TRUST SECURITIES & BROKERAGE LTD

ANTI-MONEY LAUNDERING & COMBATING THE FINANCING OF TERRORISM POLICY & PROCEDURES

1.2 VERSION

TABLE OF CONTENTS

FOREWARD
POLICY COMPLIANCE
POLICY REVISION

1. INTRODUCTION. (SECTION A)
1.1 PURPOSE.
1.2 SCOPE
1.3 RESPONSIBILITY
1.4 REVIEW AND CHANGES
1.5 DATE OF NEXT REVIEW
1.6 GENERAL DEFINATION
1.7 THE MONEY LAUNDERING OFFENCE UNDER SECTION 3 OF AML ACT 2010
1.8 PUNISHMENT OF MONEY LAUNDERING UNDER SECTION 4 OF AML ACT 2010
1.9 NATIONAL EXECUTIVE COMMITTEE TO COMBAT MONEY LAUNDERING

2. ROLES & RESPONSIBLITIES (SECTION B)
2.1 ACCOUNT OPENING (KYC/CDD/AML/CFT) PROCEDURES
2.2 VERIFICATION OF DOCUMENTS
2.3 CUSTOMER DUE DILIGENCE.
2.4 ON GOING DUE DILLIGENCE
2.5 ENHANCED DUE DILLIGENCE
2.6 SIMPLIFIED DUE DILLIGENCE
2.7 RISK ASSESMENT
2.8 RISK MITIGATION & APPLYING RISK BASED APPROACH
2.8(I) HIGH RISK CLASSIFICATION FACTORS
2.9 NEW PRODUCTS, PRACTICES AND TECHNOLOGIES
2.10 BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS
2.11 NATIONAL RISK ASSESSMENT: 2019 UPDATE
2.12 TARGETED FINANCIAL SANCTION (TFC)
2.13 POLITICALLY EXPOSED PERSONS (PEPS)
2.14 REPORTING & FREEZING FUND OF AL-QAIDA/BAN ENTITIES
2.15 POLITICALLY EXPOSED PERSONS (PEPs).
2.16 BUSINESS RELATIONS WITH (PEPs)
2.17 RECORD KEEPING
2.18 PAYMENTS/RECEIPTS OF FUNDS
2.19 HANDLING & REPORTING OF SUSPICIOUS CASES
2.20 EXAMPLE OF SUSPICIOUS TRANSACTIONS
2.21 SCREENING AND TRAINING
2.22 COMPLIANCE OFFICER (APPOINTMENT & RESPONSIBLITIES)
2.23 INTERNAL AUDIT
2.24 ALL STAFF MEMBERS
2.25 CONSEQUENCES.
2.26 REFERENCES

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 Dept. 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 documents as per the document check list. The Authorized Account Opening Officer shall ensure that the following customer information is collected.

Individual/ Sole proprietorship	Partnership	Institutions/ Corporates
▪ Copy of CNIC of Principal and Joint holders/ NICOP for Non-Residential Pakistanis ▪ Passport for Foreign Nationals ▪ Evidence of sources of Income ▪ Business/ Employment Proof ▪ NTN Certificate (If available) ▪ Nominee details (Not in case of Joint holders) ▪ Proof of ownership of mobile number in the name of investor.	▪ Name of Partnership and Partners ▪ Copy of CNIC/NICOP of all Partners ▪ Partnership Deed ▪ Copy of Latest Financials ▪ Certificate of Registration (If registered partnership firm) ▪ NTN Certificate	▪ Name of Directors and Officers ▪ Registered Address ▪ Copy of CNIC/NICOP of all Directors and Authorized Signatories ▪ Certificate of Incorporation ▪ Certificate of Commencement of Business ▪ Certified copy of Board Resolution ▪ Memorandum & Articles of Association/ Bye Laws/ Trust Deed ▪ Audited Accounts of the Institutions/ Corporates
Trust	**Club Societies and Associations**	**Executors/ Administrations**
▪ Copy of CNIC of all Trustees ▪ Certified copy of Trust Deed ▪ Copy of Latest Financials of the Trust ▪ Document Evidence of Tax Exemption (If any)	▪ List of Members of Governing Body ▪ Copy of CNIC/ NICOP of Members of Governing Body	▪ Copy of CNIC of all Executors/ Administrators ▪ Certified Copy of Letter of Administration
▪ Trustee/ Governing Body Resolution	▪ Certified Copy of Certificate of Registration ▪ Certified Copy of by-laws/ Rules and Regulations ▪ Copy of Latest Financials of Society/Association	

2.2.1 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 Customer Due Diligence

(1) No person shall open or maintain anonymous account or an account in fictitious name.

(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) Identifying the customer or beneficial owner and verifying the customer's/beneficial owner's identity on the basis of documents, data or information obtained from customer and/or from reliable and independent sources;

(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 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 and should take reasonable steps to obtain-

(a). evidence to determine authority of such person to act on behalf of the customer, which shall be verified through documentary evidence including specimen signature of the customer;

(b). identification and verification of the person purporting to act on behalf of the customer;

(c). identification and verification of the customer;

(8) Each customer shall be categorized as high or low risk, depending upon the outcome of the CDD process;

(9) Company will 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) Company is required to 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;

(11) Where house employees person are 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.

(12) 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 instead should file an STR in accordance with regulation 14.

(13) 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.

2.4 On-Going Due Diligence

For TSBL Customer Due Diligence (CDD) is not a one-time exercise at the time of account opening only. In order to guard against misuse of our good office against criminal transactions, we need to be vigilant at all the times, and keep monitoring transactions of our customers to ensure that the transactions executed in any particular account are within the understanding of company in terms of the customer's profile, risk category, historical pattern of the transactions and their historic funding source. For example, if a domestic individual customer orders a transaction that is significantly different from the average historical transaction size, company has to became alert and be satisfied that no suspicious reportable activity is taking place. Similarly, if a regular domestic customer, all of a sudden shows foreign sources of funds, this is likely to require further investigation by Company.

(1) All business relations with customers shall be monitored on an ongoing basis to ensure that the transactions are consistent with the Company's knowledge of the customer, its business and risk profile and where appropriate, the sources of funds.

(2) Background and purpose of all complex and unusual transactions, which have no apparent economic or visible lawful purpose and the background and purpose of these transactions, shall be inquired and findings shall be documented with a view of making this information available to the relevant competent authorities when required.

(3) Company staff shall periodically review the adequacy of customer information obtained in respect of customers and beneficial owners and ensure that the information is kept up to date and relevant, by undertaking reviews of the existing records, particularly for higher risk categories of customers and the review period and procedures thereof should be defined by company, as per risk based approach.

(4) In relation to sub-regulation (3), customers' profiles should be revised keeping in view the spirit of Know Your Customer/CDD and basis of revision shall be documented and customers may be consulted, if necessary.

(5) Where company files an STR on reasonable grounds for suspicion that existing business relations with a customer are connected with ML/TF the company may considers it appropriate to retain the customer-

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

(b). the customer's business relations with the company shall be subject to proportionate risk mitigation measures, including enhanced ongoing monitoring.

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

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

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

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

2.5 Enhanced Due Diligence (EDD)

(1) The Company shall implement appropriate internal risk management systems, policies, procedures and controls to determine if any customer presents high risk of ML/TF.

(2) For the purposes of sub-regulation (1), circumstances where a customer presents high risk of ML/TF include but are not limited to the following:-

(a). customers belonging to countries which are non-compliant with anti-money laundering regulations according to FATF;

(b). such body corporate, partnerships, associations and legal arrangements including non-governmental organizations or not-for-profit organizations which receive donations; and

(c). legal persons or arrangements with complex ownership structures.

(3) The Company shall perform EDD proportionate to risk posed to the business relationship by the customers that are identified as high risk or are notified as such by the Commission.

(4) EDD measures include but are not limited to the following:-

(a). obtain approval from Company senior management to establish or continue business relations with such customers;

(b). establish, by appropriate means, the sources of wealth and/or funds or beneficial ownership of funds, as appropriate; including company's own assessment to this effect; and

(c). Conduct enhanced monitoring of business relations with the customer during the course of business relations.

2.6 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.

(1) 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.

2.7 Risk Assessment

(2) The relevant departments of company shall take appropriate steps to identify, assess and understand, its money laundering and terrorism financing risks in relation to:

(b). its customers;
(c). the jurisdictions or countries its customers are from or in;
(d). the jurisdictions or countries the Company has operations or dealings in;
(e). the products, services, transactions and delivery channels of the Company.

(3) The appropriate steps referred to in sub-regulation (1), shall include-

(a). documenting the Company risk assessments;
(b). considering all the relevant risk factors before determining the level of overall risk and the appropriate type and extent of mitigation to be applied;

(c). keeping the risk assessments up-to-date;
(d) Categorizing the overall entity level risk as high, medium or low based on the result of risk assessment; and
(e) Having appropriate mechanisms to provide its risk assessment information to the Commission.

2.8 Risk Mitigation and Applying Risk Based Approach

The Company must implement following counter ML and TF measures, with regard to the ML and TF 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 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; and

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

2.8(I) Examples of Risk Classification Factors

Below are some examples that can be helpful indicators of risk factors/indicators that may be considered while assessing the ML/TF risks for different risk categories relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels.

High-Risk Classification Factors

(1) ***Customer risk factors***: The institution will 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 RP for ML or TF, and the consequent impact if indeed that occurs. Risk factors that may be relevant when considering the risk associated with a customer or a customer's beneficial owner's business include:

(a) The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the RP and the customer).
(b) Non-resident customers.
(c) Legal persons or arrangements
(d) Companies that have nominee shareholders.
(e) Business that is cash-intensive.
(f) 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;
(g) Politically exposed persons
(h) shell companies, especially in cases where there is foreign ownership which is spread across jurisdictions;
(i) trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets.
(j) Requested/Applied quantum of business does not match with the profile/particulars of client

(k) real estate dealers,
(l) dealers in precious metal and stones, and
(m) lawyers/notaries

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.

2.9 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.

2.10 Beneficial Ownership of Legal Persons and Legal Arrangements

(1) Where the customer is a legal person, in addition to other measures the Company shall acquire and use requisite information and data obtained from a reliable source, for the following purposes:

- understand the nature of the customer's business and its ownership and control structure.

- identify and verify the identity of the natural persons (whether acting alone or together) who owns or ultimately has controlling ownership interest in the legal person.

- where there is doubt under clause (b) as to whether the natural persons who ultimately own or have controlling ownership interest in the legal person are the beneficial owners or where no natural persons ultimately own or exert control through ownership interest in the legal person.

- Where no natural persons are identified under clause (b) or (c), identify the natural persons having executive authority in the legal person, or in equivalent or similar positions.

(2) Where the customer is a legal arrangement, the Company shall,

- for trusts, identify and verify the identity of the settlor, the trustee, the protector (if any), the beneficiaries (including every beneficiary that falls within a designated characteristic or class), and any natural person exercising ultimate ownership, ultimate control or ultimate effective control over the trust (including through a chain of control or ownership); and

- for other types of legal arrangements, identify and verify the identity of persons in equivalent or similar positions, as those described under clause (a).

2.11 **National Risk Assessment: 2019 update:**

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 analyzed 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 Balochistan 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 Balochistan 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 Balochistan, 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. Balochistan 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 Zarbe-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 Raddul-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.

2.12 **Targeted Financial Sanction (TFC)**:

The term targeted financial sanctions means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.

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

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 - eg purchasing of travellers 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, promisory 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 – eg 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 - eg 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 – eg 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 etc): 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.

We should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity.

2.13 Politically exposed persons (PEPs)

Business relationships with family members or close associates of PEPs involve reputation risks similar to those PEPs themselves. TSBL shall evaluate the risks to its business operations when dealing with PEPs. The following factors shall guide identification of PEPs' risk characteristics:

- Nature of the client and the client's businesses - The source of the client's wealth, the nature of the client's business and the extent to which the client's business history presents an increased risk for money-laundering and terrorist financing
- Purpose and activity – The size, purpose, services involved in the relationship
- Relationship – The nature and duration of TSBL relationship with the client
- Client's corporate structure
- Public information – Information is known or reasonably available to TSBL about the client

2.14 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.

2.15 Business Relations with Politically Exposed Persons (PEPs)

- In relations to foreign and domestic PEPs, Company shall implement appropriate internal risk management systems, policies, procedures and controls to determine if any customer or a beneficial owner is PEP.

- In case of foreign PEPs, Company shall perform EDD in accordance with sub-regulation (4) of regulation 9, in addition to other requirements of these regulations.

- In case of domestic PEPs, where business relationship poses higher risk, Company shall carry out EDD, in accordance with sub-regulation (4) of regulation 9 in addition to other requirements of these regulations.

- The requirements are also applicable on family members and close associates of foreign and domestic PEPs.

2.16 Record Keeping

- The Company Shall maintain all necessary records on transactions, both domestic and international, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions) for a minimum period of (5) five years from completion of the transaction:
- Provided that the Company may retain those records for longer period where transactions, customers or accounts involve litigation or it is required by court or other competent authority.
- The records 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 type and identifying number of any account involved in the transactions so as to provide, when necessary, evidence for prosecution of criminal activity and the transactions records may be maintained in paper or electronic form, provided it is admissible as evidence in a court of law.
- The records of identification data obtained through CDD process like copies of identification documents, account opening forms, Know Your Customer forms,

verification documents, other documents and result of any analysis along with records of account files and business correspondence, shall be maintained for a minimum period of (5) five years after termination of the business relationship.

- The Company shall ensure, to timely make available, all CDD and transaction records to the Commission, FMU and Law Enforcement Agencies whenever required.

2.17 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.

2.18 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.
-

2.19 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 Institution

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.

2.20 Screening and Training

TSBL shall create awareness amongst its employees on AML/CFT & 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.

TSBL 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.

TSBL 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;

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. 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.

2.21 COMPLIANCE OFFICER APPOINTMENT & RESPONSIBLITIES.

The Company shall,

(a). Appoint a Management level Officer as Compliance Officer, who shall report directly to the Board of Directors or to another equivalent executive position or committee;

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

(c). the compliance officer shall primarily be responsible for the areas including, but not limited to-

- the Company effective compliance with the relevant provisions of these Regulations, the AML Act, the Anti-Money Laundering Rules, 2008, the Anti-Money Laundering Regulations, 2015 and other directions and guidelines

issued under the aforementioned regulations and laws, as amended from time to time;

- ensuring that the internal policies, procedures and controls for prevention of ML/TF are approved by the board of directors of the Company and are effectively implemented;
- Monitoring, reviewing and updating AML/CFT policies and procedures, of the Company;
- providing assistance in compliance to other departments and branches of the Company;
- timely submission of accurate data/ returns as required under the applicable laws;
- monitoring and timely reporting of Suspicious and Currency Transactions to FMU; and
- such other responsibilities as the Company person may deem necessary in order to ensure compliance with these regulations.

2.22 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.

2.23 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.

2.24 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).

2.25 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).

_____