Instructions No. 2 of 2016

On Anti-Money Laundering and Counter-Terrorism Financing Measures for Banks

The National Committee for Anti-Money Laundering and Counter-Terrorism Financing ,

Pursuant to the provisions of Decree Law no. (20) of 2015 on Anti-Money Laundering and Counter Terrorism Financing and amendments thereto, particularly Articles 6/1, 20/14 and 23/3 thereof,

Based on the powers conferred upon it,

And to serve the public interest,

Has issued the following instructions:

Article 1

Definitions

1. The terms and expressions contained in these instructions shall have the meanings indicated below, unless the context indicates otherwise:

Law: Decree law no. 20 of 2015 on Anti-Money Laundering and Counter-Terrorism Financing

Committee: The National Committee for Anti-Money Laundering and Counter-Terrorism Financing (NCAML/CFT).

Unit: The Financial Follow-up Unit (FFU).

PMA: The Palestine Monetary Authority.

Politically Exposed Person (PEP): any person along with their family members, relatives, and associates, who is or has been entrusted with prominent public functions or political positions in Palestine or abroad including political party leaders, judges, legislative council members, prosecutors, heads of State-Owned Enterprises, heads of charitable institutions, bodies or associations and NGOs or

authorities of the State of Palestine or of any other foreign state and heads and representatives of international organizations.

Customer: the natural person or legal entity dealing with the bank.

Occasional Customer: a customer that does not have an ongoing business relationship with the bank.

Beneficial Owner: the natural person who ultimately owns or controls a customer or the account of the person on whose behalf a transaction is conducted, or the person who exercises ultimate, actual control over a legal entity or its management.

Business Relationship: the relationship between the customer and the bank in terms of banking activities and services provided by the bank to its customers.

Customer Due Diligence (CDD): Identifying the customer, determining their legal status, activity, sources of property and the purpose and nature and beneficial owner (if any) of the business relationship, in addition to verifying such and the ongoing monitoring of transactions carried out as part of the business relationship using any of the means identified in relevant legislations, and identifying the nature and purpose of the future relationship between the bank and the customer.

The Committee of enforcing UN Security Council Resolutions (UNSCRs): The committee formed by presidential decree in charge of implementing UNSCRs issued under Chapter VII, relevant to AML/CFT and combatting the proliferation of WMDs.

Shell Bank: a bank that has no fixed place of business where it receives customers, does not employ one or more persons to conduct actual activity and exercise effective management, does not keep records of its transactions, and is not subject to inspection by the relevant supervisory authority in the country where it was incorporated or in another country.

Wire Transfer: Any transfer executed through a bank using electronic means on behalf of an originator requesting the transfer, whereby the money is transferred to another bank and can be received by a beneficiary, irrespective of whether the originator and the beneficiary are the same person.

2. Definitions included in Decree Law no. 20 of 2015 on AML/CFT shall apply wherever mentioned in the present instructions.

Article 2

Scope of Application

The provisions of the present instructions shall be applicable to all banks operating in the State of Palestine and licensed to operate by the PMA or branches of Palestinian banks operating abroad to the extent permitted by laws and regulations in force in such countries.

Article 3

Prohibitions

Banks are prohibited from undertaking the following:

1. Dealing with anonymous persons, persons with false or fictitious names or persons with which they are banned to deal as per legislations in force or based on the instructions of the PMA.
2. Opening numbered accounts.
3. Dealing with shell banks.

Article 4

Customer Due Diligence

Banks shall undertake CDD measures in the following cases:

1- Upon establishing a business relationship with the customer.

2- When an occasional customer wishes to carry out any financial transaction with a value equal to or greater than five thousand US dollars or of an equivalent value in other currencies whether conducted as a single transaction or several transactions that appear to be linked; in case the transaction amount is unknown at the time it is conducted, the customer identity should be identified as soon as the amount is known or as soon as the threshold is reached.

3- When an occasional customer wishes to carry out a local or international wire transfer regardless of its value.

4- Upon a request to initiate or receive local or international wire transfers regardless of their value.

5- Whenever there is a suspicion of money laundering or terrorism financing.

6- Whenever the bank has doubts regarding the accuracy or adequacy of previously obtained customer identification information.

Article 5

Customer Identification and Identity Verification Procedures

Banks shall abide by the following:

1. Use official documents provided by the customer at the beginning of the business relationship to identify such customer, the nature of his/her activity or source of property and verify such information by obtaining a signed and certified copy of such documents.
2. Take necessary steps to verify the authenticity of information obtained from the customer using reliable and independent sources including contacting the official entities that issued the documents mentioned under paragraph 1 of this Article.
3. The following identification measures shall be taken in case the customer is a natural person:
    a. Full name of the customer, his/her nationality, date and place of birth, ID number, passport number for non-Palestinians, current and permanent residence address, telephone number, business address, nature of business or activity, the purpose of the business relationship, income and source of wealth of the customer, and any other information that the bank deems necessary.
    b. Agents shall present a duly certified copy of the power of attorney in addition to identity documents of both the agent and the principal, in cases where a person deals with the bank on behalf of the customer.
    c. For incompetent or incapacitated persons, identity documents of that person and the person legally representing them must be obtained in line with the identification and verification procedures stipulated in this Article.
    d. In order to open an account, special forms adopted by the bank and its branches shall be used, including an affidavit from the customer certifying that he/she is the original owner and sole beneficiary.
    e. Understand the intended use of the account, regarding property going through the account and the anticipated number, type and frequency of transactions.
4. Requesting a written statement from each customer identifying the beneficial owner of the financial transaction that he/she wishes to carry out, identifying and verifying the identity of the

beneficial owner in line with the identification and verification procedures stipulated in the present instructions.

5. The following measures shall be taken in case the customer is a legal entity:

a. Identifying the name, address, head office, legal status, registration date and number, names of owners and shares in the legal entity, in order for the bank to understand the ownership structure of the legal entity. The bank shall also identify managers of the entity and the purpose and nature of the business relationship and verify information indicated in this paragraph by obtaining certified documents, including the following:

- Registration certificate issued in line with laws in force in Palestine, including certificates issued by the Ministry of Economy, Chambers of Commerce or Industry, municipalities or any other competent authority to register legal entities.
- Articles of Association
- By-laws
- Authorized persons (presenting supporting documents to that effect).
- Identity of legal representatives

b. Names of shareholders whose shares exceed 10% of the capital shall be verified and documents supporting this information should be annexed to the requested documents with the exception of public shareholding companies.

c. In case the beneficial owner of the entity is a politically exposed person, identification and verification procedures specific to PEPs as stipulated in the Law and these instructions shall apply.

d. When identifying the beneficial owner of a legal entity, measures must be taken to understand the ownership and control structure of the entity. This includes relying on information from official documents obtained until the bank is satisfied that it has identified the beneficial owner.

e. Understand the intended use of the account regarding property going through the account and the anticipated number, type and frequency of transactions

f. Provisions of paragraph 5 of the present article shall apply to foreign companies and the bank may request any other information it deems appropriate.

6. Regarding charities, NGOs or NPOs and the like, the name of the organization must be identified, along with its head office, legal form, type of activity, date of establishment, purpose of the business relationship, authorized persons, their nationalities and telephone numbers. The

information indicated in this paragraph must be verified by obtaining certified documents, including the following documents duly certified and authenticated:

a. Registration certificate of the association, NGO or NPO issued by the competent registration authority.
b. Articles of Association
c. Documents indicating authorized persons to manage their account. The identity of the authorized person must be established in line with the identification measures stipulated in the present instructions. The identification of authorized persons must be regularly updated.
d. Identity of the legal representative.

7. The bank may delay the verification of the customer or beneficial owner identity until after the establishment of the business relationship when all of the following conditions are fulfilled:
   a) Verification procedures shall be conducted as soon as possible.
   b) Delay of the verification procedures is essential not to interrupt the normal course of business provided that such delay does not entail any risks of money laundering or terrorism financing.
   c) Examining ML/TF risks for the case where verification was delayed and controlling such risks.
   d) The bank has adopted clear procedures to that effect.
8. Information requested under this Article for legal entities shall be updated annually, including for charity organizations, NGOs and NPOs. Information for natural persons shall be updated every two years. The updating requirement shall be implemented in all cases whenever the accuracy of the information obtained is doubtful.

Article 6

Higher Risks

Banks shall comply with the following:

1- Classify all their customers according to the level of ML and TF risks they pose, and periodically review and update such classification.

2- Apply enhanced due diligence measures when ML/TF risks are higher.

3- Apply simplified due diligence measures only when ML or TF risks are considered low, by conducting an appropriate risk assessment by the State or the financial institution. Simplified due diligence measures must be commensurate with low risk elements and shall not be acceptable when there is a suspicion of ML or TF suspicion, or when high risks are noticed, and/or upon the instructions of the PMA.

4- Establishing necessary internal policies, measures and procedures to avoid risks related to the misuse of indirect or non-face-to-face relationships with customers or any transactions carried out electronically.

5- When dealing with Politically Exposed Persons (PEPs) as classified in instructions no. number 1/2014 issued by the NCAML, banks must show special care, as they are considered high risk persons, by applying the following measures:

a- Applying the identification and verification measures set out in article 5 of the present instructions.
b- Obtaining senior management approval prior to establishing or pursuing a business relationship with a PEP.
c- Verifying the source of property to be deposited, and their sources of wealth.
d- Establish a risk management system for PEPs or the beneficial owners of this category.
e- Ensure a close and continuous follow-up of the transactions of such customers.
f- Take the necessary measures to verify the circumstances surrounding any business relationship or transaction carried out with a PEP and its purposes if the bank concludes that any of these elements is not based on clear economic justifications, and to keep records of the results of these measures.

Article 7

Wire Transfer Identification Measures

In addition to the due diligence measures stipulated under article 5 of the present instructions, banks shall comply with the following:

1- Obtain detailed information on the person requesting the outgoing wire transfer (originator), including their name, account number, identity or passport number, purpose of the transfer,

relationship with the beneficiary, the beneficiary's name, account number, address, bank and bank address, and obtain the supporting documents thereto.

2- In case of an incoming wire transfer, detailed information must be obtained on the transfer's beneficiary, bank account number, identity or passport number, purpose of the transfer, the relationship between the originator and the beneficiary, the name of the originator, their bank, account number, and address in the originator's country. The information mentioned should be document supported, while relevant due diligence measures set out in article 5 of the present instructions must also be fulfilled.

3- Establish special policies, procedures and measures when dealing with wire transfer risks in cases of ML and TF, provided the volume and/or frequency of the transfers are taken into consideration, and while applying continuous due diligence measures to examine the activity of the originator in comparison with the nature of their real activity and sources of income.

4- If the information required in paragraphs 1 and 2 of this article is not fulfilled, the wire transfer should not be executed.

5- Banks shall refrain from carrying out any wire transfers to any person or entity designated on the list of the International Sanctions Committee under UNSCR No. 1267 of 1999, or any lists issued by the UNSC Resolutions Implementation Committee.

Article 8

Risk-Based Approach

Banks shall adopt a risk-based approach that should include at a minimum the following:

1- Identify, understand and analyze money laundering and terrorism financing risks

2- Take into consideration the results of the risk assessment set forth in paragraph 1 of this article, in implementing AML measures, and establish policies and strategies in line with these risks.

3- Submit the results of the measures applied as per this article to the PMA upon request.

Article 9

Special care

The bank should grant special attention to the following cases:

1- When leasing safe deposit boxes

2- When receiving requests of facilities against deposits

3- When a person deposits cash amounts or traveler's cheques in an existing account through persons who do not duly represent the account holder

4- When collecting cheques of unknown third parties from abroad

5- When requesting big, complicated or offshore transactions or deals, and any type of unusual deal or transaction with unclear financial purposes.

6- Large or repeated foreign exchange transactions (currency purchase and sale in financial centers) based on cash amounts

7- Exchanging large amounts of small bank against larger denominations.

8- Depositing large amounts or making repeated deposits of multiple amounts constituting a large total and not commensurate with the stated nature of activity and usual transaction volume of the customer.

9- Operating an account mainly for the purpose of transferring or receiving large amounts of money to or from foreign countries, which may appear to the bank operator unjustified by the customer's activity.

10- Collecting abroad-issued or nominal bearer's cheques of high amounts that are not in line with the stated nature of activity and usual transaction volume of the customer, or when the customer claims that such property are gambling gains, for instance.

11- Large or repeated transactions that are related to an external activity and that the bank deems do not match the volume of this activity.

Article 10

Record keeping

Banks must retain all records and documents for at least 10 years from the date of the completion of the financial transaction, the end of the business relationship, or after an occasional transaction is executed. In case the account was closed due to an investigation in money laundering or terrorism financing, information and documents must be kept until the end of the investigation. The record keeping mechanism shall be in line with standards accepted by Palestinian courts and/or laws in force in the country. Records shall include:

1. Information related to due diligence measures taken in line with Article 5 of the present instructions
2. Information to clarify financial transactions and commercial and cash operations whether domestic or foreign
3. Accounts files and correspondence
4. Copies of personal identification documents or registration certificates

Article 11

Internal Procedures

Banks shall abide by the following:

1. Appoint a reporting officer at senior management level and a deputy reporting officer in case of his/her absence in charge of the following:
    a. Notifying the Unit immediately, in paper form or electronically, of transactions suspected to be related to money laundering, terrorism financing or any predicate offense, whether such transactions have taken place or not, using the form annexed to the present instructions and drafted specifically for such cases, and refrain from closing the account(s) of the suspected persons.
    b. Receiving notifications from any bank employee whenever he/she suspects that an attempted transaction may be linked to money laundering, terrorism financing or any predicate offense.

c. Providing the Unit with information on transactions suspected to be related to money laundering, terrorism financing, or any predicate offense, in addition to any other information requested and facilitating its review of any relevant records or documents for the performance of its duties.
d. Verifying compliance of the bank with provisions of the Law and instructions issued pursuant thereto.
e. Training employees in order to enhance their capacities to detect money laundering schemes.
f. Establishing AML/CFT policies and an internal procedural guide for compliance with provisions of the Law, regulations and instructions issued pursuant thereto.
g. Retaining all documents and internal reports received from and sent to the Unit.
h. Preparing periodic reports on unusual transactions or transactions suspected to be linked to money laundering and terrorism financing.
i. Establishing the necessary systems to classify customers according to their risk level in light of information and data available to the bank and reviewing such periodically.
j. Establishing systems and procedures that ensure the performance of internal audit bodies of their role in examining internal control and supervision systems to guarantee their effectiveness in AML/CFT and reviewing such periodically, in order to complement any lack therein and update and develop the effectiveness and efficiency thereof.

2. The reporting officer must be able to act independently and maintain the confidentiality of information received or sent by him/her as per the present instructions. The Reporting Officer shall have access to records and data required to perform the tasks of inspection and revision of systems and procedures adopted by the financial entity to combat money laundering and counter terrorism financing.
3. Designate the adequate, fit and qualified human resources in the field of AML/CFT, proportionate to the size of the bank, its operations and risks it faces.

Article 12

Daily Financial Transactions Reports

1- Banks must provide the Unit with daily reports on financial transactions carried out by or through it, and include information on the parties to the financial transaction and its value in line with the following:

a- All outgoing or incoming wire transfers into or out of Palestine with a value equal to or exceeding USD 5,000 or its equivalent in other currencies.
b- All domestic wire transfers amongst banks with a value equal to or exceeding USD 5,000 or its equivalent in other currencies.
c- All types of cheques with a value equal to or exceeding USD 5,000 or its equivalent in other currencies.
d- Deposits or withdrawals with a value equal to or exceeding USD 5,000 or its equivalent in other currencies.
e- Documentary credits and policies with a value equal to or exceeding USD 5,000 or its equivalent in other currencies, including transfers related to the execution of those credits.

2- Financial transactions identified in this article are deemed unusual transactions for the purposes of combating money laundering and terrorism financing.

3- Reports shall be submitted on the above identified financial transactions via the electronic means adopted by the Unit.

4- Technical instructions shall be issued to ensure compliance with this article based on instructions issued by the Unit in coordination with the PMA.

Article 13

Implementation of UNSCRs

Banks shall immediately implement obligations under resolutions issued by the Committee for the Implementation of UN Security Council Resolutions, circulated by the PMA, and establish the necessary electronic system to guarantee effective implementation thereof.

Article 14

Reporting Form

Banks shall resort to the Guidance Manual annexed to the present instructions to help identify patterns suspected of including money laundering or terrorism financing operations, and rely on it as a staff awareness raising tool while ensuring it is constantly updated and improved.

Article 15

Repeal

1. Anti-Money Laundering instructions no. 1/2009 for banks operating in Palestine issued by the Committee shall be repealed.
2. All texts conflicting with the present instructions shall be repealed.

Article 16

Entry into force

All competent authorities shall implement the provisions of the present instructions, each within their own purview. The present instructions shall enter into force on the day they are published in the Official Gazette.

Issued in Ramallah on: 08/06/2016 AD

Equivalent to: 03/Ramadan/1437 AH

The National Committee for Anti-Money Laundering and Counter-Terrorism Financing .

Reporting Form

Form no: 1

To be used by the FFU	
Receipt no.:	
Date of Receipt:	
Time of Receipt:	

Form to be used by banks to report a transaction suspected to include elements of money laundering, terrorism financing or predicate offense

First: Bank information:

1- Bank Name			
2- Supervisory Authority			
3- Branch where transaction took place			
4- Branch address			
5- Branch phone and fax numbers	Phone: /	Fax:	
6- Name of Manager		Phone:	Fax:

Second: Customer information

A- If the customer is a natural person

7- Name:		
8- Gender:	□ Male	□ Female
9- Nationality		

10- Occupation:	
11- Place of work:	12- Address:

13- Date of birth	Day	Month	Year	14- Place of birth	

15- Address according to identification documents			
	Street:	City:	Province:

16- Permanent Place of Residence:	

17- Permanent residential address abroad (if any)				
18- Phone numbers and email:	Home	Work	Mobile	E-mail

19- Identity document type:			
20- Identity document information:			
No.	Place of Issue:		
Date of Issue:	Day:	Month:	Year:
Date of Expiry:	Day:	Month:	Year:

B- If the customer is a legal entity

(B-1) Information about the legal entity:

21: Name	
22: Legal Form	

23: Headquarters address			
	Street:	City:	Province:

24: Establishment Date:	Day	Month	Year	25: Contributed Capital	

26: Activity description as per the Commercial Register				
27: Commercial Registration No.				
28: Registration Date and Authority				
29: Licensed Operator Nb:	30: Type	□ Exempted	□ Small	□ Regular

(B-2) Information on the natural person that is the authorized signatory on behalf of the legal entity:

31: Full Name	Name of person	Name of Father	Name of Grandfather	Last Name
32: Gender	□ Male		□ Female	
33: Nationality				

34: Occupation:		
35: Place of work:		36: Address

37: Nature of the relationship with the legal entity:	

38: Date of Birth	Day	Month	Year	39: Place of Birth	

40: Address according to identification documents			
	Street:	City:	Province:

41: Permanent Residence Address	

42: Permanent Residence Address abroad (If any)	

43: Phone Numbers & email:	Home	Work	Mobile	Email

44: Type of Identity document:			
45: Identity document information:			
No:	Place of Issue:		
Date of issue:	Day:	Month:	Year:
Date of expiry:	Day:	Month:	Year:

Third: Beneficiary Information (If any)

46: Name of Beneficiary:	
47: Address:	
48: Nationality:	

49: Beneficiary's Bank:	
50: Beneficiary's Account No:	

Fourth: Suspicious Transaction Information

51: Transaction Date:	Day:	Month:	Year:
52: Transaction Suspicion Date:	Day:	Month:	Year:
53: Type of transaction:			

54: Transaction Value:	
55: Currency:	

56: Type of account used for the purposes of the transaction:			
57: Account No:			
58: Date of opening the account:	Day:	Month:	Year:

59: Description of the transaction:

60. Reasons and grounds of suspicion:		
* Were any previous reports submitted about the same person carrying out a suspicious transaction?	□ Yes (reporting date):	□ No

Money Laundering and Counter Financing of Terrorism (AML/CFT) Guidance Manual

The present manual is intended to enhance AML measures in order to ensure property compliance with such guidance and controls by all banks operating in Palestine.

I. Stages of Money Laundering

The process of money laundering goes through three stages:

1. Placement: starts with the launderer placing cash proceeds derived from any of the offenses stated in Article 3 of the AML/CFT Decree Law No. 20 of 2015, into the banking system.
2. Layering: is the stage where the link between illicit proceeds and their source is concealed by conducting repeated financial and banking transactions.
3. Integration: where the laundered properties are integrated into the economy such that it becomes difficult to distinguish between such property and property from legitimate sources.

II. The methods used to counter the financing of terrorism are fundamentally aligned with the methods used to conceal the sources of property, that may be from legitimate sources or illegitimate criminal activity.

III: The following methods are used in money laundering and terrorism financing operations. They can take the following forms:

a. Financial and banking transactions involving the use of cash, including:

1. Unusually large cash deposits inconsistent with the customer's business activity, whether the customer is a natural person or a company.
2. Customer repeatedly deposits cash where the sum of such deposits, within a certain period of time, is inconsistent with the customer's activity.
3. Substantial increase in the cash deposits of a customer, with no apparent cause, particularly if such deposits are subsequently transferred within a short period of time to a party with no obvious connection to the customer.

4. The use of cash withdrawals and deposits instead of bank transfers or other negotiable and readily marketable instruments for no obvious reason.
5. Customers seeking to exchange large amounts of small denomination bank notes with large ones without justification.
6. The transfer of large sums of money from Palestine or the use of incoming international transfers with instructions for payment in cash.
7. Large and unusual cash deposits using ATMs to avoid direct contact with bank employees, especially if such deposit amounts are inconsistent with the customer's income from business activity.
8. A customer performs several large cash transactions on the same day at multiple bank branches or has several individuals perform the transaction on his/her behalf.
9. Customer retrieves a part of the amount he/she intended to deposit when becoming aware of customer due diligence measures to be followed for unusual transactions, as per instructions.
10. Cash deposits containing a considerable amount of counterfeited, worn or old bank notes.
11. Customer suddenly and promptly withdraws their available balance without reasonable or acceptable justification.

b. Personal bank accounts:

1. Keeping different accounts and depositing amounts of cash in each with a total balance amounting to a large sum that is inconsistent with the nature of the customer's business.
2. Accounts where the nature of performed transactions does not seem to match the nature of the customer's business activity, but are used to receive and/or distribute large sums with no obvious purpose or irrelevant to the account holder and/or business.
3. Customers keeping a number of accounts with several banks within the same geographical area, who later transfer all balances in the accounts to a single account and transfers the sum to a party abroad.
4. Deposits of third-party cheques with large amounts, endorsed to the account holder, but that do not appear to match with the relationship with the account holder or the nature of his/her business activity.
5. Effecting large cash withdrawals from an account from which relatively small amounts were withdrawn in the past, or from an account which has just received an unexpected large amount from abroad.

6. A large number of people making deposits in the same account without a satisfying explanation.
7. The customer submits business financial statements that are markedly different from other similar businesses working in the same sector.
8. Companies with relatively large business activities submitting financial statements that are unaudited and unapproved by an independent auditor.
9. A company that accepts cheques from its customers and does not make any considerable cash withdrawals against these cheques from its accounts, suggesting the possibility of having other sources of income.
10. A drastic change in the management of a customer's account in a way that does not match their information.
11. Bank accounts of a company or institution showing poor or irregular activity.

c. Transfers:

1. Receipt of large transfers with instructions for payment in cash that are inconsistent with the customer's business activity.
2. Receipt of regular large transfers from areas known for the prevalence of certain offenses such as the production of drugs or drug trafficking.
3. Receipt of transfers from abroad to dormant bank accounts.
4. Prompt transfer of deposits into the account to a foreign jurisdiction whether in one transaction or several ones.
5. The customer uses his/her account as an intermediary account to transfer property between other parties or accounts.
6. Transfer of similar amounts of property (on a daily or weekly basis) that constitute in total a large sum of property.
7. Ordering transfers for an individual that does not have an account with the bank using a variety of payment methods, the individual value of each being lower than the threshold set within the instructions.
8. Incoming transfers with instructions to convert to cheques to be sent by mail to an individual that does not have an account with the bank.
9. Making large transfers to countries known to be bank secrecy havens.
10. The beneficiary uses the value of transferred amounts received to his/her account to purchase various cash payment instruments to make payments to a third party.

11. Receipt of large transfers by a beneficiary account that normally does not receive such values, and in a manner that is inconsistent with the customer's nature of work.
12. A customer repeatedly conducts international transfers of property which he/she claims to be from an international source.
13. A customer deposits bearer instruments into his/her account then transfers them to a third or fourth party.
14. The account of an exchange office receives cash deposits or transfers of amounts lower than the threshold set in the instructions.

d. Safety deposit boxes, in any of the following forms:

1. Customer makes unusually regular visits to his/her own safe box.
2. Non-resident customer keeps safety deposit boxes without apparent explanation, particularly when safe custody service is offered by banks operating in the areas where he/she resides.
3. Customer rents multiple safety deposit boxes.

e. Investment related transactions:

1. Customer buys securities to be held at the bank's safety deposit service, where this does not appear to be consistent with the customer's apparent standing;
2. Customer conducts borrowing transactions against deposits from a company or offshore subsidiary, particularly if located in countries where production of drugs or drug trafficking is known to be prevalent;
3. Customer introduces large amounts from abroad to be invested in foreign transactions or securities, where the size of the investment is inconsistent with the nature of the customer's financial profile.
4. Customer frequently trades (selling and buying) in securities in circumstances that appear to be unusual.
5. Customer purchases securities to be held in the bank's safety deposit boxes, where this does not appear to be consistent with the customer's apparent business activity and financial status;
6. Customer seems generally uninterested with common investment decisions to be taken such as investment account fees or appropriate investment vehicle.
7. Customer liquidates a large financial position through a series of small cash transactions.

8. Customer makes cash deposits, payment orders, traveler's checks or counter checks with amounts lower than the threshold stipulated in the instructions to finance an investment account.
9. Customer uses investment accounts as a means to transfer property to external parties, especially off-shores.
10. Customer enters substantial amounts from abroad to be invested in foreign currencies or securities, when the size of said investment is inconsistent with the customer's financial situation.

f. International banking and financial transactions:

1. Acknowledge the identification of a person by external bodies existing in countries known for the production and/or trafficking of drugs;
2. Having large balances inconsistent with the size of business activities of the customer, in addition to frequent transfer to account(s) abroad.
3. Customer deposits foreign currencies or traveller's cheques frequently into bank account in a manner inconsistent with the normal activity of that account.

g. Bank facilities, including:

1. Customers pays off in unexpectedly large property facilities that are irregular
2. Customer applies for loans guaranteed by assets owned by a third party, such that the source of these assets is unidentified by the bank or the size of these assets is inconsistent with the customer's financial profile.

h. Electronic banking services, including:

1. Customer account receives several small electronic transfers, then makes large transfers in the same manner to another country.
2. Customer deposits large payments regularly using different means including electronic deposit or receiving large payments regularly from countries known to be producers and/or traffickers of drugs.

i. **Appropriate measures to be implemented by the bank include:**

1. Provide an automated program to monitor all unusual bank transactions.
2. Establish internal procedures that include measures to be followed by the bank employee when he/she suspects a money laundering transaction.

Issued in the city of Ramallah, on 08/06/2016

Corresponding to: 03/Ramadan/1437 AH

The National Committee for Anti-Money Laundering and Counter-Terrorism Financing .