ADEEL & NADEEM SECURITIES (PVT.) LIMITED

AML/CFT Policy & Procedures & Controls

Table of Contents

Contents

ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM POLICIES & PROCEDURES

1. *Introduction Purpose and Scope*

These Policies and Procedures are in line with requirements of Anti Money Laundering and Countering Financing of Terrorism Regulations, 2018, the related Guidelines issued by the SECP and NRA 2019

These Policies and related Procedures establish the standards to which Adeel & Nadeem Securities (Pvt.) Limited (ANSPL) ("the Company") should adhere to. This document will be used to create an understanding amongst employees concerning the risks of Money Laundering and Terrorist Financing. Accordingly, the Company is required to adopt Risk-Based Approach ("RBA") to prevent the Company as a conduit for Money Laundering or Terrorist Financing activities

2. *Policy Statement*

The ANSPL is committed to fully comply with all applicable laws and regulations regarding anti money laundering procedures. ANSPL has adopted and will enforce the provisions set forth in AML/CFT Regulations in order to prevent and detect money laundering, terrorist financing and other illegal activities.

Therefore, it is imperative that every member, officer, director, and employee (each, an "Employee") is familiar with and complies with the policy and procedures set forth in this document.

This Compliance Statement is designed to assist all clients in adhering to ANSPL's policy and procedures, which, if followed diligently, are designed to protect themselves, ANSPL, its Employees, its facilities and its activities from money laundering or other illegal activities.

To ensure that the ANSPL's policies and procedures are adhered to, ANSPL shall designate an Anti-Money Laundering Compliance Officer (the "Compliance Officer"). The Compliance Officer is responsible for establishing and conducting Employee training programs to ensure that

all appropriate Employees are aware of the applicable AML/CFT Laws and Regulations, ANSPL's AML/CFT Policies & procedures and their responsibilities with respect to these policies.

To ensure that the ANSPL's policies and procedures are adhered to, ANSPL shall designate an Anti-Money Laundering Compliance Officer (the "Compliance Officer"). The Compliance Officer is responsible for establishing and conducting Employee training programs to ensure that all appropriate Employees are aware of the applicable AML/CFT Laws and Regulations, ANSPL's AML/CFT Policies & procedures, guidelines /information provided by NRA 2019, regulations about Red Flag indicators for misuse of legal person, Proliferation Financing Warning Signs/Red Alert and their responsibilities with respect to these policies.

3. *Objectives of ANSPL's Anti-Money Laundering / Counter Financing of Terrorism Policy and Procedures*

An effective Anti-Money Laundering and Countering the Financing of Terrorism **("AML/CFT")** regime requires financial institutions to adopt and effectively implement Appropriate ML and TF control processes and procedures, not only as a principle of good Governance but also as an essential tool to avoid involvement in ML and TF. AML and CFT Regime Is governed under "Governing Laws, Rules, and Regulations"

- Comply with all AML/CFT Rules & Regulations of the jurisdictions it operates in;
- Appointment of a Compliance Officer who shall ensure adherence to the ANSPL's AML/CFT Policy and Procedures;
- Require all Employees to prevent, detect and report to the Compliance Officer all potential instances in which ANSPL or its employees, its facilities or its activities have been or are about to be used for money laundering, terrorist financing and other illegal activities;
- Require all Employees to attend anti-money laundering training sessions, so that all such Employees are aware of their responsibilities under ANSPL's policies and procedures; and as affected by current developments with respect to anti-money laundering events.

4. *Guidelines On SECP AML/CFT Regulations*

The Guidelines are applicable to all Regulated Persons ("RPs") including Securities Brokers as defined under the SECP AML/CFT Regulations conducting relevant financial business and designed to assist RPs in complying with the Regulations. It supplements the Regulations and the AML/CFT regime by clarifying and explaining the general requirements of the legislation to help RPs in applying national AML/CFT measures, developing an effective AML/CFT risk assessment

and compliance framework suitable to their business, and in particular, in detecting and reporting suspicious activities

5. What is Money Laundering?

Money laundering involves the placement of illegally obtained money into legitimate financial systems so that monetary proceeds derived from criminal activities are transformed into funds with an apparently legal source.

Money laundering has many destructive consequences both for society as a whole and for those entities involved in money laundering activities. With respect to society as whole, money laundering may provide resources for drug dealers, terrorists and other criminals to operate and expand their criminal activities.

With respect to entities, any involvement whether it be to instigate, assist, conceal, or ignore the source, nature, location, ownership or control of money laundering activities, can lead to both civil and criminal proceedings against both the individual and the entity involved .

Additionally, the adverse effects, including the adverse publicity to the Firm associated with involvement in money laundering events cannot be emphasized enough.

Money laundering transactions may include:

- Advising a potential or existing client on how to structure a transaction to avoid reporting and/or record keeping requirements;
- Engaging in any activity while willfully or recklessly disregarding the source of the funds or the nature of the Clients transaction;
- Engaging in any activity designed to hide the nature, location, source, ownership or control of proceeds of criminal activity;
- Dealing in funds to facilitate criminal activity; or Dealing in the proceeds of criminal activity.

Money laundering can involve the proceeds of drug dealings, terrorist activities, arms dealings, mail fraud, bank fraud, wire fraud or securities fraud, among other activities.

6. What Is Terrorist Financing?

Terrorist financing refers to the processing of funds to sponsors involved in or those who facilitate terrorist activity. Terrorist individuals/ groups/ organization derive income from a variety of sources, often combining both lawful and unlawful funding, and where the agents

involved do not always know the illegitimate end of that income. The forms of such financing can be grouped into two types:

6.1 Financial Support - In the form of donations, community solicitation and other fundraising initiatives. Financial support may come from states and large organizations, or from individuals.

6.2 Revenue Generating Activities - Income is often derived from criminal activities such as kidnapping, extortion, smuggling or fraud. Income may also be derived from legitimate economic activities such as diamond trading or real estate investment.

7. *The Three Lines of Defense*

The Company will promote self-assessment culture at every level, making each function primarily accountable for its domain of responsibilities rather than dwelling on Compliance, Risk Management and Internal Audit to identify non-compliances, including ML/TF related non-compliance, in their reviews. To promote this Company will enforce three lines of defense concept;

First Line: Although each unit will act as first line of defense for its own activities, the business units (e.g. front office, customer-facing staff/traders) and Operations department in particular will ensure in-depth knowledge of AML/CFT related requirements and will carry out the AML/CFT due diligence policies and procedures and be allotted sufficient resources and training to do this effectively;

Second Line: This includes Compliance Department, Risk Management Department, Finance Department, Human Resources Department and Information Technology. These support functions will provide support for AML/CFT related compliances in the capacity of Company's second line of defense whereby, Finance will screen payments and ensure that cheques are received and paid to the customer only within defined threshold, Human Resource will perform adequate screening of each employee and ensure their timely trainings as per training schedule, Compliance will review fulfillment of all KYC related requirements at the time of on-boarding of customers/employees, review account closing and fund transfer processes at specified intervals, review of ongoing monitoring activities, provide support for continuous staff trainings, raising STRs and coordinating with all departments and regulatory bodies.

Third Line: The Internal Audit function along with Board Audit Committee will act as the Company's final line of defense, which will ensure that first two lines of defense are performing their duties, including AML/CFT related compliances, as per Company's

established policies and procedures, and these policies and procedures are aligned with country's regulatory framework.

In order to enable all employees in discharging their duties as first line of defense, policies and procedures will be clearly specified in writing and communicated to all employees. These will contain a clear description for employees of their obligations and instructions as well as guidance on how to keep the activities of the Company in compliance with the Regulations. These include internal procedures for detecting, monitoring and reporting suspicious transactions.

As part of second line of defense, the CO must have the authority and ability to oversee the effectiveness of the Company's AML/CFT systems, compliance with applicable AML/CFT legislation and provide guidance in day to-day operations of the AML/CFT policies and procedures.

CO must be a person who is fit and proper to assume the role and who:

- has sufficient skills and experience to develop and maintain systems and controls (including documented policies and procedures);
- reports directly and periodically to the Board on AML/CFT systems and controls;
- has sufficient resources, including time and support staff;
- has access to all information necessary to perform the AML/CFT compliance function;
- ensures regular audits of the AML/CFT program;
- maintains various logs, as necessary, which should include logs with respect to declined business, politically exposed person ("PEPs"), and requests from Commission, FMU and Law Enforcement Agencies ("LEAs") particularly in relation to investigations; and
- Responds promptly to requests for information by the SECP/LEAs.
- Maintains confidentiality of affairs unless under duty to disclose to competent authority by operation of any law.

An independent Internal Audit function, the third line of defense, should periodically conduct AML/CFT audits on an Institution-wide basis and be proactive in following up their findings and recommendations. As a general rule, the processes used in auditing should be consistent with internal audit's broader audit mandate as approved by the Board, subject to any prescribed auditing requirements applicable to AML/CFT measures

8. *Risk Assessment And Applying A Risk Based Approach*

- The SECP AML/CFT Regulations move emphasis from one-size-fits-all approach to Risk Based Approach ('RBA'), requiring ANSPL to carryout ML/TF risk assessment and apply RBA to prevent or mitigate ML and TF.
- ANSPL, before determining what is the level of overall risk and the appropriate level and

type of mitigation to be applied, take into account all the relevant risk factors, such as geography, products and services, delivery channels, types of customers, or jurisdictions within which it or its customers do business. As is the case for ANSPL' overall risk management, ANSPL' senior management should understand the nature and level of the risks that they are exposed to and ensure that systems and processes are in place to identify, assess, monitor, manage and mitigate ML/TF risks.

- The RBA enables ANSPL to ensure that AML/CFT measures are commensurate to the risks identified and allow resources to be allocated in the most efficient ways. ANSPL should develop an appropriate RBA for their organization, structure and business activities and apply the RBA on a group-wide basis, where appropriate. As a part of the RBA, ANSPL:

i. Identify ML/TF risks relevant to them;
ii. Assess ML/TF risks in relation to-
    a. Their customers (including beneficial owners);
    b. Country or geographic area in which its customers reside or operate and where ANSPL operates;
    c. Products, services and transactions that ANSPL offers; and
    d. Their delivery channels.
iii. Design and implement policies, controls and procedures that are approved by its Board of Directors to manage and mitigate the ML/TF risks identified and assessed;
iv. Monitor and evaluate the implementation of mitigating controls and improve systems where necessary;
v. Keep their risk assessments current through ongoing reviews and, when necessary updates;
vi. Document the RBA including implementation and monitoring procedures and updates to the RBA; and
vii. Have appropriate mechanisms to provide risk assessment information to the Commission.

- Under the RBA, where there are higher risks, ANSPL are required to take enhanced measures to manage and mitigate those risks; and correspondingly, where the risks are lower, simplified measures may be permitted. However, simplified measures are not permitted whenever there is a suspicion of ML/TF. In the case of some very high- risk situations or situations which are outside ANSPL's risk tolerance, ANSPL may decide not to take on the accept the customer, or to exit from the relationship.

Under the RBA, the following mechanism will be applied:

- where there are higher risks, the Company takes enhanced measures to manage and mitigate those risks; and
- Correspondingly, where the risks are lower, simplified measures are permitted. However, simplified measures are not permitted whenever there is a suspicion of ML/TF
- In the case of some very high-risk situations or situations which are outside the Company's

risk tolerance, the Company may decide not to take or accept the customer, or to exit from the relationship. CO in such cases will consider need to raise an STR to FMU.

- Since the nature of the TF differs from that of ML, the risk assessment must also include an analysis of the vulnerabilities of TF. Many of the CFT measures entities have in place will overlap with their AML measures. These may cover, for example, risk assessment, CDD checks, transaction monitoring, and escalation of suspicion and liaison relationships with the authorities. The guidance provided in these guidelines, therefore, applies to CFT as it does to AML, even where it is not explicitly mentioned.

There are three levels of risk assessment, which review ML/TF risks from different perspectives. Together, the three assessments inform RPs of potential risks to help combat ML/TF. The three risk assessments inform each other and combined provide a picture of the ML/TF risks Pakistan faces. The three levels of risk assessments are:

1. *National Risk Assessment (NRA)*
   The NRA reviews ML/TF 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 contribute to the NRA, and it provides a comprehensive overview of threats and crime trends. SECP encourages RPs to use the NRA to stay informed about emerging threats and trends.
2. *Sector Risk Assessment (SRA)*
   SECP produce a risk assessment for the sectors it regulates aiming to improve RPs' understanding of the ML/TF sector risks, and to inform them of the risk indicators, trends and emerging issues. The SRA is reviewed from time to time to check how ML/TF risks affect the regulated sectors.
3. *Risk Assessment by RPs*
   RPs must carry out a risk assessment of ML/TF in their business taking into account guidance material from SECP and the Financial Monitoring Unit. The entity risk assessment is part of SECP anti-money laundering and countering financing of terrorism guidance materials.
   Every RP shall regularly create and maintain an updated document that describes its current assessment of its ML/TF/PF risk in light of the latest National Risk Assessment. This document will be formally approved by the management and board of directors of the RP and must provide a list of proposed actions needed to address any deficiencies in risk mitigants, controls processes and procedures identified by the assessment. In addition, the document must include a view on the AML/CFT risks with respect to its customers, products, delivery channels, geography and the quality of the RPs risk mitigants, such as controls processes and procedures involving more detailed steps.

The ML/TF/PF risk assessment is not a one-time exercise and is required to be carried out annually and as required under SECP SRO 920(1)2020 on TFS Obligation and reporting. https://www.secp.gov.pk/laws/directives/.
For guidance to prepare Internal AML/CFT Risk Assessment, please refer to Section 13 - Risk Assessment and Applying a Risk Based Approach.

8.1 Identification, Assessment and Understanding Risks Mechanism

- ANSPL understand, identify and assess the inherent ML/TF risks posed by its customer base, products and services offered, delivery channels and the jurisdictions within which it or its customers do business, and any other relevant risk category. The risk assessment policies and procedures adopted by ANSPL should be appropriate to their size, nature and complexity.

- ML/TF risks may be measured using several risk categories and for each category applying various factors to assess the extent of the risk for determining the overall risk classification (e.g. high, medium or low). ANSPL should make their own determination as to the risk weights to be given to the individual risk factors or combination of risk factors. When weighing risk factors, ANSPL should take into consideration the relevance of different risk factors in the context of a customer relationship.

- In the second stage, the ML/TF risks that can be encountered by ANSPL need to be assessed analyzed as a combination of the likelihood that the risks will occur and the impact of cost or damages if the risks occur. This impact can consist of financial loss to ANSPL from the crime, monitory penalties from regulatory authorities or the process of enhanced mitigation measures. It can also include reputational damages to the business or the entity itself. The analysis of certain risk categories and their combination is specific for ANSPL so that the conclusion on the total risk level must be based on the relevant information available.

- For the analysis, ANSPL identify the likelihood that these types or categories of risk will be misused for ML and/or for TF purposes. This likelihood is for instance high, if it can occur several times per year, medium if it can occur once per year and low if it is unlikely, but not possible. In assessing the impact, ANSPL can, for instance, look at the financial damage by the crime itself or from regulatory sanctions or reputational damages that can be caused. The impact can vary from minor if they is an only short- term or there are low-cost consequences, to very major, when they are found to be very costly inducing long-term consequences that affect the proper functioning of the institution.

Risk Assessment (Lower Complexity)

The Company will assess risk by only considering the likelihood of ML/TF activity. This assessment will involve considering each risk factor that have been identified, combined with business experience and information published by the Commission and international organizations such

as the FATF. The likelihood rating will correspond to:

- Unlikely - There is a small chance of ML/TF occurring in this area of the business;
- Possible - There is a moderate chance of ML/TF occurring in this area of the business;
- Almost Certain - There is a high chance of ML/TF occurring in this area of the business

Risk Assessment (Moderate Complexity)

- Another way to determine the level of risk is to work out how likely the risk is going to happen and cross-reference that with the consequence of that risk.
- Using likelihood ratings and consequence ratings can provide the Company with a more comprehensive understanding of the risk and a robust framework to help arrive at a final risk rating. These ratings, in combination with structured professional opinion and experience, will assist the Company in applying the appropriate risk management measures as detailed in the program.
- Cross-referencing possible with moderate risk results in a final inherent risk rating of moderate. The program should then address this moderate risk with appropriate control measures. Company will need to undertake this exercise with each of the identified risks.

Risk Assessment (Higher Complexity)

- The Company will further assess risk likelihood in terms of threat and vulnerability.
- Determining the impact of ML/TF activity can be challenging but to focus AML/CFT resources in a more effective and targeted manner. When determining impact, Company can consider a number of factors, including:
  - ✓ Nature and size of your business (domestic and international);
  - ✓ Economic impact and financial repercussions;
  - ✓ Potential financial and reputational consequences;
  - ✓ Terrorism-related impacts;
  - ✓ Wider criminal activity and social harm;
  - ✓ Political impact;
  - ✓ Negative media.

- The Company wills more weight to certain factors to provide a more enhanced understanding of your ML/TF risk.
- In addition, Company may consider how its risks can compound across the various risk factors.

8.2 *Risk Mitigation and Applying Risk Based Approach.-*

ANSPL

- 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;

- monitor the implementation of those policies, procedures and controls and enhance them if necessary;

- perform enhanced measures where higher risks are identified, to effectively manage and mitigate those higher risks; and

- have an independent audit function to test the system.

8.3 *Risk Mitigation*

i. ANSPL have appropriate policies, procedures and controls that enable them to manage and mitigate effectively the inherent risks that they have identified, including the national risks. They should monitor the implementation of those controls and enhance them, if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with legal and regulatory requirements.

ii. The nature and extent of AML/CFT controls will depend on several aspects, which include:

1) The nature, scale and complexity of ANSPL's business
2) Diversity, including geographical diversity of ANSPL's operations
3) ANSPL's customer, product and activity profile
4) Volume and size of transactions
5) Extent of reliance or dealing through third parties or intermediaries.

iii. Some of the risk mitigation measures that ANSPL may consider include:

1) determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by customers;
2) setting transaction limits for higher-risk customers or products;
3) requiring senior management approval for higher-risk transactions, including those involving PEPs;
4) determining the circumstances under which they may refuse to take on or terminate/cease high risk customers/products or services; determining the circumstances requiring senior management approval (e.g. high risk or large transactions, when establishing relationship with high risk customers such as PEPs)

8.4 *House Often ANSPL will Update the Risk Assessment*

- Once the identification procedures have been completed and the business relationship is established, **ANSPL** is required to monitor the conduct of the relationship to ensure that it is consistent with the nature of business stated when the relationship/account was opened.
- **ANSPL** shall conduct ongoing monitoring of their business relationship with its Customers. Ongoing monitoring helps the **ANSPL** to keep the due diligence information up-to-date, and review and adjust the risk profile of the customers, where necessary.
- **ANSPL** conduct on-going due diligence which include scrutinizing the transactions undertaken through the course of business relationship with a Customer.
- **ANSPL** will be required to update the Risk Assessment of their Customer as per following schedule or on the occurrence of a triggering event, whichever is earlier:

    a. For its High Risk Customers, their Risk Assessment shall continuously be reviewed and updated, but a comprehensive review should be done at least monthly.
    b. For its Medium Risk Customers, their Risk Assessment shall be updated quarterly basis.
    c. For its Low Risk Customers, their Risk Assessment shall be updated 6 monthly.

- **ANSPL** may update the Customer CDD record on triggering of following events:
    a. Material changes to the customer risk profile or changes to the way that the account usually operates;
    b. Where it comes to the attention of the **ANSPL** that it lacks sufficient or significant information on that 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.
- **ANSPL** update Risk Profiling of the Customer in the following circumstances:
    a. New products or services being entered into;
    b. A significant increase in a customer's salary being deposited;
    c. The stated turnover or activity of a corporate customer increases;
    d. A person has just been designated as a PEP;
    e. The nature, volume or size of transactions changes.
- **ANSPL** shall be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts. Possible areas to monitor could be:
    a. Transaction type;

b. Frequency;
c. Amount;
d. Geographical origin/destination;
e. Account signatories.

9. *New Products, Practices and Technologies.-*

ANSPL-

- 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:
- undertake the risk assessments, prior to the launch or use of such products, practices and technologies, and ANSPL take appropriate measures to manage and mitigate the risks,
- 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 favor anonymity,

RPs in coordination with compliance function should have systems in place to identify and assess ML/TF/PF risks that may arise from new and pre-existing product such as:

(a) New products, markets or sales channels;
(b) New internal organization or new offices and departments;
(c) New data and transaction screening systems and verification of documentation:
(d) The use of virtual or digital currencies and assets;

10. *Anti-Money Laundering Compliance Officer*

The ANSPL has appointed a dedicated Compliance Officer to oversight the Compliance function who will be reporting to the Board of Directors of the ANSPL. Any Employee shall immediately notify the Compliance Officer if he/she suspects or has any reason to suspect that any potentially suspicious activity has occurred or will occur if a transaction is completed. Employees are encouraged to seek the assistance of the Compliance Officer with any questions or concerns they may have with respect to the ANSPL's AML/CFT Policy & Procedures.

- Responsibilities of the Compliance Officer include the following:
- Review of Account Opening Forms and sign off from Compliance perspective
- Coordination and monitoring of ANSPL's day-to-day compliance with applicable

Anti-Money Laundering Laws and Regulations and ANSPL's own AML/CFT Policy and Procedures; Conducting Employee training programs for appropriate personnel related to the ANSPL's

- AML/CFT policy and procedures and maintaining records evidencing such training;
- Receiving and reviewing any reports of suspicious activity from Employees; Determining whether any suspicious activity as reported by an Employee warrants reporting to senior management of the Firm;
- Coordination of enhanced due diligence procedures regarding Clients; and Responding to both internal and external inquiries regarding ANSPL's AML/CFT policy and procedures.

11. *Reporting of Suspicious Transactions / Currency Transaction Report*

Reporting of Transactions (STRs/CTRs).-

- ANSPL 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.
- ANSPL implement appropriate internal policies, procedures and controls for meeting their obligations under the AML Act.
- ANSPL 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 ANSPL, 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, Page 12 of 21 pattern, or normal operation of the account or are not commensurate with the level of income of a customer ANSPL be viewed with suspicion, be properly investigated and referred to Compliance Officer for possible reporting to FMU under the AML Act.
- ANSPL should 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 ANSPL 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 ANSPL are strictly prohibited to disclose the fact to the customer or any other quarter that a STR or related information is being or has been reported to any authority, except if required by law.

ANSPL without disclosing the contents of STRs, ANSPL intimate to the Commission on bi-annual basis the number of STRs reported to FMU and the ANSPL ensure that status report (indicating No. of STRs only) ANSPL reach the AML Department within seven days of close of each half year.

A suspicious activity will often be one that is inconsistent with a customer's known, legitimate activities or with the normal business for that type of account. Where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, the transaction must be considered unusual, and ANSPL should put "on enquiry". ANSPL should also pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

- Where the enquiries conducted by ANSPL do not provide a satisfactory explanation of the transaction, it may be concluded that there are grounds for suspicion requiring disclosure and escalate matters to the AML/CFT CO.
- Enquiries regarding complex, unusual large transactions, and unusual patterns of transactions, their background, and their result should be properly documented, and made available to the relevant authorities upon request. Activities which should require further enquiry may be recognizable as falling into one or more of the following categories. This list is not meant to be exhaustive, but includes:

(1) any unusual financial activity of the customer in the context of the customer's own usual activities;
(2) any unusual transaction in the course of some usual financial activity;
(3) any unusually linked transactions;
(4) any unusual method of settlement;
(5) any unusual or disadvantageous early redemption of an investment product;
(6) any unwillingness to provide the information requested.

- Where cash transactions are being proposed by customers, and such requests are not in accordance with the customer's known reasonable practice, ANSPL will need to approach such situations with caution and make further relevant enquiries. Depending on the type of business ANSPL conducts and the nature of its customer portfolio, ANSPL may wish to set its own parameters for the identification and further investigation of cash transactions.

- Where ANSPL has been unable to satisfy that any cash transaction is reasonable, and therefore should be considered as suspicious. ANSPL is also obligated to file Currency Transaction Report (CTR), for a cash-based transaction involving payment, receipt, or transfer of Rs. 2 million and above.
- If ANSPL decides that a disclosure should be made, the law require ANSPL to report STR without delay to the FMU, in standard form as prescribed under AML Regulations 2018. The STR prescribed reporting form can be found on FMU website through the link below.
- The process for identifying, investigating and reporting suspicious transactions to the FMU should be clearly specified in the reporting entity's policies and procedures and communicated to all personnel through regular training.
- ANSPL is required to report total number of STRs filed to the Commission on bi- annual basis within seven days of close of each half year. The CO should ensure prompt reporting in this regard.
- Vigilance systems should require the maintenance of a register of all reports made to the FMU. Such registers should contain details of:

    (1) the date of the report;
    (2) the person who made the report;
    (3) the person(s) to whom the report was forwarded; and
    (4) reference by which supporting evidence is identifiable.

It is normal practice for ANSPL to turn away business that they suspect might be criminal in intent or origin. Where an applicant or a customer is hesitant/fails to provide adequate documentation (including the identity of any beneficial owners or controllers), consideration should be given to filing a STR. Also, where an attempted transaction gives rise to knowledge or suspicion of ML/TF, that attempted transaction should be reported to the FMU.

Once suspicion has been raised in relation to an account or relationship, in addition to reporting the suspicious activity ANSPL should ensure that appropriate action is taken to adequately mitigate the risk of ANSPL being used for criminal activities. This may include a review of either the risk classification of the customer or account or of the entire relationship itself. Appropriate action may necessitate escalation to the appropriate level of decision-maker to determine how to handle the relationship, taking into account any other relevant factors, such as cooperation with law enforcement agencies or the FMU.

Sanctions Compliance.-

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. There are also sanctions that target those persons and organizations involved in terrorism. The types of sanctions that may be imposed include:

- targeted sanctions focused on named persons or entities, generally freezing assets and prohibiting making any assets available to them, directly or indirectly
- economic sanctions that prohibit doing business with, or making funds or economic resources available to, designated persons, businesses or other entities, directly or indirectly;

- currency or exchange control;
- arms embargoes, which would normally encompass all types of military and paramilitary equipment;
- prohibiting investment, financial or technical assistance in general or for particular industry sectors or territories, including those related to military or paramilitary equipment or activity;
- import and export embargoes involving specific types of goods (e.g. oil products), or their movement using aircraft or vessels, including facilitating such trade by means of financial or technical assistance, brokering, providing insurance etc.; and (7) visa and travel bans.
- Targeted financial sanctions relating to the prevention, suppression and disruption of proliferation of Weapons of Mass Destruction (WMD) and its financing.

As required by Regulations Company will screen all its customers against consolidated sanctions list available on UNSC's website and will decline business relationship with the individuals/entities and their associates that are either, sanctioned under UNSC Resolutions adopted by Pakistan or proscribed under the Anti-Terrorism Act, 1997.

The UNSC Resolution 1267 (1999), 1989 (2011), 2253 (2015) and other subsequent resolutions, which impose sanctions covering; asset freeze, travel ban and arms embargo, against individuals and entities associated to Al- Qaida, Taliban, and the Islamic State in Iraq (Daesh) organizations. The regularly updated consolidated lists are available at the UN sanctions committee's website, at following link;

https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

The UNSC Resolution 1373 (2001), 1998 (2011) on terrorism and financing of terrorism requiring member states to proscribe individual and entities, who commit or attempt to commit terrorist act, freeze without delay the funds and other financial assets or economic resources, and prohibit making any funds or financial or other related services available to such proscribed

persons and entities.

The UNSC Resolution 1718(2006), 2231(2015) and its successor resolutions [1] on proliferation of WMD and its financing, and Targeted Financial Sanctions (TFS) on countries and specifically identified individual and entities associated with it. The resolution requires, inter-alia freezing without delay the funds or other assets of, any person or entity designated, or under the authority of UNSC. The regularly updated consolidated lists of person and entities designated under UNSCRR 1718 (2006) and its successor resolutions (on the DPRK) and listed

under UNSCR 2231 (2015) (on Iran) is available at the UN sanctions committee's website, at following link;

https://www.un.org/sc/suborg/en/sanctions/1718
/materialshttps://www.un.org/sc/2231/list.shtml

Government of Pakistan, Ministry of Foreign Affairs issues Statutory Regulatory Orders (SROs) under the United Nations (Security Council) Act, 1948 (Act No XIV of 1948) to give effect to the UNSC Resolutions and implement UNSC sanction measures in Pakistan. The said SROs are communicated to the Company, from time to time, and have a binding legal effect under the Act No. XIV of 1948, Company will ensure compliance with the sanctions communicated through SROs. A list of such SROs issued by the Federal Government till date is also available at the following links:

UNSCR1267http://www.mofa.gov.pk/contentsro1.php

http://www.mofa.gov.pk/contentsro2.php

UNSCR 1718 http://www.secdiv.gov.pk/page/sro-unscr-sanctions

---

1 The UNSC sanction with respect to proliferation of WMD primarily encapsulates currently the Islamic Republic of Iran and the Democratic People's Republic of Korea's sanctions regime. The UNSC resolution on Iran is 2231 (2015). The UNSC resolution on Democratic People's

The Federal Government, Ministry of Interior issues Notifications of proscribed individuals /entities pursuant to the Anti-Terrorism Act, 1997, to implement sanction measures under UNSCR 1373(2001). The regularly updated consolidated list is available at the National Counter Terrorism Authority's website, at following link; http://nacta.gov.pk/proscribed-organizations/.

The individuals and entities designated under the aforementioned resolutions are subject

to sanctions including assets freeze, travel ban and ban on provision of any funds, financial assets or economic recourses. Such sanctions also extend to any funds, financial assets and economic resources indirectly owned by the designated individuals, and to individuals or entities acting on their behalf or on their direction.

The Company will, taking note of the circumstances where customers and transactions are more vulnerable to be involved in TF and PF activities[2], identify high-risk customers and transactions, and apply enhanced scrutiny. Company will conduct checks on the names of potential and new customers, as well as regular checks on the names of existing customers, beneficial owners, transactions, and other relevant parties against the names in the abovementioned lists, to determine if the business relation involves any sanctioned person/entity, or person associated with a sanctioned person/entity/country.

The Company will also screen its entire customer database when the new names are listed through UNSC Resolution or the domestic NACTA list. Company will undertake reasonable efforts to collect additional information in order to identify, and avoid engaging in prohibited activities and, to enable follow-up actions.

Where there is a true match or suspicion, Company will take steps that are required to comply with the sanction's obligations including immediately -

- Freeze without delay[3] the customer's fund or block the transaction, if it is an existing customer;
- Reject the customer, if the transaction has not commenced;
- lodge a STR with the FMU; and (d) notify the SECP and the MOFA.

Republic of Korea are 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (20 17), 2375 (2017) and 2397 (2017).

2 The circumstances that the Company shall take note of where customers and transactions are more vulnerable to be involved in PF activities relating to both DPRK and Iran sanction regime are listed on Annexure 7 as PF Warning Signs/Red Alerts.[3] According to FATF, without delay is defined to be ideally within a matter of hours of designation by the UNSC

The Company will submit an STR when there is an attempted transaction by any of the listed persons.

The Company will ascertain potential matches with the UN Consolidated List to confirm whether they are true matches to eliminate any "false positives". The reporting institution

must make further enquiries from the customer or counter-party (where relevant) to assist in determining whether it is a true match. In case there is not 100% match but sufficient grounds of suspicion that customer/ funds belong to sanctioned entity/ individual, the Company will consider raising an STR to FMU.

Cash Transactions (CTR)

*. Where cash transactions are being proposed by Customers, and such requests are not in accordance with the customer's known reasonable practice, the ANSPL will need to approach such situations with caution and make further relevant enquiries.
* Where the ANSPL has been unable to satisfy that any cash transaction is reasonable, and therefore should be considered as suspicious. It is also obligated to file Currency Transaction Report (CTR), for a cash-based transaction involving payment, receipt, or transfer of Rs. 2 million and above.
*. If the ANSPL decides that a disclosure should be made, the law requires the ANSPL to report STR without delay to the FMU, in standard form as prescribed under AML Regulations 2015. The STR prescribed reporting form can be found on FMU website through the link
*. ANSPL did not received any cash above Rs.25000/- from clients. In special circumstances we have received cash above Rs.25000/- from clients we are bound to report the cash transaction to PSX within 24 hours.
http://www.fmu.gov.pk/docs/AMLRegulations2015.pdf.

12. *Internal Controls (Audit Function, Outsourcing, Employee Screening And Training)*

- ANSPL are expected to have systems and controls that are comprehensive and proportionate to the nature, scale and complexity of their activities and the ML/TF risks they identified. ANSPL should establish and maintain internal controls in relation to:
    1. an audit function to test the AML/CFT systems, policies and procedures;
    2. outsourcing arrangements;
    3. employee screening procedures to ensure high standards when hiring employees; and
    4. an appropriate employee training program.
- The type and extent of measures to be taken should be appropriate to the ML/TF risks, and to the size of ANSPL.

TREC HOLDER PSX 32

12.1Audit Function

A ANSPL should, on a regular basis, conduct an AML/CFT audit to independently evaluate the effectiveness of compliance with AML/CFT policies and procedures. The frequency of the audit should be commensurate with ANSPL's nature, size, complexity, and risks identified during the risk assessments. The AML/CFT audits should be conducted to assess the AML/CFT systems which include:

- test the overall integrity and effectiveness of the AML/CFT systems and controls;
- assess the adequacy of internal policies and procedures in addressing identified risks, including;
  - (a) CDD measures;
  - (b) Record keeping and retention;
  - (c) Third party reliance; and
  - (d) Transaction monitoring;
- assess compliance with the relevant laws and regulations;
- test transactions in all areas of ANSPL, with emphasis on high–risk areas, products and services;
- assess employees' knowledge of the laws, regulations, guidance, and policies & procedures and their effectiveness in implementing policies and procedures;
- assess the adequacy, accuracy and completeness of training programs;
- assess the effectiveness of compliance oversight and quality control including parameters for automatic alerts (if any), and
- assess the adequacy of ANSPL's process of identifying suspicious activity including screening sanctions lists.

12.2 Outsourcing

- ANSPL shall maintain policies and procedures in relation to outsourcing where they intend to outsource some of their functions. ANSPL conduct the due diligence on the proposed service provider to whom it intends to outsource as appropriate and also ensure that the service provider ("OSP") is fit and proper to perform the activity that is being outsourced.
- Where ANSPL decides to enter into an outsourcing arrangement, ANSPL ensure that the outsourcing agreement clearly sets out the obligations of both parties. ANSPL entering into an outsourcing arrangement should develop a contingency plan and a strategy to exit the arrangement if the OSP fails to perform the outsourced activity as agreed.

- The OSP should report regularly to ANSPL within the timeframes as agreed upon with ANSPL. ANSPL should have access to all the information or documents relevant to the outsourced activity maintained by the OSP. ANSPL must not enter into outsourcing arrangements where access to data without delay is likely to be impeded by confidentiality, secrecy, privacy, or data protection restrictions.
- ANSPL ensure that the outsourcing agreement requires OSPs to file a STR with the FMU in case of suspicions arising in the course of performing the outsourced activity.

12.3 *Employee Screening*

- ANSPL should maintain adequate policies and procedures to screen prospective and existing employees to ensure high ethical and professional standards when hiring. The extent of employee screening should be proportionate to the potential risk associated with ML/TF in relation to the business in general, and to the risks associated with the individual positions.
- Employee screening should be conducted at the time of recruitment, periodically thereafter, i.e., at least annually and where a suspicion has arisen as to the conduct of the employee.
- ANSPL ensure that their employees are competent and proper for the discharge of the responsibilities allocated to them. While determining whether an employee is fit and proper, ANSPL may:
    (1) Verify the references provided by the prospective employee at the time of recruitment
    (2) Verify the employee's employment history, professional membership and qualifications
    (3) Verify details of any regulatory actions or actions taken by a professional body
    (4) Verify details of any criminal convictions; and
    (5) Verify whether the employee has any connections with the sanctioned countries or parties.

13. *Anti-Money Laundering Employee Training Program*

- ANSPL should ensure that all appropriate staff, receive training on ML/TF prevention on a regular basis, ensure all staff fully understand the procedures and their importance, and ensure that they fully understand that they will be committing criminal offences if they contravene the provisions of the legislation.

- Training to staff should be provided at least annually, or more frequently where there are changes to the applicable legal or regulatory requirements or where there are significant changes to ANSPL's business operations or customer base.
- ANSPL should provide their staff training in the recognition and treatment of suspicious activities. Training should also be provided on the results of ANSPL's risk assessments. Training should be structured to ensure compliance with all of the requirements of the applicable legislation.
- Staff should be aware on the AML/CFT legislation and regulatory requirements, systems and policies. They should know their obligations and liability under the legislation should they fail to report information in accordance with internal procedures and legislation. All staff should be encouraged to provide a prompt and adequate report of any suspicious activities.
- All new employees should be trained on ML/TF know the legal requirement to report, and of their legal obligations in this regard.
- ANSPL consider obtaining an undertaking from their staff members (both new and existing) confirming that they have attended the training on AML/CFT matters, read ANSPL's AML/CFT manuals, policies and procedures, and understand the AML/CFT obligations under the relevant legislation.
- Staff members who deal with the public such as sales persons are the first point of contact with potential money launderers, and their efforts are vital to an organization's effectiveness in combating ML/TF. Staff responsible for opening new accounts or dealing with new customers should be aware of the need to verify the customer's identity, for new and existing customers. Training should be given on the factors which may give rise to suspicions about a customer's activities, and actions to be taken when a transaction is suspicious.
- Staff involved in the processing of transactions should receive relevant training in the verification procedures, and in the recognition of abnormal settlement, payment or delivery instructions. Staff should be aware of the types of suspicious activities which may need reporting to the relevant authorities regardless of whether the transaction was completed. Staff should also be aware of the correct procedure(s) to follow in such circumstances.
- All staff should be vigilant in circumstances where a known, existing customer opens a new and different type of account, or makes a new investment e.g. a customer with a personal account opening a business account. Whilst ANSPL may have previously obtained satisfactory identification evidence for the customer, ANSPL should take steps to learn as much as possible about the customer's new activities.

- Although Directors and Senior Managers may not be involved in the handling ML/TF transactions, it is important that they understand the statutory duties placed upon them, their staff and the firm itself given that these individuals are involved in approving AML/CFT policies and procedures. Supervisors, managers and senior management (including Board of Directors) should receive a higher level of training covering all aspects of AML/CFT procedures, including the offences and penalties arising from the relevant primary legislation for non-reporting or for assisting money launderers, and the requirements for verification of identity and retention of records.
- The CO should receive in-depth training on all aspects of the primary legislation, the Regulations, regulatory guidance and relevant internal policies. They should also receive appropriate initial and ongoing training on the investigation, determination and reporting of suspicious activities, on the feedback arrangements and on new trends of criminal activity.

14. Anti-Money Laundering Compliance Officer

The ANSPL has appointed a dedicated Compliance Officer to oversight the Compliance function who will be reporting to the Board of Directors of the ANSPL. Any Employee shall immediately notify the Compliance Officer if he/she suspects or has any reason to suspect that any potentially suspicious activity has occurred or will occur if a transaction is completed. Employees are encouraged to seek the assistance of the Compliance Officer with any questions or concerns they may have with respect to the ANSPL's AML/CFT Policy & Procedures.

- Responsibilities of the Compliance Officer include the following:
- Review of Account Opening Forms and sign off from Compliance perspective
- Coordination and monitoring of ANSPL's day-to-day compliance with applicable Anti-Money Laundering Laws and Regulations and ANSPL's own AML/CFT Policy and Procedures;
- Conducting Employee training programs for appropriate personnel related to the ANSPL's;
- AML/CFT policy and procedures and maintaining records evidencing such training;
- Receiving and reviewing any reports of suspicious activity from Employees;
- Determining whether any suspicious activity as reported by an Employee warrants reporting to senior management of the Firm;
- Coordination of enhanced due diligence procedures regarding Clients; and Responding to both internal and external inquiries regarding ANSPL's AML/CFT policy and procedures.

15. Client Identification Procedures

15.1. General

ANSPL's AML/CFT policy and procedures are intended to ensure that, prior to accepting funds from Clients, all reasonable and practical measures are taken to confirm the Clients' identities.

ANSPL may take assistance from the bank or other financial institutions for completing client identification process. The assistance shall not relieve the ANSPL for identification process to be conducted by the company.

These Client Identification Procedures are based on the premise that the ANSPL will accept funds from a new and existing Client only after:

ANSPL has confirmed the Client's identity and that the Client is acting as a principal and not for the benefit of any third party unless specific disclosure to that effect is made; or If the Client is acting on behalf of others, ANSPL has confirmed the identities of the Underlying third parties.

The Client Identification Procedures should be reviewed in light of the specific characteristics presented by a Client and in any instance the Compliance Officer may determine to apply enhanced measures for reasons other than those discussed in section below.

As a reference tool, an Individual Client KYC Checklist is used. Employees are encouraged to provide the Compliance Officer with any revisions they consider appropriate. The Compliance Officer shall retain copies of all documents reviewed or checklists completed in connection with its Client Identification Procedures in accordance with ANSPL's Client Records Retention policy.

Every Customer shall be identified for establishing business relationship. For this purpose, investors need to fill out the Account Opening Form available at the customer support counters at ANSPL office or download it from ANSPL website.

15.2. Client Identification Procedures for Natural Persons

For Identity and due diligence purposes, at the minimum following information shall be obtained, verified and recorded on KYC/CDD form or account opening form:

- Full name as per Identity document of the Applicant

- Date of Birth, Gender, Marital status, Religion, Occupation, and Qualification
- Residential Status, Nationality, Country of Residence
- Details of Employer/Business
- CNIC/NICOP/SNIC/POC/Passport Number
- Existing Mailing and Permanent address
- Residential Telephone Number, Office Telephone Number, Fax Number, Mobile Number and Email address
- NTN and STN number
- Nature and Type of Account
- Details of Bank Account
- Details of Investor Account maintaining with CDC and Details of Sub Account maintaining with other Broker(s)
- Source of Income, Gross Annual Income, Sources of Fund for Stock Market, Expected value of Investment
- Knowledge of stock Market and Investment experience
- Normal or expected mode of transaction

15.3 Joint Accounts:

In case of Joint account, the customer due diligence measures on all of the joint account holders shall be performed as if each of them were individual customers of the ANSPL

In order to confirm the identity of the Client, copies of the following documents will be obtained and retained for ANSPL's record:

- Duly filled and signed Account Opening Form (AOF) by Title and Joint Account Holder(s).
- Bank Verification on AOF from the bank where Title Account Holder is maintaining a bank account.
- Physical presence of Title and Joint Account Holder(s) at any of the ANSPL Office along with valid original ID document.

- ☐ Attested Copies of valid ID document of Title and Joint Account Holder(s).
- ☐ Attested Copies of valid ID document of witnesses.
- ☐ Local Mobile Number and/or email address.
- ☐ Copy of Zakat Declaration (CZ-50) duly attested by notary public as per the prescribed format for Zakat exemption (Optional).
- ☐ For Non-Muslims, written request for Zakat non-applicability.
- ☐ Power of Attorney duly attested by Notary Public on prescribed format duly signed by all Account Holders (optional).
- ☐ Copy of NTN certificate, if NTN is provided in AOF.
- ☐ Copy of NICOP for non-resident Pakistanis, Passport for foreigners duly attested by Consulate office of Pakistan or Notary Public of respective country.
- ☐ Bank statement or utility bill; or other residential identifying information;
- ☐ Bank references.
- ☐ Proof of Employment/ Business
- ☐ If the account is opened by the officer of government, Special resolution/Authority from the Federal/Provincial/Local Government department duly authorized by the Ministry of Finance or Finance department of the concerned provincial or Local Government.

If a customer has authorized another person, than the additional documentation are required. These include:

- ☐ Attested copies of ID document of Authorized person
- ☐ Power of Attorney duly attested by Notary Public on prescribed format duly signed by all Account Holders with the following minimum information:
- ☐ Name of Authorized person and his/her Relationship
- ☐ CNIC/NICOP/Passport number
- ☐ Contact Details and email address
- ☐ Specimen Signature of the person so authorized.

The authorized person is only allow to issue instruction for buy or sale of securities on behalf of client and all payments or receipt of funds must be made to or from the client own accounts

and must include CNIC number clearly marked on all payment Cheques.

15.4. *Identification Client Procedures for Corporations, Partnerships, Trusts and Other Legal Entities*

ANSPL shall take reasonable steps to ascertain satisfactory evidence of an entity Client's name and address, its authority to make the contemplated investment

For Identity and due diligence purposes, at the minimum following information shall be obtained, verified and recorded on KYC/CDD form or account opening form:

- Full name as per Identity document
- Company registration /Incorporation number
- Date and country of Incorporation
- Date of Business Commenced
- Residential Status
- Type of Business
- Name of parent Company
- Email, website and contact numbers
- Registered and mailing address
- NTN number and Sales Tax number
- Details of Contact Person and authorized person to operate the account
- Nature and Type of Account
- Details of Bank Account
- Details of Investor Account maintaining with CDC and Details of Sub Account maintaining With other Broker(s)
- Financial and General Information including Investment experience, Expected value of Investment, recent change in ownership of the company, customer type,
- Normal or expected mode of transaction

ANSPL will obtain the following documents, as appropriate under the circumstances:

- Certified true copy of Board Resolution. (Specimen provided as per Annexure ") / Power of Attorney*
- Certified true copies of Constitutive Documents of the Applicant (Memorandum & Articles of Association, Act / Charter / Statute / By laws / Rules & Regulations, Certificate of Incorporation, Certificate of Commencement of Business, Prospectus for Modaraba, Relevant licenses and registration issued by Regulatory Bodies etc.)*
- Certified copy of list of Directors / Trustee (if applicable)*
- List of authorized signatories.
- List of Nominated persons allowed placing orders.
- Attested copies of C.N.I.C. / N.I.C.O.P / Passports of the Authorized Signatories.
- Attested copies of C.N.I.C. / N.I.C.O.P / Passports of the Contact Person.
- Attested copies of C.N.I.C. / N.I.C.O.P / Passports of the Witnesses.
- Certified copy of N.T.N. Certificate. (If exempted please provide Exemption Certificate).
- Latest Audited Accounts of the Company.

15.5 Beneficial Ownership of Natural Person / Legal Persons and Legal Arrangements:

Natural Person

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 ANSPL should 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 ANSPL may obtain a self-declaration for source and beneficial ownership of funds from the customer and perform further due diligence measures accordingly.

The Beneficial Owner is the natural person at the end of the chain who ultimately owns or controls the customer. The definition of BO in the Regulations is as below:

> "beneficial owner" in relation to a customer of a regulated person means, the natural person who ultimately owns or control a customer or the natural person on whose behalf

a transaction is being conducted and includes the person who exercise ultimate effective control over a person or a legal arrangement"
The ANSPL shall identify and verify the identity of the customer, and understand the nature of its business, and its ownership and control structure.

15.6 *Legal Persons and Legal Arrangements*

For legal persons or arrangements, it is essential to understand the ownership and control structure of the customer. This may be done based on plausibility and records. In any case of lack of transparency or doubt, or higher risk, verification is needed. For legal persons, the primary source for verification of ultimate beneficial ownership is the Register of Ultimate Beneficial Ownership. For complex structures, foreign entities or foreign owned entities, ANSPL are required to develop and have the necessary knowledge to correctly identify and verify such clients and their beneficial owners using information and data publicly available on the internet

* The purpose of the requirements set out regarding the identification and verification of the applicant and the beneficial owner is two fold
* First, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the applicant to be able to properly assess the potential ML/TF risks associated with the business relationship ;and second, to take appropriate steps to mitigate the risks.

* If the ANSPL has any reason to believe that an applicant has been refused facilities by another ANSPL due to concerns over illicit activities of the customer, it should consider classifying that applicant:

*. As higher-risk and apply enhanced due diligence procedures to the customer and the relationship;

* filing an STR; and/or

* not accepting the customer in accordance with its own risk assessments and procedures.

* The ANSPL shall accept copies of the documents for identifying a Customer verified by seeing originals during establishing business relationship

15.7. *Customers' Screening:*

In terms of AML/CFT Regulations, it is prohibited to provide services to proscribed individual & entities or to those who are known for their association with such individuals & entities, whether under the proscribed name or with a different name. Accordingly, it is imperative for ANSPL to monitor its relationships on a continuous basis and ensure that no such relationship exists. Further, in case, if any such relationship is found, immediately report the same to Financial Monitoring Unit (FMU) and take any other action, as per law. In pursuance of above, all customers should be properly screened through UN/OFAC sanctioned lists as available in the data base of the company.

15.8. *Approval*

The account will only be processed for account opening after it has been authorized by Compliance officer and incase of High risk customer, by the senior management of ANSPL.

15.9. *Verification Of Identity & NADRA Verisis*

The ANSPL shall verify identities of customers (Natural or Artificial persons) from NCS data base and retain on record copies of all reference documents used for identification and verification and also ANSPL shall verify the identification of a customer using reliable independent source documents, data or information including verification of CNICs from NADRA Verisis/Biometric. Similarly, ANSPL shall identify and verify the customer's beneficial owner(s) to ensure that the RP understands who the ultimate beneficial owner

15.10. *Timing of Verification*

Verification of the identity of the customers shall be completed before business relations are established including verification of Universal Identification Number (UIN) from National clearing company of Pakistan limited (NCCPL) database.

15.11. *Payment Mechanism*

The ANSPL shall accept from the account Holder(s) payment through " A/C Payee Only" crossed Cheque, bank drafts, pay orders or other crossed banking instruments in case of amounts in excess of Rs. 25,000/=. Electronic transfer of funds to the ANSPL through banks would be regarded as good as Cheque. The ANSPL shall be responsible to provide the receipt to the Account Holder(s) in the name of Account Holder(s) duly signed by authorized agents / employee of the Broker and the Account Holder(s) shall be responsible to obtain the receipt thereof. In case of cash dealings, proper receipt will be taken and given to the Account Holder(s), specifically mentioning if payment is for margin or the purchase of securities. The ANSPL shall immediately deposit in its bank accounts all cash received in whole i.e. no payments shall be made from the cash received from clients. However, in exceptional Circumstances, where it becomes necessary for the ANSPL to accept cash in excess of Rs. 25,000/=, the ANSPL shall immediately report within one business day such instances with rationale thereof to the Stock Exchange in accordance with the mechanism prescribed by the Exchange.

The ANSPL shall make all the payments of Rs. 25,000/- and above, through crossed cheques / bank drafts / pay orders or any other crossed banking instruments showing payment of amount from their business bank account. Copies of these payment instruments including cheques, pay orders, demand drafts and online instructions shall be kept in record for a minimum period of five years.

ANSPL may accept initial deposit at the time of submission of necessary documents by their prospective customer's subject to the following:

1. Initial deposit receipt will be issued after completing necessary due diligence including NCCPL verification.
2. The account numbers will be generated (NCCPL Client code and CDC Sub account number). ANSPL to obtain signatures of concerned Account Holders / Authorized Signatories as acknowledgement on the Posted Registration Detail Report generated from CDS.
3. The initial deposit will be credited to the customer's account only.
4. In case, the business relationship needed to be closed due to unsatisfactory due diligence, the ANSPL shall guide the customers to visit the office to get refund of initial deposit through Cheque.

15.12. *Account Shall Not Open*

Where CDD Measures are not completed

In case the ANSPL is not been able to satisfactorily completed required CDD measures, account shall not be opened or any service provided and consideration shall be given if the circumstances are suspicious so as to warrant the filing of an STR.

Anonymous or Fictitious Account:

ANSPL shall not open or maintain anonymous account or accounts in the name of factitious persons.

Government Accounts:

Government Account shall not be opened in the personal names of the government officials.

Proscribed Individuals/Entities:

ANSPL shall not provide services to Proscribed Individuals, Groups and Entities declared/ listed by UNSC (United Nations Security Council) and/ or by OFAC (Office of Foreign Asset Control -USA) OR those who are known for their association with such entities and persons, whether under the proscribed name or with a different name.

16. Risk Profiling Of Customers (CDD/EDD/SDD)

All relationships shall be categorized with respect to their risk levels i.e. High, Medium and Low based on the risk profiling of customer (through KYC/CDD application and as guided in the operational Manual for making effective decision whether to perform Simplified Due Diligence (SDD) or Enhanced Due Diligence (EDD) both at the time of opening and ongoing monitoring of business relationship.

Standard CDD is likely to apply to most of the customers. It involves the collection of identity information of the customer, any beneficial owner of the customer, or any person acting on behalf of the customer. It also includes the verification of that information. For beneficial owners the verification is according to the level of risk involved.

Simplified CDD can only be conducted on a specified set of circumstances such as government departments, local authorities and certain listed companies.

EDD must be conducted when RP considers that the level of risk involved is such that EDD should apply. EDD requires the collection and verification of the same information as standard CDD as well as, according to the level of risk involved, the collection and verification of information relating to the source of wealth (SoW) and source of funds (SoF) of the customer.

The approval for opening of PEP and Non-Governmental Organizations (NGOs)/Not-for-Profit Organizations (NPOs) and Charities account will be obtained from Senior Management

(Business Head) after performing EDD. Further Personal accounts will not be allowed to be used for charity purposes/collection of donations. Customer KYC / CDD profile will be reviewed and/or updated on the basis of predefined frequency, in accordance with the risk profile of the customer, as per procedure defined in operational Manual.

- High Risk At least Once in a Year or One-off*
- Medium Risk At Least Once in 2 Years or One-off*
- Low Risk At least Once in 3 Years or One-off*

*In case of any material change in the relationship or deviation from customer profile, CDD will be conducted and customer profile will be updated immediately without lapse of above defined period. Further RPs are entitled to ask customers all relevant CDD questions and may refuse business if the necessary questions are not answered, or the necessary data and documents are not provided.

16.1. High-Risk Clients

The Compliance Officer will provide and will continuously update a list of the types of Clients that ANSPL considers to be of 'high risk,' such that enhanced due diligence procedures are warranted compared to the routine Client Identification Procedures.

Following are the examples of Clients who pose a high money laundering risk in the light of UNSCR, NACTA and PNRA 2019:

1. Non-resident customers;
2. Legal persons or arrangements including non-governmental organizations; (NGOs)/ not-for-profit organizations (NPOs) and trusts / charities;
3. Customers belonging to countries where CDD/KYC and antimony laundering regulations are lax or if funds originate or go to those countries;
4. Customers whose business or activities present a higher risk of money laundering such as cash based business;
5. Customers with links to offshore tax havens;
6. High net worth customers with no clearly identifiable source of income;
7. There is reason to believe that the customer has been refused brokerage services by another brokerage house;
8. Non-face-to face / on-line customers;

9. Establishing business relationship or transactions with counterparts from or in countries not sufficiently applying FATF recommendations; and
10. Politically Exposed Persons (PEPs) or customers holding public or high profile positions.
11. Those Customers belonging to the Porous Borders Areas (in light of NRA 2019 Paragraph # 26, 27, 300 and 308)
12. Those Customers who belonging to the High Risk Areas which define in NRA (Southern Punjab, KPK, Baluchistan)
13. Those Customers who are identified as Afghan Refuges / Diaspora (in light of NRA 2019 Paragraph # 28, 29 and 133)
14. Those Customers who's Non-Resident or Foreigners are transfer their funds across the borders (in light of NRA 2019 Paragraph # 274)

16.2 Politically Exposed Persons:

Definition of PEP:

• A Politically Exposed Person (PEP) is defined by the Financial Action Task Force (FATF) as an individual who is, or has been entrusted with a prominent public function. Due to their position and influence, it is recognized that many PEPs are in positions that potentially can be abused for the purpose of committing money laundering (ML) offences and related predicate offences, including corruption, bribery, and conducting activity related to terrorist financing (TF). The potential risks associated with PEPs justify the application of additional anti-money Laundering/counter l terrorist financing (AML/CFT) preventative measures with respect to business relationships with PEPs.

POLITICALLY EXPOSED PERSONS CATEGORIES

• The difference between foreign and domestic PEPs may be relevant for firms making specific risk assessments. To help clients gain a holistic view of potential risk. In the first instance PEPs are classified at a high level in the following categories:

Foreign PEPs

Individuals who are, or have been entrusted with prominent public functions by a foreign country, for example heads of state or government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

Domestic PEPs

Individuals who are, or have been entrusted domestically with prominent public functions, for example heads of state or of government, senior politicians, senior government judicial or military officials, senior executives of state owned corporations, important political party officials.

International organization PEPs

Persons who are, or have been entrusted with a prominent function by an international organization, refers to members of senior management or individuals who have been entrusted with equivalent functions i.e. directors, deputy directors, and members of the board or equivalent functions.

Family members

Individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership

Close associates

Individuals who are closely connected to a PEP, either socially or professionally

16.3. *Enhanced Client Identification Procedures for 'High-Risk' Natural Persons*

Enhanced Client Identification Procedures for 'high risk' natural persons as Clients include, but are not limited to, the following:

- Assessing the Client's business reputation through review of financial or professional references, generally available media reports or by other means;
- Considering the source of the Client's wealth: including the economic activities that generated the Client's wealth, and the source of the particular funds intended to be used to make the investment;
- Reviewing generally available public information, such as media reports, to determine whether the Client has been the subject of any criminal or civil enforcement action based on violations of anti-money laundering laws or regulations or any investigation, indictment, conviction or civil enforcement action relating to financing of terrorists;
- Conducting a face-to-face meeting with the Client to discuss/confirm the account opening documents.

The enhanced due diligence procedures undertaken with respect to 'high risk' Clients must be thoroughly documented in writing, and any questions or concerns with regard to a 'high risk'

TREC HOLDER BOX 32

Clients should be directed to the Compliance Officer.

16.4. *Enhanced Client Identification Procedures for 'High-Risk' Corporations, Partnerships, Trusts and Other legal Entities*

Enhanced Client Identification Procedures for 'high risk' corporations, partnerships and other legal entities include, but are not limited to, the following:

- Assessing the Client's business reputation through review of financial or professional references, generally available media reports or by other means;
- Reviewing recent changes in the ownership or senior management of the Client;
- Conducting a visit to the Client's place of business and conducting a face-to-face meeting with the Client to discuss/confirm the account application, the purpose of the account and the source of assets;
- Reviewing generally available public information to determine whether the Client has been the subject of any criminal or civil enforcement action based on violations of anti-money laundering laws or regulations or any criminal investigation, indictment, conviction or civil enforcement action relating to financing of terrorists.

16.5 *On-Going Due Diligence & Monitoring*

1) All business relations with customers shall be monitored on an ongoing basis to ensure that the transactions are consistent with the "ANSPL"' knowledge of the Customer, its business and risk profile and where appropriate, the sources of funds.
2) "ANSPL" shall obtain information and examine, as far as possible the 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) "ANSPL" 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, particularly for higher risk categories of customers and the review period and procedures thereof should be defined by "ANSPL" in their AML/CFT policies, 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 "ANSPL" files an STR on reasonable grounds for suspicion that existing business relations with a customer are connected with ML/TF and the "ANSPL" considers it appropriate to retain the customer

i) The "ANSPL" shall substantiate and document the reasons for retaining the customer; and

ii) The customer's business relations with the "ANSPL" shall be subject to proportionate risk mitigation measures, including enhanced ongoing monitoring.

6) "ANSPL" shall not form business relationship with entities/individuals that are:

i) Proscribed under the United Nations Security Council Resolutions and adopted by the Government of Pakistan;

ii) Proscribed under the Anti-Terrorism Act, 1997(XXVII of 1997); and

iii) associates/facilitators of persons mentioned in (a) and (b).

7) The "ANSPL" should monitor their relationships 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 "ANSPL" shall take immediate action as per law, including freezing the funds and assets of such proscribed entity/individual and reporting to the Commission

The regulated person (ANSPL) should conduct ongoing due diligence on the business relationship by scrutinizing transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the regulated person's knowledge of the customer, their business and risk profile, including where necessary, the source of funds;

16.6. Simplified Due Diligence (SDD)

There might be circumstances where the risk of money laundering or financing of terrorism may be low as information on the identity of the customer and the beneficial ownership is publicly available and/or the turnover in the account is meager. In such circumstances, and provided there has been an adequate analysis of the risk, following SDD measures will be applied.

SDD measures shall include:

- Decreasing the frequency of customer identification updates;
- Reducing the degree of on-going monitoring and scrutinizing transactions based on a reasonable monetary threshold; and
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but intended purpose and nature of account may be ascertained from the relationship established or from the type of transactions.

SDD measures should not be considered in following situations:

- When there is a suspicion of money laundering or financing of terrorism;
- There are no exceptions in reporting suspicion to FMU within the provisions of AML Act.

17. *Red Flags Indicators/Warning Signs for Misuse of Legal Persons*

ANSPL are required to take appropriate measures to prevent the misuse of legal persons for Money Laundering/Terrorism Financing. Further, Immediate Outcome-5 also states that an effective system should be in place with effective measures to prevent legal persons from being used for criminal purposes. In Pakistan, following are the different types of legal persons that can be formed under various laws:

17.1 *Companies Formed under the Companies Act 2017, namely:*

- Single Member Limited Companies
- Private companies.
- Public companies (also referred to as listed companies).
- Public interest companies.
- Public sector companies.
- Companies limited by guarantee (s 2 (19)).
- Foreign companies (registered under Part 12 of the Companies Act).
- Associations (formed as charities and not for profit companies) under s 42.

17.2 *Limited Liability Partnerships (LLPs)*

Limited Liability partnerships (LLPs)formed under the Limited Liability Partnership Act 2017 and defined under than Act as having separate legal personality (Part 2, s 3), namely:

- Domestic limited liability partnerships.
- Foreign limited liability partnerships (registered under s 2(m) and Part 10).

17.3 *Cooperatives Formed Under Prevailing Cooperative Societies Laws*

Cooperatives formed under prevailing Cooperative Societies laws at provincial level. These entities have independent legal status as legal persons upon registration.

17.4 *Proprietorship Concerns formed by an individual*

Proprietorship Concerns formed by an individual, which is required to be dully declared by the individuals in their tax returns and to be registered as a proprietorship concerns in their National Tax Number (NTN) Certificate.

17.5 *Association of Person Section 80 of Income Tax Ordinance, 2001*

Association of Person Section 80 of Income Tax Ordinance, 2001 defines association of persons which includes a firm, a Hindu undivided family, any artificial juridical person and anybody of persons formed under a foreign law but does not include a company.

To identify a suspicion that could be indicative of Money Laundering (ML) or Terrorism Financing (IF), FMU has prepared the red flags indicators that are specially intended as an aid for the reporting entities. 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 misuse of legal person for ML / TF activity. A combination of these red flags, in addition to analysis of overall financial activity, business profile may indicate that the legal person is being potentially misused for ML/TF activity.

17.6 *Customer Behavior:*

1. When a legal person or its beneficial owner or any of its associate natural person or transaction is from a high risk jurisdiction in relation to which FATE has called for countermeasures or enhanced client due diligence measures or jurisdiction known to have inadequate measures to prevent money laundering and the financing of terrorism.
2. The legal person that is associated with terrorism activities or the legal person that has been declared proscribed.
3. When any associated natural person of the legal person is proscribed for terrorism /terrorism financing related activities.
4. The legal person who is suspected to be using forged, fraudulent, or false identity documents for due diligence and record keeping purposes.
5. The employee Director/signatory/beneficial owner of the legal person is unusually concerned with the reporting threshold or AML/CFT policies.
6. Legal Person linked to negative/adverse news or crime (named in a news report on a crime committed or under Law Enforcement investigation/inquiry).
7. Legal Person or any of its associated natural person / entity found positive match while screening against UN Security Council Resolutions (UNSCRs).
8. The legal person attempts to establish business relationship but fails to provide adequate documentary proof regarding its beneficial ownership details up to the satisfaction level of Financial Institutions or DNFBPs.
9. The beneficial ownership of the legal person appears to be doubtful while establishing relationship.
10. The complex formation structure that does not commensurate with nature of business activities or where legal person fails to disclose actual beneficial owner.
11. Multiple Legal Persons have been registered at same address or having similar contact details without any plausible reason.
12. Multiple types of legal persons are established with similar name and with same beneficial ownership.
13. The legal person owned by foreign nationals or by group of companies registered at foreign jurisdiction and failed to meet the CDD/KYC requirements regarding disclosure of ultimate beneficial ownership.
14. Unable to establish relationship between the beneficial owner and authorized signatory of the company.

15. Use of influential names (government linked / high profile entities) where the link with the high-profile entity whose name has been used cannot be directly validated.

16. Legal Person is invoiced by organizations located at any offshore jurisdiction that does not have adequate money laundering laws and is known for highly secretive banking and corporate tax haven.

17. Company records consistently reflect sales at less than cost, thus putting the company into a loss position, but the company continues without reasonable explanation of the continued loss.

18. Company has a long period of inactivity following incorporation, followed by a sudden and unexplained increase in financial activities.

19. Company is registered at an address that is also listed against numerous other companies or legal arrangements, indicating the use of mailbox service.

20. Company beneficial owners, shareholders or directors are also listed as beneficial owners, shareholders or directors in multiple other companies.

17.7 *Transactional Patterns:*

1. Transactions that are not consistent with the usual business profile of the legal person:
   a) Transactions that appear to be beyond means of the legal person based on its nature of business or declared business profile.
   b) Transactions that appear to be more than the usual amount for a nature of business in which legal person is involved.
2. Frequent/multiple transaction involving entities with the same beneficial owner, which did not make economic sense
3. The legal entity is engaged in a business that is not normally cash-intensive but appears to have substantial amounts of cash transactions.
4. Legal person deliberately avoids traditional banking service without legitimate reasons.
5. The transactions are structured to avoid reporting threshold requirements.
6. Large or frequent cash-based transactions, which do not commensurate with the stated business profile/ activities of the legal person.
7. Numerous transactions by a legal person, especially over a short period, such that the amount of each transaction is not substantial but the cumulative total of which is substantial, such transactional pattern do not commensurate with the legal person declared business profile.
8. Co-mingling of business and personal funds without any plausible reason.
9. Export / Import proceeds and other receipts and payments from/ to unrelated counterparties, which are not in-line with the legal person's business nature.
10. Round Tripping pattern of transactions that confuse the legitimate trading of business and apparently do not provide any economic benefit to the legal person.
11. High turnover of funds within a relatively short time without any plausible reason.
12. Unclear relationships between connected companies or transactional counterparties.

13. Deposit or attempt to deposit of funds via drafts / Cheques issued in favor of different form of legal person but with the similar name.
14. Proceeds received from or payments sent to an unrelated foreign buyer against which no export shipments were sent, or no imports were made.
15. Proceeds received! Sent against under or overvalued invoices of goods exported / imported.

17.8 *Analyses of various types of crimes and their ML ratings*

Assessment as to how various types of crimes and their ML threats will change the existing ratings assigned to various customer types such as the following:

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

The Adeel & Nadeem Securities (Pvt.) Ltd. is committed to fully comply with all applicable laws and regulations regarding anti money laundering/Counter Financing Terrorism/Proliferation Financing procedures and regulations

To ensure that the Adeel & Nadeem Securities (Pvt.) Ltd.'s policies and procedures are adhered to, Adeel & Nadeem Securities (Pvt.) Ltd. has designated an Anti-Money Laundering Compliance Officer (the "Compliance Officer"). The Compliance Officer is responsible for

establishing and conducting Employee training programs to ensure that all Employees are aware of the applicable AML/CFT/Proliferation Financing Laws and Regulations, AML/CFT Policies & procedures, guidelines /information provided by NRA 2019 and their responsibilities with respect to these policies. All Employees are required to attend anti-money laundering training sessions, so that all such Employees are aware of their responsibilities under ANSPL policies and procedures and as affected by current developments with respect to anti-money laundering events

17.9 The Compliance Officer duties/Responsibilities include the following:

a) Periodic Review of SAOF from Compliance perspective;
b) Monitoring of day-to-day compliance with applicable AML/CFT/Proliferation Financing Laws and Regulations and Adeel & Nadeem Securities (Pvt.) Ltd.'s own AML/CFT Policy and Procedures;
c) Receiving and reviewing any reports of suspicious activity from Employees;
d) Determining whether any suspicious activity as reported by an Employee and reporting the same to senior management of the Firm;
e) Coordination with staff members to apply enhanced due diligence procedures to Clients/Legal person and Responding to both internal and external inquiries regarding Adeel & Nadeem Securities (Pvt.) Ltd. AML/CFT/Proliferation Financing policy and procedures in order to mitigate the risk;
f) The Compliance Officer is required to watch and report consistent unusual transaction conducted by a legal person and cash transaction involving payment, receipt, or transfer of Rs. **2 million** and above shall to the management/higher authorities of the company. If the ANSPL decides that a disclosure should be made, the law requires the ANSPL to report STR without delay to the FMU, in standard form as prescribed under AML Regulations 2015. The STR prescribed reporting form can be found on FMU website through the link;
g) Once suspicion has been raised in relation to an account or relationship, in addition to reporting the suspicious activity, the ANSPL shall ensure that appropriate action is taken to adequately mitigate its risk being used for criminal activities;
h) Where an applicant or a Customer is hesitant/fails to provide adequate documentation (including the identity/source of funds/bank account statement of any beneficial owners or controllers), the MLS shall consider filing a STR and close the account of such client.

18. Proliferation Financing Warning Signs/Red Alerts

ANSPL 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:

1. Customers and transactions associated with countries subject to sanctions;
2. Instruments that could particularly be used to finance prohibited transactions, such as certain trade financing products and services;
3. Customers involved with and/or transactions related to items, materials, equipment, goods and technology prohibited by UNSCRs;
4. Reasonableness of invoiced goods against market value, inconsistency or discrepancies in trade-related documentation.

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

1. Significant withdrawals or deposits of bulk cash that could potentially be used to evade targeted financial sanctions and activity-based financial prohibitions;
2. 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);
3. Clearing of funds, granting of export credits or guarantees to persons or entities that are associated with trading transactions relating to the DPRK;
4. 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;
5. 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
6. 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
7. Using real property that DPRK owns or leases in Pakistan for any purpose other than diplomatic or consular.

19. General Reporting Procedures

- The Compliance Officer on behalf of the organization is nominated to receive disclosures under this regulation.

- Anyone in the organization, to whom information comes in the course of the relevant business as a result of which he suspects that a person is engaged in money laundering, must disclose it to the Compliance Officer;

- Where a disclosure is made to the Compliance Officer, the officer must consider it in the light of any relevant information which is available to ANSPL and determine whether it gives rise to suspicion: and

- Where the Compliance Officer determines in consultation with the Senior Management, the information must be disclosed to the Regulatory Authority after obtaining an Independent legal advice.

20. Other Offences - Failure to Report Offences

- Failure by an individual in the regulated sector to inform the Regulatory Authority or the ANSPL's Compliance Officer, as soon as racticable, of knowledge or suspicion (or reasonable grounds for knowing or suspecting) that another person is engaged in money laundering;

- Failure by Compliance Officers in the regulated sector to make the required report to Regulatory Authority as soon as practicable, if an internal report leads them to know or suspect that a person is engaged in money laundering.

De Minimis Concessions

Note that the obligation to report does not depend on the amount involved or the seriousness of the offence. There are no De Minimis Concessions.

21. Client Records Retention

Copies of all documents related to ANSPL's Client Identification Procedures will be retained for an appropriate period of time and, at a minimum, the period of time required by applicable law or regulation.

The documents ANSPL retains are copies of documents reviewed in connection with Client Identification Procedures or enhanced due diligence procedures, Client identification checklists, if any, or similar due diligence documentation, and any other documents required to be retained by applicable anti-money laundering legislation.

ANSPL will retain documents for so long as a Client is a client of ANSPL and for a minimum of five years after this relationship ends.

ANSPL shall, however, retain those records for longer period where transactions, customers or accounts involved litigation or it is required by court or other competent Authority.

ANSPL shall satisfy, on timely basis, any enquiry or order from the relevant competent authorities including Law enforcement agencies and FMU for supply of information and records as per law.

AMLA: The AMLA 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)."

22. Review of Existing Client Base and Detection of Suspicious Activity and Reporting

The ANSPL shall perform such CDD measures as may be appropriate to its existing customers having regard to its own assessment of materiality and risk but without compromise on identity and verification requirements.

The Compliance Officer shall coordinate a periodic review of the ANSPL's existing Client list,

and ensure the adequacy of due diligence performed on existing Clients. In addition, ANSPL's policies, procedures and controls may provide for the detection of suspicious activity, and if detected may require further review to determine whether the activity is suspicious,

ANSPL requires any Employee who detects suspicious activity or has reason to believe that suspicious activity is taking place immediately to inform his or her immediate supervisor as well as the Compliance Officer.

Under no circumstances may an Employee discuss the suspicious activity, or the fact that it has been referred to the Compliance Officer, with the Client concerned (Required by Law).

The Compliance Officer shall determine in consultation with the higher management whether to report to appropriate law enforcement officials (i.e. FMU-Financial Monitoring Unit) any suspicious activity of which he becomes aware within 7 working days of knowing the suspicious activity (Required by Law).

22.1. *Where CDD Measures are not completed*

If the CDD of an existing customer is found unsatisfactory, the relationship should be treated as High Risk and reporting of suspicious transaction be considered as per law and circumstances of the case.

For existing customers who opened accounts with old CNICs or old account opening form, the ANSPL shall ensure that same shall be present in ANSPL's records. The ANSPL may **INACTIVE** the accounts without CNIC and account opening form (after serving one-month prior notice) until the subject regulatory requirement is fulfilled.

22.2. *Compliance report for SECP*

ANSPL will report to SECP of any suspicious UIN through NCCPL terminal two times in every month. However, if there is no suspicious UIN, the ANSPL will submit "NIL" Report

22.3. *Reporting*

In order to ensure quality reporting, the reason(s) for suspicion should be supported with proper analysis and should contain following elements:

(a) Information on the person/entity conducting the suspicious transaction/activity;

(b) Details of the transaction, such as the pattern of transactions, type of products or services and the amount involved;

(c) Description of the suspicious transaction or its circumstances

(d) Tax profile of person/entity (if available)
(e) If the reported subject (e.g. client/customer) has been the subject of a previous STR then the reference number with date should be provided.
(f) Information regarding the counterparties, etc.
(g) Any other relevant information that may assist the FMU in identifying potential offences and individuals or entities involved.

viii. There are two types of suspicious reports which can be submitted by the RP to FMU.

(a) STR- A is to be reported on parties (Person, Account or Entity) involved in any suspicious activity, which does not involve transaction (s) or transmission of funds, However, STR-F should be filed in case where the transactions have been conducted.

(b) STR-F is to be reported on parties (Person, Account or Entity) for reporting of transactions and/or financial activity in which funds are involved and appears to be suspicious. An activity/event in which funds transmitted from one party to another must be reported as STR-F.

ix. The link of the goAML registration guide is provided as follows: http://www.fmu.gov.pk/docs/RegistrationGuideFMU.pdf. The link of the goAML reporting guide is provided as follows: http://www.fmu.gov.pk/docs/Financial-Monitoring-Unit-FMU-goAML-Web-Users-Guide-Updated-2020.pdf.

ii. As per Gazette notification SRO 73 (I)/2015 dated 21-01-2015, the minimum amount for reporting a CTR to FMU is two million rupees. Accordingly, all cash-based transactions of two million rupees or above involving payment, receipt, or transfer are to be reported to FMU as CTR. Aggregation of cash transactions during the day for the purpose of reporting a CTR is not required. However, if there is a suspicion that the customer is structuring the transaction into several broken cash transactions to evade reporting of CTR, the same may be reported in the form of an STR.

v. Similar to STR reporting to the FMU, all CTR reporting is via the FMU's online goAML system – refer: https://goamlweb.fmu.gov.pk/PRD/Home.

23. *Registration Details Update*

In accordance to the Directives under the PSX Rule book, CDC Regulations an Updation in Registration detail of any client can only be done after obtaining of the below mentioned document.

☐ *Contact Details Update*

For change of contact details i.e. contact number, local mobile number, email address etc. duly signed letter or Updation Form or by an email sent through registered email address is required as per the operating instructions. However, Title Account Holder may personally visit along with original CNIC for change of address without any documentary proof.

- *Zakat Status Update*

To update Zakat status as Zakat non-payable, letter or Updation Form along with notarized copy of Zakat Declaration is required.

- *Dividend Mandate Update*

Dividend Mandate i.e. bank details for receiving dividend warrant directly into bank account is added/updated upon letter or Updation Form.

- *NTN Update*

NTN is updated either upon receiving duly signed letter/Updation Form or by an email sent through registered email address.

- *Signature Update*

Physical presence is required along with original CNIC to update the record and for nonresident / foreign account duly signed signature card.

24. Account Closing and In Active / Dormant Account

24.1. Account Closing

- Non Operative Accounts (Which are not active or not in contact last 6 Months) are closed without any prior notice.
- Duly filled and signed Account Closing Request / Form.
- Approval from NCCPL to close the client Account (UIN)
- Intimation to CDC about closure of Sub-Account

24.2. In Active / Dormant Account

- In case a customer has no active business with the RP, and cannot be reached, or refuses to engage in updating because there is no active business, account should be marked inactive with the instruction that relationship cannot be re-activated without full CDD
- For customers whose accounts are dormant or in-operative, withdrawals will not be allowed until the account is activated on the request of the customer. For activation, the regulated person shall conduct NADRA Verisis or biometric verification of the customer and obtain attested copy of customer's valid identity document (if already not available) and fulfil the regulatory requirements

25. Employee Due Diligence & Screening

In order to ensure that unscrupulous elements do not become employees/agents, appropriate screening procedures should be followed to ensure high standards of staff in terms of honesty, integrity, ethics and professionalism To complete the process the HR department must issue confidential letters to the last employer and employee provided reference. Employee reference must be non-blood relatives and preferred to be from the employees of past employers.

26. Regular Review/Audit of the Manual

A regular review of the program should be undertaken to ensure that it is functioning as designed. Such a review could be performed by external or internal resources, and should be accompanied by 2 formal assessment or written report.

27. Future Amendments

The management will review and may amend or otherwise modify this Policy Statement from time to time with the approval of Board of Directors of the Company. Such review will preferably be carried out every year and will take into account among others the revisions in applicable regulatory framework specifically. The AML/CFT Policy & Procedures will be reviewed on as and when required basis but not later than two years.