TRUST SECURITIES & BROKERAGE LTD

ANTI MONEY LAUNDERING & COMBATING THE FINANCING OF TERORISM AND PROLIFERATION FINANCING

POLICY & PROCEDURES

1.3 VERSION

TRUST SECURITIES & BROKERAGE LTD

TABLE OF CONTENTS

Foreword

This Document lays down the Anti-Money Laundering & Combating the Financing of Terrorism Policies and Procedures to be followed by personnel working in each functional area. Money Laundering now has become a Global concern and is the mother of all crimes. These guidelines have been framed to ensure effective practices are implemented to counter the problem of Money Laundering & Combating Financing Terrorism and that TSBL is not made the victim of any Financial Crime. It is company's endeavour to ensure compliance in letter and spirit to the regulations under AML Act and the requirements as per the regulators However, as part of our commitment for continual improvement, each reader and follower of this manual is encouraged to identify improvement opportunities and bring them to the attention of the appropriate authority for evaluation and subsequent incorporation in the manual.

Each reader is also urged to identify those activities that may have undergone a change since the introduction of the manual, as well as new activities that have not been included and obsolete activities that still form a part of the document but are not relevant in the current context and bring them to the immediate attention of their supervisors for appropriate modification in the policy.

Policy Compliance

Consistent compliance with this policy is essential to its effectiveness. The Company including all Staff, Management and Executives are expected to adhere to this policy. Internal Audit and Compliance Department will monitor and assess the compliance of all Branches and report quarterly to the Board of Directors. Non-compliance or breach of this policy may result in disciplinary action.

Policy Revision

The AML / CFT Policy & Procedures is reviewed every year or at planned intervals whenever material changes occur to reflect the regulatory requirements.

SECTION A

1. INTRODUCTION

1.1 Purpose

The purpose of this document is to lay down the Anti-Money Laundering policies of Company in order to create awareness among all relevant staff members and all Department Heads about Money Laundering and the ways and means of combating the same effectively.

1.2 Scope

The scope of this document is to combat any act of money laundering and establish effective controls within the organization to ensure that the company restrain itself from being made a vehicle for Money laundering. To implement adequate due diligence on new and existing customers sound **Know-Your-Customer (KYC)** norms, continuous training of all relevant staff members and good reporting procedures to safeguard the organization from the dangers of Money Laundering.

1.3 Responsibility

Responsibility for approving the manual will lie with the BOD. Responsibility for ensuring implementation of the policies and procedures laid down in this manual will lie with the AML Compliance Officer. The Compliance Officer of the Company will be owner and custodian of this manual. The owner takes the ultimate responsibility for maintaining this manual to keep it updated according to changing needs of the organization and in response to changes in applicable regulations. No individualistic practices that are in conflict or are inconsistent with the contents of this manual will be allowed.

1.4 Review and Changes

Any changes in laws and regulations may also trigger a review of this policy document. The Compliance Officer of TSBL is responsible for keeping track of all regulatory pronouncements applicable to this policy. He will advise the BOD accordingly to initiate a review of the policies whenever applicable.

Any changes in the policy will be effected only upon approval by the Board of Directors. At the time of change the version number and date from which the document is effective will be changed as follows;

Version Number: The first issue of the document will bear the Version Number as 1.0. For any minor change in the document the version number will increase to 1.1, 1.2 and so on. In case of a major change in the system wherein the entire procedure needs to be re-written and re-issued, the new issue will be released with version number 2.0. Earlier versions will be marked obsolete and withdrawn from circulation

Effective Date: This is the date from which the document is effective and this is the date from which implementation and compliance to the document is expected. The document may be released earlier but with an effective date, which is later, which means that the compliance to the procedure is to start only from the date mentioned on the document.

1.5 Date of next review

TSBL will ensure that this policy document is reviewed at least once in a year so as to keep pace with the developments in the regulations and market. The next date of review will be within one year from the date of effect.

1.6 General Definition

Money laundering is the process, by which the criminals in possession of illegitimate money attempt to conceal the true origins and ownership of their wealth. Anti-money laundering (AML) efforts and Combating the Financing of Terrorism (CFT) have emerged as top priority with Governments and private business sector. More recent geopolitical events have brought the topic again into sharp focus. The rapid transformation of the financial market place and the trend towards convergence of the markets with the concurrent forces towards deregulation poses new challenges in the drive against money laundering and calls for adequate risk reduction strategies.

1.7 The Money Laundering Offence

As per Section 3 of the Money Laundering Act 2010 any person who intentionally commits any of the following acts shall be deemed to have committed the offence of money laundering:

a) Acquires, converts, possesses, uses or transfers property, knowing or having reason to believe that such property is proceeds of crime;

b) Conceals or disguises the true nature, origin, location, disposition, movement or ownership of property, knowing or having reason to believe that such property is proceeds of crime;

c) Holds or possesses on behalf of any other person any property knowing or having reason to believe that such property is proceeds of crime; or

d) Participates in associates, conspires to commit, attempts to commit, aids, abets, facilitates, or counsels the commission of the acts specified in clauses (a), (b) and (c)

1.8 Punishment for Money Laundering.

Whoever commits the offence of money laundering shall be punishable with rigorous imprisonment for a term which shall not be less than one year but may extend to ten years and shall also be liable to fine which may extend to one million rupees and shall also be liable to forfeiture of property involved in the money laundering.

Provided that the aforesaid fine may extend to five million rupees in case of a company and every director, officer or employee of the company found guilty under section 4 of the act and shall also be punishable under section 4 of the act.

1.9 National Executive Committee to combat money laundering.

The National Executive Committee is consisting of the following members. Namely: -

a.	Minister for Finance or Advisor to the Prime Minister on Finance/concerned Minister.	Chairman
b.	Minister for Foreign Affairs	Member
c.	Minister for Law and Justice	Member
d.	Minister for Interior	Member
e.	Governor SBP	Member
f.	Chairman SECP	Member
g.	Chairman NAB	Member
h.	Director-General	Member
i.	Director-General (FMU)	Secretary
j.	Any other member to be nominated by the Federal Government.	

SECTION B

2 ROLES AND RESPONSIBILITIES OF EMPLOYEES

2.1 Account Opening, KYC/AML Procedures and Processes

As per the Company policy and procedures no new account shall be approved unless the customer furnishes all the required information and provide documents as per following check list **Annexure-1** (prescribed by SECP) for different types of customers. The Authorized Account Opening Officer shall ensure that the information and documents are obtained / collected from the customer accordingly: -

Annexure-1

S. No.	Type of Customer/Features	Information /Documents to be Obtained
1.	Individuals	A photocopy of any one of the following valid identity documents: (i). Computerized National Identity Card (CNIC)/Smart National Identity Card (SNIC) issued by NADRA. (ii). National Identity Card for Overseas Pakistani NICOP/SNICOP) issued by NADRA. (iii). Form-B/Juvenile card issued by NADRA to children under the age of 18 years. (iv). Pakistan Origin Card (POC) issued by NADRA. (v). Alien Registration Card (ARC) issued by National Aliens Registration Authority (NARA), Ministry of Interior (local currency account only). (vi). Valid Proof of Registration (POR) Card issued by NADRA (vii). Passport having valid visa on it or any other proof of legal stay along with passport (foreign national individuals only).
2.	Joint Account	(i). A photocopy of any one of the documents mentioned at Serial No. I; (ii). In the case of joint accounts, CDD measures on all of the joint account holders shall be performed as if each of them is individual customers of the RP.
3.	Sole Proprietorship	(i). Photocopy of identity document as per Sr. No.1 above of the proprietor. (ii). Attested Copy of registration certificated for registered concerns. (iii). Sales Tax registration or NTN, wherever applicable (iv). Account opening requisition on business letter head. (v). Registered/Business address.
4.	Partnership	(i). Photocopy of identity document as per Sr. No.1 above of all the partners and authorized signatories. (ii). Attested copy of "Partnership Deed". (iii). Attested copy of Registration Certificate with Registrar of Firms. In case the partnership is unregistered, this fact shall be clearly mentioned on the Account Opening Form. (iv). Authority letter from all partners, in original, authorizing the person(s) to operate firm's account. (v). Registered Business address.

5.	Limited Liability Partnership (LLP)	(i). Photocopies of identity documents as per Sr. No. 1 above of all the partners and authorized signatories. (ii). Certified Copies of: (a) 'Limited Liability Partnership Deed/Agreement. (b) LLP-Form-III having detail of partners/designated partner in case of newly incorporated LLP. (c) LLP-Form-V regarding change in partners/designated partner in case of already incorporated LLP (iii). Authority letter signed by all partners, authorizing the person(s) to operate LLP account.
6.	Limited Companies/Corporations	(i). Certified copies of: (a) Resolution of Board of Directors for opening of account specifying the person(s) authorized to open and operate the account; (b) Memorandum and Articles of Association; (ii). Certified copy of Latest 'Form-A/Form-B'. (iii). Incorporate Form II in case of newly incorporated company and Form A/Form C whichever is applicable; and Form 29 in already incorporated companies (iv). Photocopies of identity documents as per Sr. No. 1 above of all the directors and persons authorized to open and operate the account; (v). Photocopies of identity documents as per Sr. No. 1 above of the beneficial owners.
	Branch Office or Liaison Office of Foreign Companies	(i). A copy of permission letter from relevant authority i-e Board of Investment. (ii). Photocopies of valid passports of all the signatories of account. List of directors on company letter head or prescribed format under relevant laws/regulations. (iii). Certified copies of (iv). Form II about particulars of directors, Principal Officer etc. in case of newly registered branch or liaison office of a foreign company (v). Form III about change in directors, principal officers etc. in already registered foreign companies branch or liaison office of a foreign company (vi). A Letter from Principal Office of the entity authorizing the person(s) to open and operate the account. (vii). Branch/Liaison office address.
8.	Trust, Clubs, Societies and Associations etc.	(i) Certified copies of: (a) Certificate of Registration/Instrument of Trust (b) By-laws/Rules & Regulations (ii) Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate the account. (ii) Photocopy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body. (iv) Registered address/ Business address where applicable.

9.	NGOs/NPOs/Charities	(i) Certified copies of: (a) Registration documents/certificate (b) By-laws/Rules & Regulations (ii) Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing (iii) Body, for opening of account authorizing the person(s) to operate the account. (iv) Photocopy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing/Body /Board of Trustees /Executive Committee, if it is ultimate governing body. (v) Any other documents as deemed necessary including its annual accounts/ financial statements or disclosures in any form which may help to ascertain the detail of its activities, sources and usage of funds in order to assess the risk profile of the prospective customer. (vi) Registered address/ Business address.
8.	Agents	(i). Certified copy of 'Power of Attorney' or 'Agency Agreement'. (ii). Photocopy of identity document as per Sr. No. 1 above of the agent and principal. (iii). The relevant documents/papers from Sr. No. 2 to 7, if agent or the principal is not a natural person. (iv). Registered / business address.
9.	Executives and Administrators	(i). Photocopy of identity document as per Sr. No. 1 above of the Executor/Administrator. (ii). A certified copy of Letter of Administration or Probate. (iii). Registered address/Business address.
10.	Minor Accounts	(i). Photocopy of Form-B, Birth Certificate or Student ID Card (as appropriate). (ii). Photocopy of identity document as per Sr. No. 1 above of the guardian of the minor.
11.	Executors and Administrators	(i) Photocopy of identity document as per Sr. No. 1 above of the Executor/Administrator. (ii) A certified copy of Letter of Administration or Probate. (iii) Registered address / Business address
12.	Minor Accounts	(i) Photocopy of Form-B, Birth Certificate or Student ID card (as appropriate). (ii) Photocopy of identity document as per Sr. No. 1 above of the guardian of the minor.

2.2 Verification

All verification shall be done only after meeting the customer in person and seeing his original documents. The duplicate copies shall be stamped with Original seen and signed by the executive verifying it.

2.3 Risk Assessment

The Company shall take appropriate steps in accordance with section 7F of the AML Act to identify, assess and understand its money laundering, and terrorism financing risks for customers, countries or geographic areas and products, services, transactions or delivery channels. The Company shall:

(a) document its risk assessments;

(b) consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;

(c) keep its risk assessments up to date;

(d) categorize its own overall entity level risk as high, medium or low based on the result of risk assessment; and

(e) have appropriate mechanisms to provide risk assessment information to the commission.

2.4 Risk Mitigation and Applying Risk Based Approach

The Company must implement following counter ML/TF/PF measures, with regard to the ML/TF/PF risks and the size of its business.

(a). develop and implement policies, procedures and controls, which are approved by its board of directors, to enable the Company to effectively manage and mitigate the risks that are identified in the risk assessment of ML/TF/PF or notified to it by the Commission;

(b). monitor the implementation of those policies, procedures and controls and enhance them if necessary;

(c). perform enhanced measures where higher risks are identified, to effectively manage and mitigate those higher risks including regular monitoring and review of those risks; and

(d). have an independent audit function to test the system.

The Company may take simplified measures to manage and mitigate risks, if lower risks have been identified. Simplified measures should not be permitted whenever there is a suspicion of ML/TF.

Explanation: - For the purposes of this regulation the expression “risk-based approach” means applying measures to manage and mitigate money laundering and terrorist financing risks that are commensurate with the risks identified.

2.5 New Products, Practices and Technologies

The Company shall:

(a). identify and assess the money laundering and terrorism financing risks that may arise in relation to-

(i). the development of new products and new business practices, including new delivery mechanisms; and

(ii). the use of new or developing technologies for both new and pre-existing products;

(b). Undertake the risk assessments, prior to the launch or use of such products, practices and technologies, and shall take appropriate measures to manage and mitigate the risks.

(c). in complying with the requirements of clauses (a) and (b), pay special attention to any new products and new business practices, including new delivery mechanisms; and new or developing technologies that favour anonymity.

2.6 Customer Due Diligence

The company shall conduct Customer Due Diligence in the circumstance and matters set out in section 7A (1) and 7(E) of AML Act and for the purpose of conducting CDD as required under section 7A (2) of AML Act, 2010 the company shall comply with sections 9-25 of SECP AML/CFT Regulations, 2020.

(1) The company shall not enter into a business relationship or conduct any transaction with a customer who is anonymous or provides a fictitious name. The company shall take steps to ensure that its customers are who they purport themselves to be.

(2) Relevant staff shall apply CDD measures when establishing business relationship with a customer and when there is doubt about the veracity or adequacy of previously obtained customer identification data.

(3) Customer due diligence (CDD) in broader term include-

(a) The company shall verify the identification of customer using reliable independent source documents, data or information including verification of CNICs from NADRA Verysis /Biometric. Similarly, identify and verify the customer's beneficial owner(s) to ensure that the company understands who the ultimate beneficial owner is and shall obtain such documents from different type of customers as set out in Annexure-1.

(b) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and

(c) Monitoring of accounts / transactions on on-going basis to ensure that the transactions being conducted are consistent with the staff's knowledge of the customer, the customer's business and risk profile, including, the source of funds and, updating records and data/ information to take prompt action when there is material departure from usual and expected activity through regular matching with information already available.

(4) The company should verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or may complete verification after the establishment of the business relationship, provided that-

(a). this occurs as soon as reasonably practicable;
(b). this does not interrupt the normal conduct of business; and
(c). the ML/TF/PF risks are effectively managed.

(5) Company shall not form business relationship with entities and/or individuals that are:

(a). designated under the United Nations Security Council Resolutions and adopted by the Government of Pakistan;

(b). proscribed under the Anti-Terrorism Act, 1997(XXVII of 1997); and

(c). Associates/facilitators of persons mentioned in (a) and (b)."

(6) Company shall adopt risk management procedures concerning the conditions under which a customer may utilize the business relationship prior to verification. The types of circumstances where the Company permits completion of verification after the establishment of the business relationship should be recorded in their CDD policies.

(7) For all accounts, staff person should determine whether the person is acting on behalf of a customer or the customer represented by an authorized agent or representative he should take reasonable steps and shall-

(a) Identify every person who acts on behalf of the customer,

(b) Verify the identity of that person using reliable and independent documents, data and information as set out in Annex-1.

(c) Verify the authority of that person to act on behalf of the customer.

(8) The company must assess each customer's risk to allow for correct application of EDD, Standard and simplified or special measures for PEPs and other designated categories as per regulations and shall categorize each customer's risk depending upon the outcome of the CDD process necessary minimum customer risk ratings categories are High, Medium and Low.

(9) Company shall maintain a list of all such customers/accounts where the business relationship was refused or needed to be closed on account of negative verification;

(10) Where the relevant staff unable to satisfactorily complete required CDD measures, account shall not be opened or existing business relationship shall be terminated and consideration shall be given if the circumstances are suspicious so as to warrant the filing of an STR in relation to the customer.

(11) Where company forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it may not pursue the CDD process, and shall file an STR.

(12) Government entities accounts shall not be opened in the personal names of the government officials and account which is to be operated by an officer of the Federal or Provincial or Local Government in his/her official capacity, shall be opened only on production of a special resolution or authority from the concerned administrative department or ministry duly endorsed by the Ministry of Finance or Finance Department/Division of the concerned Government.

Explanation: -

For the purposes of this regulation the expression "Government entities" includes a legal person owned or controlled by a Provincial or Federal Government under Federal, Provincial or local law.

2.7 Beneficial Ownership of Legal Persons and Legal Arrangements

(1) The Beneficial Owner is the natural person at the end of the chain who ultimately owns or controls the customer. Beneficial Owner as per AMLA means:

(a) natural person who ultimately owns or controls a customer or the natural person on whose behalf a transaction is being conducted; or

(b) natural person who exercises ultimate effective control over a legal person or legal arrangement

(2) The Company shall identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner by using reliable and independent document, data or sources of information as set out in aforementioned Annex 1, such that the company is satisfied that it knows who the beneficial owner is.

(3) For customers that are legal persons or legal arrangements, the company shall identify the customer and verify its identity by obtaining the following information in addition to the information required in Annex 1:

a. name, legal form and proof of existence;

b. the powers that regulate and bind the legal person or arrangement, as well as the names of the relevant persons having a senior management position in the legal person or arrangement; and

c. the address of the registered office and, if different, a principal place of business.

(4) For customers that are legal persons or legal arrangements, it is essential to for the company to understand the nature of the customer's business and its ownership and control structure.

For customers that are legal persons, the company shall identify and take reasonable measures to verify the identity of beneficial owners by:

(a) identifying the natural person(s) (if any) who ultimately has a controlling ownership interest (as defined under relevant laws) in a legal person; and

(b) to the extent that there is doubt under (a) as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural person(s) (if any) exercising control of the legal person or arrangement through other means; and

(c) where no natural person is identified under (a) or (b) above, the identity of the relevant natural person who holds the position of senior managing official.

For customers that are legal arrangements, the company shall identify and take reasonable measures to verify the identity of beneficial owners as follows:

a. for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);

b. for waqfs and other types of legal arrangements, the identity of persons in equivalent or similar positions as specified in (a).

c. Where any of the persons specified in (a) or (b) is a legal person or arrangement, the identity of the beneficial owner of that legal person or arrangement shall be identified.

(1) For the beneficial ownership in the context of natural person, where a natural person seeks to open an account in his/her own name, the company shall inquire whether such person is acting on his own behalf. However, in relation to student, senior citizens and housewife accounts (where doubt exists that the apparent account holder is acting on his own behalf) the company shall obtain a self-declaration along with evidence of source of income or source of funds with respect to the investment in securities and / or beneficial ownership of funds from the customer and perform further due diligence measures accordingly.

(2) The company may adopt a risk-based approach to the verification of beneficial ownership of a customer. Identifying beneficial ownership of a customer is an obligation that must be satisfied, regardless of the level of risk associated with that customer. However, the reasonable steps to take to verify the identity and information depend upon on the risk assessment of the customer.

(3) The company shall assess different levels of money laundering/terrorism financing risks posed by its customers' beneficial owners. For example, the company should consider whether a beneficial owner is a politically exposed person or has links with a high-risk country or region.

2.8 On-Going Monitoring / Customer Due Diligence

For TSBL Customer Due Diligence (CDD) is not a one-time exercise at the time of on boarding/account opening only. In order to guard against misuse of our good office against criminal transactions, the company need to be vigilant at all the times and once the identification procedures have been completed and the business relationship is established, the company shall monitor the conduct of the business relationship to ensure that it is consistent with the nature of business stated when the relationship / account was opened. The Company shall conduct ongoing monitoring of its business relationship with its customers on an ongoing basis however; the frequency for ongoing monitoring period shall be quarterly. Whereas transactions and activity of the customer's shall be monitored on continuous basis and enhance monitoring by increasing the number and timing of controls applied on "High Risk" customers. Ongoing monitoring helps the company to keep the due diligence information up-to-date, review and adjust the risk profiles of the customers, where necessary.

(1) The Company shall conduct ongoing due diligence on the business relationship, including:

(a) scrutinizing transactions undertaken throughout the course of relationship to ensure that the transactions being conducted are consistent with the company's knowledge of the customer, their business and risk profile, including where necessary, the source of funds;

(b) Examining the background and purpose of all complex and unusual transactions that have no apparent economic or visible lawful purpose. The background and purpose of the transactions will be inquired by the customer and findings shall be documented with a view to making this information available to the relevant competent authorities, when required.

(c) Carrying our reviews of existing records and ensuring that documents, data or information collected for the CDD purposes is kept up-to-date and relevant, particularly for higher risk categories of customers.

(2) In relation to sub-regulation (b), the company shall review and revise the profiles of the customers keeping in view the CDD and basis of revision shall be documented.

(3) Additionally, The Company will assess the effectiveness of its risk mitigation procedures and controls, identify areas for improvement and update their systems as appropriate to suit the change in risks. This allows them to manage their AML/CFT/PF risk effectively. For this purpose, the Company monitors:

a) changes in customer profile or transaction activity/behavior in the normal course of business including incidents related to suspicious transactions and terrorist financing sanctions (TFS);

b) changes in risk relative to countries and regions to which the company or its customers are exposed;

c) the potential for abuse of products and services because of their size, unusual patterns, ambiguity and complexity;

d) deficiencies in internal cooperation and coordination mechanisms, and employee awareness of their roles in AML/CF/PF compliance and other functions/areas; and

e) selection, training and performance of agents, intermediaries and third parties who are in any way involved in the AML/CFT/PF processes of the Company.

(4) The Company shall ensure that CDD data or information is kept up-to-date by undertaking routine reviews of existing records. The Company shall consider updating customer CDD records within the time frames set by the Company's based on the level of risk posed by the customer or on the occurrence of a triggering event, whichever is earlier. Examples of triggering events include:

(a) Material changes to the customer risk profile or the way that account usually operates;

(b) Company lacks sufficient or significant information on a particular customer;

(c) Where a significant transaction takes place;

(d) Where there is a significant change in customer documentation standards;

(e) Significant changes in the business relationship;

(f) Transaction restructuring to circumvent the applicable threshold

(5) Annexure 4 and 5 gives some examples of potentially suspicious activities or "red flags" for ML/TF/PF, enabling the Company to recognize possible ML/TF/PF schemes. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is unusual or suspicious or one for which there does not appear to be a reasonable business or legal purpose.

(6) In case a customer has no active business with the Company, and cannot be reached, or refuses to engage in updating because there is no active business, the Company shall mark the account inactive with the instruction that relationship cannot be re-activated without full CDD.

(7) In case due diligence cannot be updated, a formal ending of the relationship should be done by following the legal process for ending a customer relationship under the applicable laws.

(8) Regulation encouraged to invest in computer systems for transactions monitoring specifically designed to assist the detection of ML/TF/PF. It is recognized that this may not be necessary in a risk-based approach. In such circumstances, The Company shall ensure that it has alternative systems in place for conducting on-going monitoring.

(9) Alternate or manual systems of ongoing monitoring may rely on Compliance Officer generated lists or instructions and regular lists generated from IT system such as:

(a) High transaction list for each day;

(b) Periodic list of transactions over determined thresholds;

(c) Periodic list of new clients and relations closings;

(d) Monthly or yearly lists of inactive clients;

(e) Ad Hoc reviews, meaning reviews triggered by an event, new information from supervisors and media reports.

(10) The Company shall implement the measures as set out in 7D of the AML Act.

(11) The Company shall comply with the provisions of the AML Act and rules, regulations and directives issued thereunder for reporting suspicious transactions/currency transactions in the context of money laundering or financing of terrorism.

(12) Where the Company files an STR with respect to a customer with whom it has an existing business relationship, and if the regulated person considers it appropriate to retain the customer, then the company shall;

(a). substantiate and document the reasons for retaining the customer; and

(b). subject the business relationship to proportionate risk mitigation measures, including enhanced ongoing monitoring.

(6) The basis of deciding whether an STR is being filed or not shall be documented and kept on record together with all internal findings and analysis done in relation to a suspicion irrespective of the fact that transaction is subsequently reported or not.

(7) The Company shall perform ongoing monitoring of the business relationships with the customers on real time basis and periodically after each quarter.

2.9 Due Diligence of Existing Customers

(1) The Company shall also apply CDD requirement to its existing customers on the basis of materiality and risk and should conduct due diligence on existing relations at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

(2) The CDD requirements mean that if the company has a suspicion of ML/TF/PF or becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

(3) The Company is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile.

(4) For existing customers who opened accounts with old NICs, the Company shall ensure that attested copies of identity documents shall be present and attached with account opening forms. The Company shall block accounts without identity document (after serving one-month prior notice) for all withdrawals, until the subject regulatory requirement is fulfilled. However, upon submission of attested copy of identity document and verification of the same from NADRA or biometric verification, the block from the accounts shall be removed.

(5) For customers whose accounts are dormant or in-operative, withdrawals shall not be allowed until the account is activated on the request of the customer. For activation, the Company shall conduct NADRA Verisys or biometric verification of the customer and obtain attested copy of customer's valid identity document (if already not available) and fulfill the regulatory requirements.

(6) If the Company has a suspicion of ML/TF/PF or becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

(7) Finally, the Company should entertain filing a Suspicious Transaction Report it there are any indicators that support such an action.

2.10 Enhanced Due Diligence (EDD) Procedures

Enhance Due Diligence (EDD) is additional procedure needed for higher risk customers, customers that pose higher Money Laundering/Terrorist Financing and / or Proliferation Financing risks and thus present increased exposure to the Company. This includes situations where the Company consider (based on risk assessment) that the level of risk involved is such that Enhanced Customer Due Diligence should apply. In such conditions the Company shall consider high risk classification factors, apply Risked Based Approach and use increased or more sophisticated measures to obtain and verify customer's details, their Beneficial Ownership structure and take reasonable steps to do this according to the level of risk involved. For this purpose, the Company shall comply with SECP AML/CFT/PF Regulations, 2020 and Guidelines and shall;

(1) Implement appropriate internal risk management systems, policies, procedures and controls to determine where the risks of ML/TF/PF are higher, if any customer presents high risk of ML/TF/PF or in case of unusual or suspicious activity the Company shall obtain and verify information relating to the source of wealth (SoW) or source of funds (SoF) of the customer and apply Enhance Due Diligence "EDD" and in particular, increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious including but not limited to the following circumstances:-

a). business relationships and transactions with natural and legal persons when the ML/TF/PF risks are higher;

b). business relationships and transactions with natural and legal persons from countries for which this is called for by the FATF;

c). PEPs and their close associates and family members.

(2) Examples of EDD measures that could be applied for high-risk business relationships include but shall not be limited to the following measures: -

(a) Obtaining additional information on the customer (e.g., volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner;

(b) Obtaining additional information on the intended nature of the business relationship;

(c) Obtaining information on the source of funds or source of wealth of the customer;

(d) Obtaining information on the reasons for intended or performed transactions.

(e) Obtaining the approval of senior management to commence or continue the business relationship;

(f) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

(3) The Company shall obtain appropriate information and/or supporting documents (anyone from the customer as per list below) to establish source of wealth and funds as specified by SECP.

a) Employment Income: • Last month/recent pay slip; • Annual salary and bonuses for the last couple of years; • Confirmation from the employer of annual salary; • Income Tax Returns/ Wealth Statement.	**b) Business Income/ Profits / Dividends** • Copy of latest audited financial statements; • Rental statements • Dividend statements
c) Savings / deposits/ assets/property: • Statement from financial institution • Bank Statement • Taxation returns • Accountant's statements • Property ownership certificate • Share certificates	**d) Inheritance:** • Succession Certificate.
e) Sale of Property/ Business: • Copy of sale agreement/Title Deed	**f) Loan** • Loan agreement
g) Gift: • Gift Deed; • Source of donor's wealth; • Certified identification documents of donor.	**h) Other income sources:** • Nature of income, amount, date received and from whom along with appropriate supporting documentation. • Where their nature of income is such that no supporting documentation is available (for e.g., Agricultural Income) Bank Statement may be obtained.

Note: The extent to documentation required for EDD would depend on the level of risk involved.

Disclaimer: This list is indicative only and non-exhaustive. The examples provided may serve only as guidance.

(4) In relation to herein above 2.6(1) (c) the company shall implement appropriate internal risk management systems, to determine if a customer or a beneficial owner is a Politically Exposed Person "PEP" or a close associate or a family member of PEP, both prior to establishing a business relationship or conduction a transaction, and periodically throughout the course of business relationship. The company shall apply, at minimum the following EDD measures:

(a) obtain approval from senior management to establish or continue a business relationship where the customer or a beneficial owner is a PEP, close associate or family member of a PEP or subsequently becomes a PEP, close associate and family member of a PEP;

(b) take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as a PEP, close associate or family member of a PEP; and

(c) Conduct enhanced ongoing monitoring of business relations with the customer or beneficial owner identified as a PEP, close associate and family member of a PEP.

(5) In case of low-risk customer, the regulated person should obtain information of source of income however, no specific evidence is required. In case of high-risk customers, where EDD is required, evidence of source of income may be requested from the customer.

(6) However, enhanced CDD could be required again as a result of any material changes in Company's business relationship with its customer or due to ongoing CDD and account monitoring.

2.11 Politically Exposed Persons (PEPs).

(1) "Politically Exposed Persons" or "PEPs" means an individual who is or has been entrusted with a prominent public function either domestically or by a foreign Country, or in an international organization and includes but not limited to:

(i). for foreign PEPs, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations and political party officials;

(ii). for domestic PEPs, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, political party officials;

(iii). for international organization PEPs, members of senior management or individuals who have been entrusted with equivalent functions.

(2) Provided that middle ranking or more junior individuals in the above referred categories are not included in the definition of PEPs;

(3) In relation to PEPs and their close associates and family members, the company shall implement appropriate internal risk management systems, to determine if a customer or a beneficial owner is a PEP or a close associate or family member of a PEP, both prior to establishing a business relationship or conducting a transaction, and periodically throughout the course of business relationship. The company shall apply, at minimum the following EDD measures:

(a) obtain approval from senior management to establish or continue a business relationship where the customer or a beneficial owner is a PEP, close associate or family member of a PEP or subsequently becomes a PEP, close associate and family member of a PEP;

(b) take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as a PEP, close associate or family member of a PEP; and

(c) conduct enhanced ongoing monitoring of business relations with the customer or beneficial owner identified as a PEP, close associate and family member of a PEP.

(4) Business relationships with family members or close associates of PEPs involve reputation risks and/or legal risk similar to those PEPs themselves. The Company shall evaluate the risks to its business operations when dealing with PEPs.

Explanation:

a. Family members of a PEP are individuals who are related to a PEP either directly (family relationship) or through marriage or similar (civil) forms of partnership.

b. Close associates to PEPs are individuals who are closely connected to PEP, either socially or professionally.

2.12 Risk Classification Factors

Business relationships always come with associated risks that require carefully implemented measures to deal with and Risk Classification is an important parameter of the risk-based KYC approach. A risk rating helps the Company in deciding how and when to apply the appropriate checks, treatment and controls that commensurate to the level of risk. This methodology is also known as the risk-based approach which allows the company to prioritize resources accordingly to areas that require more attention. The Company implemented AML/CFT/PF regulations and Guidelines to incorporate customer due diligence in order to comply international standards based on the risk associated with existing and potential customers. When opening customer accounts or establishing business relationship with the customer(s) the Company performs risk assessment each customers risk to allow for correct application of enhanced due diligence, standard, simplified or special measures for PEPs and consider that the accounts could be used for "Money Laundering /Terrorist Financing and / or Proliferation Financing and classify the customers in different risk categories i.e. Low Risk, Medium Risk and High Risk as per the regulations relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels.

High-Risk Classification Factors

2. Customer Risk Factors

The Company shall describe all types or categories of customers that it provides business to and should make an estimate of the likelihood that these types or categories of customers will misuse the Company for ML/TF/PF, and the consequent impact if indeed that occurs. High Risk customers are those who are engaged in certain professions or avail the Company's product and services where Money Laundering possibilities are high. Customer identification situations that present a higher ML/TF/PF risk might include, but are not restricted to:

(a). The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the Company and the customer).

(b). Non-resident customers

(c). Non-Face to Face customers

(d). Legal persons or arrangements

(e). Companies that have nominee shareholders.

(f). Business that is cash-intensive and / or High-Risk Business Sectors such as Jewelers and Precious Stone Dealers, Real Estate Dealers and Developers.

(g). Unusual Account Activity

(h). The ownership structure of the customer appears unusual or excessively complex given the nature of the customer's business such as having many layers of shares registered in the name of other legal persons;

(i). Politically exposed persons and/or Close associates or Family members/ relatives of PEPs.

(j). Shell companies, especially in cases where there is foreign ownership which is spread across jurisdictions;

(k). Trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets.

(l). Requested/Applied quantum of business does not match with the profile / particulars of client

(m). Lawyers/Notaries/Accountants etc.

(n). High Net worth customers*

3. Country or Geographic Risk Factors

Country or geographical risk may arise because of the location of a customer, the origin of a destination of transactions of the customer, but also because of the business activities of the Company itself, its location and the location of its branched. Country or geographical risk, combined with other risk categories, provides useful information on potential exposure to ML/TF/PF. The factors that may indicate a high risk are as follow:

(a) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports by international bodies such as the FATF, as not having adequate AML/CFT/PF systems.

(b) Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.

(c) Countries identified by credible sources as having significant levels of corruption or other criminal activity.

(d) Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

(e) Jurisdictions as identified in Pakistan National Risk Assessment 2019 as high risk in which the customer and beneficial owner are based.

(f) Jurisdictions with respect to the threat of Money Laundering and Terrorist Financing subject to the judgment of the Company and validity of the documents obtained for the purpose of the client's profile and source of income.

4. Product, Service, Transaction or Delivery Channel Risk Factors

Comprehensive ML/TFPF risk assessment must take into account the potential risks arising from the products, services, and transactions that the company offers to its customers and the way these products and services are delivered. In identifying the risks of products, services, and transactions, the following factors should be considered:

(a) Anonymous transactions (which may include cash).

(b) Non-face-to-face business relationships or transactions.

(c) Payments received from unknown or un-associated third parties.

(d) International transactions, or involve high volumes of currency (or currency equivalent) transactions

(e) New or innovative products or services that are not provided directly by the Company, but are provided through channels of the institution;

(f) Products that involve large payment or receipt in cash; and

(g) One-off transactions.

The Company shall take appropriate steps in accordance with section 7F of AML Act, 2010, SECP AML/CFT Regulations, 2020 and Guidelines to identify, assess and understand its Money Laundering / Terrorist Financing and / or Proliferation Financing risks of the customers taking into account risk factors arising from Customer(s), Country or Geographic locations, type of product , services and transactions or delivery channels and on the outcome of risk assessment the Company categorizes / marks the Customer(s) as "High Risk" who has one or more of the above high risk factors and shall monitor perpetually for potentially suspicious activities.

EXPLANATION:

Non-Face to Face Customers

As per FATF Guidance on Digital Identity regarding Non-Face to Face business relationships, the Company not always classifies Non-Face to Face business relationships (i.e., customers who wish to open accounts through online facility) as Higher Risk for ML/TF/PF purpose. However, the Company applies Risk Based Approach and other potentially higher risk situations/factors while assessing customer risk to categorize the customer(s) as "High Risk".

High Net worth Individuals.

High net worth individuals are an attractive customer for the Company, may expose higher risk of financial transactions that may be illicit. There is no standard size of HNWI. The Company knows to whom it is offering its products and services, and can establish criterion for HNWI applicable to their particular business.

Company shall scrutinize HNWI customers to determine, whether they carry a higher risk of ML/FT/PF and require additional due diligence measures. Such scrutiny must be documented and updated as part of its Risk Assessment. However, the Company defined the following parameters for High-Net-Worth Individuals: -

Parameters for defining High Net Worth Individuals:

As per Company policy the Company shall determine High Net Worth Individuals with any of the following:

(a) In terms of Transactions (Any Customer who shall Net Buy of Rs. 50 Million within the ongoing monitoring period i.e. in a quarter and / or Fiscal Year shall be considered as High Net Worth Individual).

(b) In terms of Amount (Any Customer whose Net receipts will be Rs. 5 Million within the ongoing monitoring period i.e. in a quarter and / or Fiscal Year shall be considered as High Net Worth Individual).

2.13 Example Scenarios of Customer Types

Small and Medium Sized Enterprises: Small and medium business enterprise customers usually entail domestic companies with simple ownership structures. Most of these businesses deal with cash and multiple persons that can act on its behalf. The likelihood that funds deposited are from an illegitimate source is HIGH, since it can't be easily be identified and can have a major impact on a large number of SME customers. Thus, the risk assessment and risk rating result is HIGH.

International corporations: International corporate customers have complex ownership structures with foreign beneficial ownership (often). Although there are only a few of those customers, it is often the case that most are located in offshore locations. The likelihood of Money Laundering is High because of the limited number of customers of this type and the beneficial ownership could be questionable, with two criteria that in this scenario result in a possible risk impact of moderate and a moderate risk assessment.

2.14 Counter Measures against High-Risk Countries and Regions within Country

(1) Pursuant to recommendations by the National Executive Committee, when called upon to do so by FATF and as indicated by the Federal Government, the Company shall apply appropriate counter measures and EDD against high-risk countries that is proportionate to the risk indicated.

(2) Certain Countries or regions within Countries have a specific Higher AML/CFT risk profile. Examples are border regions, large goods transit points such as ports, or regions experiencing social unrest, that can be associated with specific crime patterns such as cash or people smuggling, drug trafficking, violent crimes, fraud and corruption, and consequently pose a higher potential risk to the Company. Conducting a business relationship with a customer from such a country/region exposes the Company to risk of channeling illicit money flows.

(3) The Company should exercise additional caution, and conduct enhanced due diligence on individuals and/or entities based in High-Risk countries / regions. The Company shall consult publicly available information to ensure that they are aware of the high-risk countries/territories. The Company should consider among the other sources, sanctions issued by the UN, the FATF High Risk and non-cooperative jurisdictions, the FATF and its regional style bodies (FSRBs).

(4) Complex legal structures may be created in jurisdictions specializing in obscuring the trail to Beneficial Owners and allowing easy creation of complex corporate vehicles, so called offshore jurisdictions. Companies engaging with foreign complex legal structures, or with local companies owned by such foreign legal structures, need to educate themselves on offshore financial centers and acquire adequate expertise to understand their customers' ownership structure up to the Beneficial Owner and be able to assess documents presented to them.

2.15 Simplified Due Diligence

(1) Where low risk is identified through adequate analysis of risk or where adequate checks and controls exist, the company may apply simplified or reduced Customer Due Diligence / Know Your Customer measures.

(2) The decision to rate a customer as low risk shall be justified in writing by the company and low risk cases may include but are not limited to the following-

(a). The Company provided that they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF recommendations and are supervised for compliance with those requirements;

(b). public listed companies that are subject to regulatory disclosure requirements to ensure adequate transparency of beneficial ownership;

(c). Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

(3) Subject to sub-regulations (2), low risk for Simplified Due Diligence measures are limited to the following-

(a). reducing the frequency of customer identification updates;

(b). reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold; and

(c). not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transaction or business relationship established:

Provided that Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

2.16 Reliance on Third Parties

(1) Under SECP AML/CFT Regulations, 2020, the Company may rely on a third party to conduct CDD on its behalf as set out in provisions 8-23 of these regulations, provided that the Company shall-

(a). Remain liable for any failure to apply such indicated CDD measures above;

(b). Immediately obtain from the Third Party the required information concerning CDD;

(c). Take steps to satisfy those copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay;

(d). Keep those copies of identification, and

(e). Satisfy itself that the Third Party is supervised by an AML/CFT regulatory authority or an equivalent foreign authority and has measures in place for compliance with AML Act obligation of CDD and record keeping.

(2) Where the Company person relies on a third party that is part of the same corporate group, the Company may deem the requirements of (1) to be met if:

(a). the corporate group applies CDD and record-keeping requirements in accordance with the AML Act and its associated regulations;

(b). the implementation of the requirements in paragraph (a) is supervised by an AML/CFT regulatory authority or an equivalent foreign authority; and

(c). the corporate group has adequate measures in place to mitigate any higher country risks.

(3) In addition to subsection (1), when determining in which country a third party may be based, the regulated person shall have regard to available information on the level of country risk.

(4) Notwithstanding any reliance upon a third party, the Company shall ultimately remain responsible for its AML/CFT obligations, including generating STRs and shall carry out ongoing monitoring of such customer itself.

Explanation:

1. When another financial sector's entity, e.g., a Bank or a Brokerage House, has already established a relationship with a customer, the Company may rely on the CDD performed by that other party. This only applies if the information and CDD is shared directly between the Company and the other entity.

2. The Company may rely on the initial CDD information provided by another financial institution in Pakistan, where the third party is regulated and supervised by SBP or SECP and where the Company can immediately obtain necessary information from the third party.

2.17 Targeted Financial Sanctions (TFS) / Sanction Compliance:

(4) Sanctions are prohibitions and restrictions put in place with the aim of maintaining or restoring international peace and security. They generally target specific individuals or entities, or particular sectors, industries or interests. They may be aimed at certain people and targets in a particular country or territory, or some organization or element within them.

(5) The term Targeted Financial Sanctions (TFS) means both assets and funds freezing and prohibitions to prevent assets or financial services from being made available, directly or indirectly, for the benefit of designated persons and entities, except as authorized by the Competent Authority i.e. Ministry of Foreign Affairs or Ministry of Interior/ National Counter Terrorism Authority (NACTA).

(6) The Company shall implement and undertake its TFS obligations to comply under the United Nations (Security Council) Act 1948 and resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing and /or Anti-Terrorism Act 1997 and any regulations made there under, including:

(a) The Company must make its Targeted Financial Sanctions (TFS) compliance program an integral part of its overall AML/CFT compliance program, and accordingly develop mechanisms, processes and procedures for screening and monitoring customers, potential customers and beneficial owners/associates of customers to detect any matches or potential matches with the stated designated/proscribed persons in the SROs and notifications issued by MoFA, NACTA and MoI.

(b) If during the process of screening or monitoring of customers or potential customers the Company finds a positive or potential match it shall immediately:

I. freeze the relevant funds and assets without delay the customer's fund/ policy or block the transaction, without prior notice if it is an existing customer in accordance with the respective SRO.

II. prohibit from making any funds or other assets, economic resources, or financial or other related services and funds in accordance with the respective SRO

III. Reject the transaction or attempted transaction or the customer, if the relationship has not commenced.

(c) In all cases referred to in (b), the company shall file a suspicious transaction report to the FMU in case that person is designated under United Nations Security Council Resolutions, or proscribed under the Anti-Terrorism Act, 1997 and simultaneously notify the Commission in the manner as may be instructed from time to time by the Commission.

(d) Implement any other obligations under the AML Act 2010, United Nations (Security Council) Act 1948 and Anti-Terrorism Act 1997 and any regulations made there under.

(7) The company shall not provide any financial services to proscribed/ designated entities and individuals or to those who are known for their association with such entities and individuals, whether under the proscribed/ designated name or with a different name. The company shall monitor its business relationships with the entities and individuals on a continuous basis and ensure that no such relationship exists directly or indirectly, through ultimate control of an account and where any such relationship is found, the company shall take immediate action as per law, including reporting to the FMU.

Explanation: -

For the purposes of this section the expression associates mean persons and entities acting on behalf of, or at the direction, or for the benefit, of proscribed/ designated entities and individuals that may be determined on the basis of appropriate screening of sanctions lists, disclosed nominee/beneficiary information, publicly known information, Government or regulatory sources or reliable media information, etc

(8) The Company shall maintain up to date data/MIS of all frozen assets/ funds, attempted or rejected transactions or account opening requests, and the same shall be made available to the Commission as and when required.

To avoid Targeted Financial Sanctions the Company should strongly focus corruption (bribery, proceeds of corruption & instances of corruption undermining AML/CFT/PF measures): Corruption (bribery of officials) to facilitate money laundering by undermining AML/CFT/PF measures, including possible influence by politically exposed persons (PEPs): e.g., investigating officials or private sector compliance staff in banks being bribed or influenced to allow money laundering to take place.

2.18 Record Keeping Procedures

The Anti-Money Laundering Act VII of 2010 section 2 defines "record" as follows:

(xxxii) "Record" includes the records maintained in the form of books or stored in a computer or any electronic device, or such other form as may be prescribed.

The AMLA Section 7C states the general record keeping requirements:

Every reporting entity shall maintain a record of all transactions for a period of at least five years following the completion of the transaction, and records of account files, business correspondence, documents, of all records obtained through CDD and the results of any analysis undertaken for a period of at least five years following the termination of the business relationship. Further, Section 7(4) requires the record to be maintained for a period of 10 years for submitted STRs and CTRs after reporting of the transaction:

"Every reporting entity shall keep and maintain all record related to Suspicious Transaction Reports and CTRs filed by it for a period of at least ten years after reporting of transaction under sub-sections (1), (2) and (3)."

The Company shall comply with the requirement of record keeping under AML Act, SECP AML/CFT Regulations, 2020 and follow SECP Guidelines to implement its obligation for keeping records as per its following policy and procedures: -

(1) The Company shall maintain records as set out in section 7C of the AML Act shall be sufficient to permit reconstruction of individual transactions including the nature and date of the transaction, the type and amount of currency involved and the customer involved in the transactions so as to provide, when necessary, evidence for prosecution of criminal activity.

(2) Where transactions, customers or instruments are involved in litigation or where relevant records are required by a court of law or other competent authority, the Company shall retain such records until such time as the litigation is resolved or until the court of law or competent authority indicates that the records no longer need to be retained.

(3) The Company shall ensure that all information obtained in the context of CDD is recorded, this includes:

(a) Documents provided by the customers(s) to the Company at the time of account opening / on-boarding when verifying the identity of the customer(s), Beneficial Owners and associates of the customer(s) i.e., Nominees, Joint Account Holders, Authorized Persons. Trustees, Board of Directors etc.

(b) Records relating to validation/verification of Customer(s) CNIC(s) along with their Beneficial Owner(s) and associates through NADRA Verisys /Biometric. (Validation/Verifications of CNICs shall also be attached with relevant Account Opening Forms / Customer Relationship Forms and soft copies in electronic form shall retain in system as per customers sub account numbers to ensure its availability for review).

(c) Transcription into the Company's own IT System of the relevant CDD information

(d) Account opening forms/Customer Relationship Forms, Know Your Customer forms any other documents and result of any analysis along with records of account files and business correspondence, shall be maintained and keep in record for a minimum period of (5) five years after termination of the business relationship.

(4) The Company shall maintain a comprehensive record of AML/CFT reports with respect to internal enquiries and reporting to FMU. Such documentation may include:

(a) the report itself and all its attached information / documents in copy;

(b) the date of the report;

(c) the person who made the report and the recipient

(d) any decision based on the STR for the specific customer or a group of customers

(e) any updating or additional documentation taken based on the report, and

(f) the reasoning underlying the decisions taken

(1) The Company shall maintain a list of all such customers/accounts where the business relationship was refused or needed to be closed on account of negative verification.

(1) The Company shall ensure, to timely available and shall provide, upon request, by the Commission, investigating or prosecuting agency and FMU, any record within 48 hours after the request has been made or such time as may be instructed by the relevant authority.

2.19 Compliance Program

(1) In order to implement compliance programs as set out in 7G of the AML Act, the Company shall implement the following internal policies, procedures and controls:

(a) compliance management arrangements, including the appointment of a compliance officer at the management level, as the individual responsible for the company's compliance with these Regulations, the AML Act and other directions and guidelines issued under the aforementioned regulations and laws;

(b) screening procedures when hiring employees to ensure the integrity and conduct, skills, and expertise of such employees to carry out their functions effectively;

(c) an ongoing employee training program; and

(d) an independent audit function to test the system.

(2) For purposes of (a) the Company shall:

(a) Appoint a Management level Officer as Compliance Officer who shall report directly to the board of directors or chief executive officer or committee;

(b) has timely access to all customer records and other relevant information which they may require to discharge their functions, as well as any other persons appointed to assist the compliance officer;

(c) be responsible for the areas including but not limited to-

i. ensuring that the internal policies, procedures and controls for prevention of ML/TF are approved by the board of directors of the regulated person and are effectively implemented;

ii. monitoring, reviewing and updating AML/CFT policies and procedures, of the regulated person;

iii. providing assistance in compliance to other departments and branches of the regulated person;

iv. timely submission of accurate data/ returns as required under the applicable laws;

v. monitoring and timely reporting of Suspicious and Currency Transactions to FMU; and

vi. such other responsibilities as the regulated person may deem necessary in order to ensure compliance with these regulations.

2.20 Screening and Training

(1) The Company shall create awareness amongst its employees on AML/CFT/PF & KYC/CDD through a robust training program that will include formal courses, workshops and newsletters. Such trainings shall incorporate current developments and changes to relevant guidelines as well as internal policies, procedures, processes and monitoring systems.

(2) The Company shall also utilise other avenues such as e-mails, display screens, posters etc. to disseminate compliance issues arising from new rules and regulations to all Staff members.

(3) The Company shall Develop and implement a comprehensive employee due diligence policy and procedure to be implemented/ carried out at the time of hiring all employees permanent, contractual, or through outsourcing. This shall include but not limited to verification of antecedents and screening procedures to verify that person being inducted/ hired has a clean history;

(4) Chalk out and implement suitable training program for relevant employees on annual basis, in order to effectively implement the regulatory requirements and Company's own policies and procedures relating to AML/CFT/PF. The employees training shall enable them to understand new developments, money laundering and financing of terrorism techniques, methods and trends. The training should also include their responsibilities relating to AML/CFT/PF.

2.21 INTERNAL AUDIT

- Incorporating compliance testing in their normal audit program.
- Reporting on results of the independent testing to the Board through the CEO as well as and the Audit Committee.
- Carrying out independent review of this policy and providing assurance to Board, Audit committee and management.

2.22 ALL STAFF MEMBERS

- Familiarising themselves with guidelines. Policies and best practices relating to their respective areas of responsibility.
- Implementing the measures and approaches diligently and to the best of their ability.
- Reporting any legal violations or other forms of misconduct in accordance with company policies and procedures.

2.23 National Risk Assessment: 2019 update:

The NRA reviews ML/TF/PF issues affecting the whole of Pakistan. It is based on information from suspicious transaction reports (STRs) and proceeds of crime asset recovery data. Information from government organizations, both domestic and international, also contributes to the NRA, and it provides a comprehensive overview of threats and crime trends. SECP encouraged using the NRA to stay informed about emerging threats and trends.

Pakistan faces a significant internal security threat which is eminent from the fact that more than 18,000 terrorist attacks have been perpetrated by terrorist organizations since 2001. But there has been an overall decrease in terrorist threats (from which TF risks emanate). The year 2018 was the fourth consecutive year where the number of terrorism incidents decreased. The declining trend of terrorism has been acknowledged by United Nations Security Council (UNSC) in its 22nd report issued by its Analytical Support and Sanctions Monitoring Team on 27th July 2018. In spite on the declining trend of terrorism, however, the updated assessment shows that the terrorist organizations within and outside Pakistan are still posing, to varying degrees, a TF threat to the country. In this regard 41 terrorist organizations were identified and analysed for which we have to be careful and vigilant in our brokerage house. Details are as follows:

No. of TOs	Risk	Names of Terrorist Organizations (TOs)
2	High	Daesh and TTP.
10	Medium High	AQ, JeM, JuD/ FIF, TTA, LeT, HQN, JuA, BLA, LeJ and BLF.
8	Medium	SSP, LeJ-Al-Almi, UBA, BRA, BLT, BRAS, HuA and Unknown.
21	Medium	Low

Jesh-ul-Islam, Lashkar-i-Islam, SMP, Lashkar-e-Balochistan, Balochistan Republican Guards, Self-radicalized (lone wolf) terrorists, Hazb-ul–Tehrir, Ahl-eSunnat Wal Jamat, Tehreek-e-Jafaria Pakistan, Jeay Sindh Mottahida Mahaz, Harkat-ul-Mujahideen, Tehreek - e- Taliban Swat, Al-Badar Mujahideen, Ansarul-Shariya, Balochistan Waja Liberation Army, Baloch Republican Party Azad, Balochistan United Army, Balochistan National Liberation Army, Balochistan Liberation United Front, Baloch Student Organization Azad, Balochistan Muslla Defa Tanzeem are the majority of the terrorist organization working in Pakistan.

Those national characteristics that can be exploited or abused for ML/TF purposes should be identified and understood with a view to apply effective AML/CFT measures. In the context of Pakistan, it is important to consider the following when assessing ML/TF risks.

Geography:

Pakistan's geographical landscape and porous borders increase its vulnerability to both ML and TF, heightening in particular Pakistan's TF risks associated to cash smuggling. Pakistan is bordered by India to the east, Afghanistan to the west, Iran to the southwest, and China in the far northeast. Pakistan has longest border with India (3,171 km) followed by Afghanistan (2,600 km) with elevation ranging up to 24,700 feet and Iran (909 km). It is separated narrowly from Tajikistan by Afghanistan's Wakhan Corridor in the northwest, and shares a maritime border with Oman. It has a 1,046 km coastline along the Arabian Sea and Gulf of Oman in the south.

Indian, Afghani and Iranian territory has also been used in past by anti-Pakistani groups to launch anti-state covert operations inside Pakistan. This makes both eastern and western borders vulnerable for ML and TF through drug trafficking, bulk cash movements, and other illicit forms of trade and we as a brokerage house have to be vigilant in this respect.

Afghan Diaspora:

Pakistan is host to approximately 1.4 million registered and 1.0 million unregistered Afghans. In 2007, Pakistan, Afghanistan and the Office of the United Nations of High Commissioner for Refugees (UNHCR) signed a tripartite agreement, which gave Afghan refugees the right to register and obtain a Proof of Registration (PoR) Card, identifying them as Afghan refugees eligible for protection and support through UNHCR under Pakistan refugee laws.

These Afghan refugees have been mostly settled in Khyber Pakhtunkhwa and Baluchistan for the last 40 years. Their children are educated and settled in Pakistan. Most second and third generation Afghan refugees are born in Pakistan and are culturally, economically and socially integrated. In some cases, they are also married to Pakistanis and the families are now integrated. In addition, the border areas of Khyber Pakhtunkhwa and parts of Baluchistan are highly active, with fast moving populations across the border because of common history, culture, language and blood ties. There are eight formal border crossings jointly managed by the Afghan and Pakistan governments, as well as many informal crossings, which remain permeable despite increased fencing and border management systems.

Conflict and Terror

The aftermath of 9/11 and the subsequent 'War on Terrorism' resulted in violence that cost Pakistan the lives of thousands and substantial financial and property losses. The mountainous terrain on the eastern and northern borders also provides isolated and largely hidden routes to organized international groups/organizations. Additionally, maritime frontiers remain vulnerable to illicit trade and trafficking as scores of trespassers are frequently apprehended for crossing into Pakistan "by mistake".

The risks maybe greatest in Baluchistan, which has the longest border among Pakistan's subnational units, and is relatively arid and unpopulated compared to the rest of Pakistan. Here, Baloch militants, who are largely secular nationalists, operate. Baluchistan has historically suffered from ethno-sectarian tensions and politically motivated violence, including violence from an active separatist movement. Separatist groups such as the BLA have targeted and killed ethnic Punjabi settlers and others as part of their terror reign.

Various armed Punjabi sectarian groups operate, and are more prevalent in the South. However, they carry out attacks in all provincial capitals, but especially Karachi and Quetta. In Sindh, the existence of economic conflicts among different ethnic groups has a negative effect on the law and order. There is a large Hazara Shia population in Quetta, the provincial capital, which has historically been a target for sectarian violence.

The numbers of Afghan refugees have been encouraged to return to Afghanistan since Operation Zarb-e-Azb and Radd-ul-Fasaad. Operation Zarb-e-Azb (June 2014) was launched against terrorist outfits operating from North Waziristan by the Pakistan Armed Forces. A comparison of pre- and post-Zarb-e-Azb security situation shows that Pakistan's security has considerably improved. Underscoring the success of Operation, the review identifies future challenges such as reforming the political status of Federally Administered Tribal Areas (FATA), ensuring economic security of its people and effective Pak-Afghan border management. In February 2017, the Pakistan Army had launched "Operation Radd-ul-Fasaad" across the country. The aim of this operation is

threefold: eliminating the residual threat of terrorism; consolidating the gains made thus far by military operations under Zarb-e-Azb; and de-weaponising society. However, due to the deteriorating security situation in Afghanistan, the number of refugees electing to return has declined in 2018 due to lack of security, inadequate education facilities, non-availability of clean water and housing facilities.

Ratings of ML threats by types of crimes

Type of Crime in Pakistan	ML Threat Rating	Domestic or Foreign ML
Illicit Trafficking in Narcotic Drugs and Psychotropic Substances;	H	Foreign
Corruption and Bribery;	H	Foreign
Smuggling; (Including in Relation to Customs and Excise Duties and Taxes);	H	Both
Tax Crimes (Related to Direct Taxes and Indirect Taxes);	H	Both
Illegal MVTS/Hawala/Hundi	H	Both
Cash Smuggling	H	
Both		
Terrorism, Including Terrorist Financing;	H	Both
Participation in an Organized Criminal Group and Racketeering	MH	Both
Trafficking in Human Beings and Migrant Smuggling;	MH	Both
Illicit Arms Trafficking;	MH	Domestic
Fraud and forgery;	MH	Domestic
Kidnapping, Illegal Restraint and Hostage-Taking;	MH	Foreign
Robbery or Theft;	MH	Domestic
Extortion;	MH	Domestic
Insider Trading and Market Manipulation	MH	Both
Cyber Crime	MH	Both
Sexual Exploitation, Including Sexual Exploitation of Children;	M	Both
Illicit Trafficking in Stolen and Other Goods	M	Both
Counterfeiting Currency;	M	Domestic
Counterfeiting and Piracy of Products;	M	Both
Murder, Grievous Bodily Injury;	M	Domestic
Environmental Crime;	ML	Both
Piracy;	ML	Both

The assessment examined which channels are being used, or are suspected of being used, for TF. For example, if funds are deposited into a bank account in Pakistan and then wired to an account in a foreign jurisdiction or vice versa, the channel being used is the banking sector. Alternatively, funds may have been raised in cash and physically carried by individuals to or from another jurisdiction.

The WB methodology rates TF threats using a scale of 5, low, medium-low, medium, medium-high and high, and assigns ratings to assessed TOs in respect of terrorism threat and its impact on TF.

The analysis of these threats was based on total Threat Intelligence. Data and other information were collected from both federal and provincial LEAs and from intelligence agencies by sending them threat assessment templates/questionnaires using the following assessment variables:

- Data on known terrorist acts and terrorists and organizations, including the number of cases registered, the number of causalities, and other adverse effects (if any), and the number of convictions.
- Future trends based on this information; including the expected future capabilities of TOs
- Data on TF cases, including cases registered, number of convictions, and financial recoveries made.
- Data on Designation/ proscription of TOs.
- Intelligence information on sources and channels used for income and movement of funds by TOs.
- Intelligence information on the direction of TF.

Currency exchanges / cash conversion: used to assist with smuggling to another jurisdiction or to exploit low reporting requirements on currency exchange houses to minimise risk of detection – e.g., purchasing of traveller's cheques to transport value to another jurisdiction.

Cash couriers / currency smuggling: concealed movement of currency to avoid transaction / cash reporting measures.

Structuring (smurfing): A method involving numerous transactions (deposits, withdrawals, transfers), often various people, high volumes of small transactions and sometimes numerous accounts to avoid detection threshold reporting obligations.

Use of credit cards, cheques, promissory notes etc. Used as instruments to access funds held in a financial institution, often in another jurisdiction.

Purchase of portable valuable commodities (gems, precious metals etc.): A technique to purchase instruments to conceal ownership or move value without detection and avoid financial sector AML/CFT measures – e.g., movement of diamonds to another jurisdiction.

Purchase of valuable assets (real estate, race horses, vehicles, etc.): Criminal proceeds are invested in high-value negotiable goods to take advantage of reduced reporting requirements to obscure the source of proceeds of crime.

Commodity exchanges (barter): Avoiding the use of money or financial instruments in value transactions to avoid financial sector AML/CFT measures – e.g., a direct exchange of heroin for gold bullion.

Use of Wire transfers: to electronically transfer funds between financial institutions and often to another jurisdiction to avoid detection and confiscation.

Underground banking / alternative remittance services (Hawala / hundi etc.): Informal mechanisms based on networks of trust used to remit monies. Often work in parallel with the traditional banking sector and may be outlawed (underground) in some jurisdictions. Exploited by money launderers and terrorist financiers to move value without detection and to obscure the identity of those controlling funds.

Trade-based money laundering and terrorist financing: usually involves invoice manipulation and uses trade finance routes and commodities to avoid financial transparency laws and regulations.

Gaming activities (casinos, horse racing, internet gambling etc.): Used to obscure the source of funds – e.g., buying winning tickets from legitimate players; using casino chips as currency for criminal transactions; using online gambling to obscure the source of criminal proceeds.

Abuse of non-profit organizations (NPOs): May be used to raise terrorist funds, obscure the source and nature of funds and to distribute terrorist finances

Investment in capital markets: to obscure the source of proceeds of crime to purchase negotiable instruments, often exploiting relatively low reporting requirements.

Mingling (business investment): A key step in money laundering involves combining proceeds of crime with legitimate business monies to obscure the source of funds.

Use of shell companies/corporations: a technique to obscure the identity of persons controlling funds and exploit relatively low reporting requirements.

Use of offshore banks/businesses, including trust company service providers: to obscure the identity of persons controlling funds and to move monies away from interdiction by domestic authorities.

Use of nominees, trusts, family members or third parties etc.: to obscure the identity of persons controlling illicit funds.

Use of foreign bank accounts: to move funds away from interdiction by domestic authorities and obscure the identity of persons controlling illicit funds.

Identity fraud / false identification: used to obscure identification of those involved in many methods of money laundering and terrorist financing.

Use "gatekeepers" professional services (lawyers, accountants, brokers: to obscure identity of beneficiaries and the source of illicit funds. May also include corrupt professionals who offer 'specialist' money laundering services to criminals.

New Payment technologies: use of emerging payment technologies for money laundering and terrorist financing. Examples include cell phone-based remittance and payment systems.

2.24 Reporting & Freezing of Funds AL-QAIDA/BAN ENTITIES

All customers shall be checked against the SECP letter Ref. No. SMD/SE/2(216)2010 dated September 22, 2010 and a Gazette Notification SRO No. 879(I) 2010 dated September 14, 2010 and SRO No. 880(I) 2010 dated September 15, 2010 from Ministry of Foreign Affairs, Government of Pakistan, for taking necessary action of freezing the funds of Al-Qaeda and Taliban related entities / individuals and List established and maintained by the 1267/1989/2253 Committee of United Nation regarding Taliban and Ban Entities.

2.25 Payment / Receipts of funds

Payment vouchers are prepared by the finance department personal after the invoices or bills are received. Payment shall only be processed after the Payment Voucher is approved by the relevant authority. The finance department maintains all necessary documents in order to make relevant entries in the finance software.

Moreover, the company has clearly defined on receipts and payments from clients through cross cheques only. The company does not deal in any sort of cash receipts exceeding Rs. 25000/- which if exceeds are to be reported to the stock exchange.

2.26 Handling & Reporting of suspicious cases

A few guidelines are given below on how to handle the situation on identifying a suspect.

- Avoid being excited or agitated on detecting a questionable person or transaction, but obtain enough information about the customer or person.
- Be courteous and diplomatic at all times.
- Handle suspected cases in the strictest confidence and information shared on a need-to-know basis with other members of the staff while such cases are being handled.
- The staff concerned shall ensure that the information gathered is treated as very confidential and discreetly report it to the Compliance Officer of the company. In case of TSBL's branch operations, then the staff shall only report it to the Branch Head, who in turn will discreetly report it to the compliance dept.
- Relevant employees shall comply with the provisions of the AML Act and rules, regulations and directives issued there under for reporting suspicious

- transactions/currency transactions in the context of money laundering or financing of terrorism.
- They shall implement appropriate internal policies, procedures and controls for meeting their obligations under the AML Act.
- Pay special attention to all complex and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions shall, as far as possible, be examined, the findings established in writing, and be available to assist the relevant authorities in inspection and investigation.
- The transactions, which are out of character, are inconsistent with the history, pattern, or normal operation of the account or are not commensurate with the level of income of a customer shall be viewed with suspicion, be properly investigated and referred to Compliance Officer for possible reporting to FMU under the AML Act.
- Note that STRs, including attempted transactions, should be reported regardless of the amount of the transactions; and, the CTRs should be reported for the transactions of rupees two million and above as per requirements of AML, Act.
- The basis of deciding whether an STR is being filed or not shall be documented and kept on record together with all internal findings and analysis done in relation to a suspicion irrespective of the fact that transaction is subsequently reported or not.
- The employees of Company are strictly prohibited to disclose the fact to the customer or any other that a STR or related information is being or has been reported to any authority, except if required by law.
- Staff without disclosing the contents of STRs, shall intimate to the Commission on bi-annual basis the number of STRs reported to FMU and the Company shall ensure that status report (indicating No. of STRs only) shall reach the AML Department from the seven days of close of each half year.

2.27 Examples of Suspicious Transactions

Examples of suspicious transactions are listed below. The list is non-exhaustive and only provides examples of ways in which money may be laundered through the capital market.

Unusual Transactions

1. Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.
2. The intensity of transactions for an inactive trading account suddenly increases without plausible reason.
3. The entry of matching buys and sells in particular securities, creating an illusion of trading. Such trading does not result in a bona fide market position, and might provide ‘cover’ for a money launderer.
4. Unusually short period of holding securities.
5. Frequent selling of securities at significant losses.
6. Structuring transactions to evade substantial shareholding.

Large Cash Transactions

7. The crediting of a customer's margin account using cash and by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.
8. Depositing large cash amounts in the reporting institution's multiple bank accounts in the same day

Transactions Incompatible with Customer's Financial Standing

9. A customer who suddenly starts making investments in large amounts when it is known to the Reporting Institution that the customer does not have the capacity to do
10. Transactions that cannot be matched with the investment and income levels of the customer.

Irregular Account Movement

11. Abnormal settlement instructions including payment to apparently unconnected parties.
12. A client whose account shows active movement of funds with low level of trading transactions.

Suspicious Behaviour/Demeanour

13. A customer for whom verification of identity proves unusually difficult and who is reluctant to provide details.
14. A group of unconnected customers who share a common correspondence address.

Suspicious Behaviour/Demeanour by an Employees of the Reporting

15. There may be circumstances where the money laundering may involve employees of Reporting Institution. Hence, if there is a change in the employees' characteristics e.g. Lavish lifestyles, unexpected increase in performance, etc. The Reporting Institution may want to monitor such situations.

2.28 CONSEQUENCES

A breach of the anti-money laundering and combating the financing of terrorism laws is a serious offence and could result in lengthy investigations, significant fines and criminal sanction (including imprisonment of employees).

2.29 REFERENCES

- This policy is line with the requirements of the Securities and Exchanges Commission of Pakistan (SECP) regulations on Anti-Money Laundering and Combating the financing of terrorism (AML/CFT).

Annexure-4

2.30 Red Flags / Indicators

A. ML/TF Warning Signs/ Red Flags

The following are some of the warning signs or "red flags" to which Company should be alerted. The list is not exhaustive, but includes the following:

(1) Customers who are unknown to the broker and verification of identity / incorporation proves difficult;

(2) Customers who wish to deal on a large scale but are completely unknown to the broker;

(3) Customers who wish to invest or settle using cash;

(4) Customers who use a cheque that has been drawn on an account other than their own;

(5) Customers who change the settlement details at the last moment;

(6) Customers who insist on entering into financial commitments that appear to be considerably beyond their means;

(7) Customers who accept relatively uneconomic terms, when with a little effort they could have a much better deal;

(8) Customers who have no obvious reason for using the services of the broker (e.g.: customers with distant addresses who could find the same service nearer their home base; customers whose requirements are not in the normal pattern of the service provider's business which could be more easily serviced elsewhere);

(9) Customers who refuse to explain why they wish to make an investment that has no obvious purpose;

(10) Customers who are introduced by an overseas agent based in a country noted for drug trafficking or distribution

(11) Customer trades frequently, selling at a loss

(12) Customers who constantly pay-in or deposit cash to cover requests for bankers' drafts, money transfers or other negotiable and readily marketable money instruments;

(13) Customers who wish to maintain a number of trustee or customers' accounts which do not appear consistent with the type of business, including transactions which involve nominee names;

(14) Any transaction involving an undisclosed party;

(15) transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral;

(16) Significant variation in the pattern of investment without reasonable or acceptable explanation

(17) Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting thresholds.

(18) Transactions involve penny/microcap stocks.

(19) Customer requests a securities provider to execute and/or clear a buy order and sell order for the same security or similar or correlated securities (and/or on behalf of the same beneficial owner), in close chronology.

(20) Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.

(21) Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.

(22) Customer invests in securities suddenly in large volumes, deviating from previous transactional activity.

(23) Customer conducts mirror trades.

Customer closes securities transaction before maturity, absent volatile market conditions or other logical or apparent reason.

B. Red Flags / Indicators on Associates Acting on Behalf of Proscribed / Designated Individuals or Entities.

The following actions and factors will help to identify suspected persons:

a). A customer is an office bearer (trustee/ member/ director/ authorized signatory etc.) of a designated/ proscribed entity.

b). A customer is a business partner of an office bearer (trustee/ member/ director etc.) of a designated/ proscribed entity.

c). A customer is a close family member of a designated/ proscribed individual who is also suspected to be associated with the business of the designated/ proscribed individual by way of financial or other assistance.

d). An entity has a designated/ proscribed individual on its board or management.

e). Unilateral sanctions listing *(i.e. NACTA Database for Proscribed individuals & entities)* identify linkage/ association of a customer with a designated/ proscribed individual or entity.

f). Media (Broadcast/ Print/ Social) news highlights customer's involvement in providing financial or other assistance to designated/ proscribed individual or entity.

g). Inquiry from law enforcement agency/ intelligence agency indicating linkage of a customer with designated/ proscribed individual or entity.

h). A customer appears to have conducted transactions on behalf of or at the direction of a designated/ proscribed individual during the process of due diligence.

C. Red Flags that specifically relate to Non-banking financial institutions (NBFIs)

a). The customer declares a proscribed person as a guarantor of loan or nominee of the customer.

b). Customer has obtained a loan from an NBFC, but the loan shall be utilized by a proscribed person.

c). Repayment of a loan to the customer is made by a proscribed person.

d). In case of Mutual Funds account to account transfer involving transfer to a proscribed individual or entity.

e). A customer who is refused financial services/ loan due to association with a proscribed person approaches another financial institution for securing a loan.

D. <u>Red Flags based on behaviour of an Account Holder associated with proscribed individuals or entities:</u>

a). A customer has provided the same residential/ office address that matches the known residential/ office address of a designated/ proscribed individual or entity.

b). A customer has provided the same personal contact number that matches the contact number provided earlier by a proscribed/ designated customer.

c). A customer depositing funds in the account of a person or entity listed in an international or foreign jurisdiction's sanctions lists maintained in accordance with UNSC resolution 1373.

d). A customer listed in an international or foreign jurisdiction's sanctions list maintained in accordance with UNSC resolution 1373, is depositing funds in another customer's account.

Annexure-5

2.31 Proliferation Financing Warning Signs/Red Alerts

The Company should take note of the following circumstances where customers and transactions are more vulnerable to be involved in proliferation financing activities relating to both DPRK and Iran sanctions regimes:

(a) customers and transactions associated with countries subject to sanctions;

(b) instruments that could particularly be used to finance prohibited transactions, such as certain trade financing products and services;

(c) customers involved with and/or transactions related to items, materials, equipment, goods and technology prohibited by UNSCRs;

(d) reasonableness of invoiced goods against market value, inconsistency or discrepancies in trade-related documentation.

In particular, the Company should be alert to the following non-exhaustive list of factors that are relevant to the DPRK sanctions regime:

(a) significant withdrawals or deposits of bulk cash that could potentially be used to evade targeted financial sanctions and activity-based financial prohibitions;

(b) opening of banking accounts by DPRK diplomatic personnel, who have been limited to one account each under relevant UNSCRs (including number of bank accounts being held, holding of joint accounts with their family members);

(c) clearing of funds, granting of export credits or guarantees to persons or entities that are associated with trading transactions relating to the DPRK;

(d) providing insurance or re-insurance services to maritime vessels owned, controlled or operated, including through illicit means, by the DPRK or classification services to vessels which there are reasonable grounds to believe were involved in activities, or the transport of items, prohibited by UNSCRs concerning the DPRK, unless the Security Council 1718 Committee determines otherwise on a case-by-case basis;

(e) direct or indirect supply, sale or transfer to the DPRK of any new or used vessels or providing insurance or re-insurance services to vessels owned, controlled, or operated, including through illicit means, by the DPRK, except as approved in advance by the Security Council 1718 Committee on a case-by-case basis; or

(f) the leasing, chartering or provision of crew services to the DPRK without exception, unless the Security Council 1718 Committee approves on a case-by-case basis in advance;38 or

(g) using real property that DPRK owns or leases in Pakistan for any purpose other than diplomatic or consular activities.

Red Flags indicators for Proliferation Financing

To identify a suspicion that could be indicative of proliferation financing activity, FMU has prepared the red flags indicators that are specially intended as an aid for the Company. These red flags may appear suspicious on their own; however, it may be considered that a single red flag would not be a clear indicator of potential proliferation financing activity. A combination of these red flags, in addition to analysis of expected overall financial activity, business profile may indicate towards potential proliferation financing activity.

Customer Behaviour:

1. When customer is involved in the supply, sale, delivery or purchase of dual-use proliferation-sensitive or military goods, particularly to higher risk jurisdictions.
2. When customer or counter-party, or its address, is the same or similar to that of an individual or entity found on publicly available sanctions lists.
3. The customer is a research body connected with a higher risk jurisdiction of proliferation concern.
4. When customer's activities do not match with the business profile provided to the reporting entity.
5. When customer is vague about the ultimate beneficiaries and provides incomplete information or is resistant when requested to provide additional information.
6. When customer uses complicated structures to conceal connection of goods imported / exported, for example, uses layered letters of credit, front companies, intermediaries and brokers.
7. When a freight forwarding / customs clearing firm being listed as the product's final destination in the trade documents.
8. When final destination of goods to be imported / exported is unclear from the trade related documents provided to the reporting entity.

Transactional Patterns:

1. Project financing and complex loans, where there is a presence of other objective factors such as an unidentified end-user.
2. The transaction(s) involve an individual or entity in any country of proliferation concern.
3. The transaction(s) related to dual-use, proliferation-sensitive or military goods, whether licensed or not.
4. The transaction(s) involve the shipment of goods inconsistent with normal geographical trade patterns i.e., where the country involved does not normally export or import or usually consumed the types of goods concerned.
5. Over / under invoice of dual-use, proliferation-sensitive or military goods, trade transactions.
6. When goods destination/shipment country is different from the country, where proceeds are sent/ received without any plausible reason.