy or a certified copy of all documents, records of data and information obtained in the context of the due diligence procedures and the identification and verification procedures mentioned in this guide, including identification and verification of the identity of the customer and / or the real beneficiary and / or persons representing the customer In conducting transactions on his behalf or other parties related to the customer.
- 2) Any additional information regarding the customer or the real beneficiary of the customer that was obtained through due diligence and strict or continuous follow-up procedures.
- 3) The original copy and / or a certified copy of the documents, records of data and information related to the purpose and nature of the banking relationship with the customer, wherever possible.
- 4) The original copy and / or a certified copy of the documents and records related to the customer's account (such as the account opening form) and correspondence that was made with the customer or the real beneficiary of the customer and that must include, at a minimum, due diligence procedures and fundamental changes related to account activity.

8.3 Electronic archiving system

The process of maintaining and archiving records and documents and the speedy retrieval of these documents is a necessary and legal requirement and the bank is keen to adhere to that. The bank has an electronic system for archiving records and documents in order to ensure the following:

- 1) Review and track the transfer of funds through the bank to any customer or real beneficiary.
- 2) The ability to identify and identify any real customer or beneficiary.
- 3) Rapid response to requests from the Monetary Authority and the competent authorities by providing them with the required documents and documents.
- 4) Compliance with legal requirements for record keeping and documentation.

8. Sanctions in the event of non-compliance with anti money laundering and terrorist financing laws

The following is a summary of the sanctions imposed by Law No. (20) of 2015:

9.1 Article (38) Exemption from sanctions

Whoever initiates to notify the unit for the crime of money laundering or terrorist financing before knowing it, or any of the competent authorities is exempted from the punishment If the notification occurred after learning about the crime, the exemption should be that the reporting would seize the rest of the perpetrators or the funds subject to the crime.

9.2 Article (39) The penalty for a legal person

1. In cases where the crime of money laundering or terrorist financing is committed by the legal person, and without prejudice to the responsibility of his natural person, a legal person is liable to a fine of no less than 10,000 Jordanian dinars and no more than 200,000 Jordanian dinars or the equivalent in circulation.
2. The person responsible for the actual management of the violating legal person shall be punished with the penalty prescribed under the provisions of paragraphs 1 and 2 of Article (37) of this law, and paragraph (1) of Article (43) of this law, if it appears his knowledge of it or the crime occurred due to a breach of duties His job.
3. The legal person is jointly responsible for the fulfillment of the fines and compensation imposed by it, if the crime that occurred in violation of the provisions of this law was committed by one of his own and his own.

9.3 Article (43) Penalty for financing terrorism crime

1. A penalty of imprisonment for a period of no less than 5 years and a financial fine of no less than 50,000 Jordanian dinars, with the confiscation of all means used or intended to be used in the crime will be charged against whoever commits or attempts to commit the crime of financing terrorism as stipulated in paragraphs 4, 5, 6 of the article (2) From this decision by law, the partner, the interferer and the instigator shall be punished with the same penalty prescribed for the original actor.
2. Anyone who refuses to implement any of the provisions of Articles (6, 7, 8, 9, 10, 11, 14, 29) of this decision is punished by imprisonment for a period of no less than one year and not exceeding 3 years or by a fine of no less than 5,000 dinars Jordanian and not more than 100,000 Jordanian dinars or its equivalent in the currency in circulation or with both of these penalties.
3. Anyone who violates the provisions of Articles (16 and 29) of this decision shall be punished by imprisonment for a period of no less than 3 months and not exceeding a year or a fine of no less than 1,000 Jordanian dinars and no

more than 10,000 Jordanian dinars, or the equivalent thereof in the currency in circulation, or both of these The two penalties.

4. Anyone who violates the provisions of Article (35) of this decision shall be punished by a fine not exceeding 10% of the value of the unauthorized funds, or upon disclosure or false declaration thereof, and the penalty will be doubled in the event of a repeat of the violation.
5. The court may prevent persons who are found guilty of violating the provisions of the articles stipulated in paragraph 2 of this article, by temporarily or permanently depriving them of their duties.

9.4 Article (44) Penalty for violating the provisions of the law decree

1. Whoever violates the provisions of this resolution by law or any regulations or instructions issued pursuant to it, and who does not intentionally or out of negligence comply with these obligations, the supervising authority should, upon discovering this violation by financial institutions and non-financial businesses and professions, take measures and impose any From the following penalties:
 - a. Alert to comply with specific instructions.
 - b. Submit periodic reports by financial institutions and non-financial businesses and professions about the measures they implement or these reports indicate compliance with the specified instructions.
 - c. Written notice.
 - d. Impose a fine of no less than 1,000 Jordanian dinars and no more than 50,000 Jordanian dinars, or its equivalent in the currency in circulation.
 - e. Depriving individuals of employment in financial institutions and non-financial businesses and professions.
 - f. Replacing or restricting powers granted to dominant managers, chiefs or owners, including the appointment of a special director.
 - g. Imposing a suspension, restriction or revocation of a license and preventing the continuation of work or profession.
2. For the purposes of informing the public, information about the actions taken under paragraph 1 of this article may be published.

9. National Bank companies and financial institutions

The Anti-Money Laundering and Terrorist Financing Unit at the National Bank:

1. Making sure that all subsidiaries have anti-money laundering and terrorist financing policies and procedures as a minimum similar to the policies of the National Bank's procedures, including electronic systems.
2. Have access to the periodic reports issued by the anti-money laundering and terrorist financing units in those subsidiaries.
3. Have access the internal audit reports of the visits to examine the effectiveness of anti-money laundering policies and procedures in those companies.
4. View the reports on the visits of the regulatory authorities to combat money laundering and terrorist financing.
5. Meeting at least once a year with anti-money laundering and terrorist financing officials in subsidiary companies to discuss the latest developments in the areas of anti-money laundering and terrorist financing and the mechanism for developing current policies and procedures.

10. Compliance Training

11.1 Significance of Compliance Training

Compliance Training is a cornerstone of building and maintaining a compliant organization. The National Bank places great emphasis on the delivery of first class compliance education at all levels. Compliance training is geared to equip people with the awareness and attitudes which they need in order to work effectively and profitably within the Bank's ethical and regulatory environment. It aims to provide every individual working in TNB with the means to achieve the following goals:-

1. To understand the relevance of compliance to the Bank's strategic objectives and to motivate themselves to become part of the "compliance culture";
2. To know what is expected of them in terms of **(1)** the requirements of The National Bank Compliance Standards and its Code of Ethics, together with the business related policies and procedures stemming from that document and **(2)** the central requirements of relevant laws and regulations affecting the Bank ; and

Regular compliance training is therefore a key requirement. Ultimately, it is the responsibility of line management and of each individual working in partnership with the Compliance Department and HR to ensure that the means made available are fully exploited in pursuance of the above goals. To this end, the means of learning will primarily be in the hands of line management and the individual.

11.2 Types of Compliance Training

The National Bank Compliance Training Programme has two distinct but complementary elements. These are:-

- Standard Classroom Induction (KYC, MLP, Compliance and Fraud Prevention)
- E-Learning

These two elements will provide the means through which individuals can achieve the goals outlined above and by which line managers can oversee implementation.

11.3 Benefits of Compliance Training

- 1) The National Bank Compliance Training Programme is a strategic approach to compliance training which emphasizes the links between good compliance and successful business.
- 2) Explain ways and methods of money laundering and terrorist financing.
- 3) Explain the factors suspecting money laundering and terrorist financing activities.
- 4) Explain the mechanism for reporting suspected money laundering and terrorist financing operations.
- 5) Explain the procedures for identifying customers and verifying the real beneficiary.
- 6) It helps to build a strong foundation of knowledge on organizational matters and ethical values that will enable employees to broaden their understanding of the legal and regulatory environments in which the bank operates, thereby enhancing the quality of their assessment and decision-making.
- 7) There will be less chance of costly errors due to ignorance of laws and regulations.

“Compliance is everyone’s responsibility”