POLICY FOR

ANTI-MONEY LAUNDERING AND

COUNTERING FINANCING OF TERRORISM

S # CONTENTS PAGE#

Policy for AML and CFT

1. Introduction, Purpose and Scope

i. Money Laundering ("ML") and Terrorist Financing ("TF") are economic crimes that threaten a country's overall financial sector reputation and expose financial institutions to significant operational, regulatory, legal and reputational risks, if used for ML and TF. This policy requires ASDA Securities 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.

ii. This policy also intends to assist ASDA Securities in complying with the Regulatory requirement. The policy supplements the Regulations and the AML/CFT regime by requiring ASDA securities to apply AML/CFT measures, develop an effective AML/CFT risk assessment and compliance framework suitable to its business, and in particular, in detecting and reporting suspicious activities.

2. Obligation of ASDA Securities in Establishing an Effective AML /CFT Governance and Compliance Regime

i. It is the obligation of ASDA Securities to establish an effective AML/CFT regime to deter criminals from using ASDA Securities as a platform for ML or TF purposes, and to develop a comprehensive AML/CFT compliance program to comply with the relevant and applicable laws and obligations.

ii. This policy and the procedures and controls prescribed are approved by the Board of Directors and senior management of ASDA Securities.

iii. This policy will be reviewed at regular intervals and on need basis to ensure it reflects any legislative changes.

3. Program and Systems to prevent ML and TF

i. ASDA Securities shall ensure that it maintains programs and systems to prevent, detect and report ML/TF. The systems should be commensurate to the size of the business and nature of the company and the ML/TF risks to which it is exposed and should include:

   a) Adequate systems to identify and assess ML/TF risks relating to persons, countries and activities which should include checks against all applicable sanctions lists;
   b) procedures to undertake a Risk Based Approach ("RBA");
   c) procedures and controls to combat ML/TF, including appropriate risk management arrangements;
   d) Customer due diligence measures;
   e) Record keeping procedures;
   f) An audit function to test the AML/CFT system;
   g) Screening procedures to ensure high standards when hiring employees; and
   h) An appropriate employee-training program.

ii. It shall be the responsibility of the senior management to ensure that appropriate systems are in place to prevent and report ML/TF and that the company is in compliance with the applicable legislative and regulatory obligations and this policy.

4. The Three Lines of Defense

i. ASDA Securities shall ensure that the following three lines of defense to combat ML/TF remains established at all material times;

- First the business units (e.g. front office, customer-facing activity): They should know and carry out the AML/CFT due diligence related policies and procedures.

  As part of first line of defense, this policy shall be communicated to all employees. Further, clear description for employees of their obligations and instructions shall be provided. The employees shall ensure that follow the procedures for detecting, monitoring and reporting suspicious transactions.

- Second the Compliance Officer, the compliance function and human resources or technology.

  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 shall have:

  i sufficient skills and experience to develop and maintain systems and controls (including documented policies and procedures);

  ii reports directly and periodically to the Board of Directors ("Board") on AML/CFT systems and controls;

  iii has sufficient resources, including time and support staff;

  iv has access to all information necessary to perform the AML/CFT compliance function;

  v ensures regular audits of the AML/CFT program;

  vi 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

  vii Responds promptly to requests for information by the SECP/Law enforcement agency.

- Third the internal audit function

  Internal audit, the third line of defense, should periodically conduct AML/CFT audits on company level and be proactive in following up their findings and recommendations.

5. Monitoring AML/CFT Systems and Controls

i. The management shall utilize back office software as well to ensure to monitor the risks identified and assessed as they may change or evolve over time due to certain changes in risk factors, which may include changes in customer conduct, development of new technologies, new embargoes and new sanctions. The management shall update the back office as appropriate to suit the change in risks.

ii. The company shall assess the effectiveness of its risk mitigation procedures and controls, and identify areas for improvement, where needed. For this purpose, the company shall consider monitoring following aspects:

   1) the ability to identify changes in a customer profile or transaction activity/behavior, which come to light in the normal course of business;
   2) the potential for abuse of products and services by reviewing ways in which different products and services may be used for ML/TF purposes, and how these ways may change;
   3) the adequacy of employee training and awareness;

4) the adequacy of internal coordination mechanisms i.e., between AML/CFT compliance and other functions/areas;
5) the compliance arrangements (such as internal audit);
6) changes in relevant laws or regulatory requirements; and
7) changes in the risk profile of countries to which the company or its customers are exposed to.

6. Documentation and Reporting

i. ASDA Securities must document its RBA. Documentation of relevant review results and responses should enable the company to demonstrate:
   1) risk assessment systems including how ASDA Securities assesses ML/TF risks;
   2) details of the implementation of appropriate systems and procedures, including due diligence requirements, in light of its risk assessment;
   3) how it monitors and, as necessary, improves the effectiveness of its systems and procedures; and
   4) the arrangements for reporting to senior management on the results of ML/TF risk assessments and the implementation of its ML/TF risk management systems and control processes.

ii. It shall be noted that the ML/TF risk assessment is not a one-time exercise and therefore, the company must ensure that ML/TF risk management processes are kept under regular review which is at least annually. Further, the management should review the program's adequacy when the company adds new products or services, opens or closes accounts with high-risk customers.

iii. ASDA Securities should be able to demonstrate through this policy the adequacy of its assessment, management and mitigation of ML/TF risks; its customer acceptance policy; its policies concerning customer identification and verification; its ongoing monitoring and procedures for reporting suspicious transactions; and all measures taken in the context of AML/CFT. The company shall maintain Risk Assessment Tables (Annex 1) AML/CFT Compliance Assessment Template (Annex 2) within the period as required by the Commission from time to time. Detailed guidance and requirements of Risk based Assessment is enclosed as Annexure 2A to this policy.

7. New Products and Technologies

i. The company shall identify and assess ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products:

ii. ASDA Securities should undertake a risk assessment prior to the launch or use of such products, practices and technologies; and take appropriate measures to manage and mitigate the risks.

iii. ASDA Securities shall prevent the misuse of technological development in ML/TF schemes, particularly those technologies that favour anonymity.

iv. ASDA Securities should ensure that its systems and procedures are kept up to date with such developments and the potential new risks and impact they may have on the products and services offered by ASDA Securities. Risks identified must be fed into the Company ' business risk assessment.

8. Customer Due Diligence

i. ASDA Securities shall ensure it take steps to know its customers. no anonymous accounts or accounts in fictitious names shall be kept and or operated. The company shall conduct CDD, which comprises of identification and verification of customers including beneficial owners (such that it is satisfied that it knows who the beneficial owner is), understanding the intended nature and purpose of the relationship, and ownership and control structure of the customer.

ii. The company shall conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the company's knowledge of the customer, its business and risk profile, including, where necessary, the source of funds. The company shall conduct CDD when establishing a business relationship if:

   (1) There is a suspicion of ML/TF. Annexure 3 gives some examples of potentially suspicious activities or "red flags" for ML/TF (not be exhaustive in nature), that will help recognize possible ML/TF schemes and may warrant additional scrutiny, when encountered. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is unusual or suspicious or one for which there does not appear to be a reasonable business or legal purpose.; or

   (2) There are doubts as to the veracity or adequacy of the previously obtained customer identification information.

iii. In case of suspicion of ML/TF, ASDA Securities should:

   (1) Seek to identify and verify the identity of the customer and the beneficial owner(s), irrespective of any specified threshold; and

   (2) File a Suspicious Transaction Reporting ("STR") with the FMU, in accordance with this policy.

iv. The company shall verify the identification of a customer using reliable independent source documents, data or information including verification of CNICs from Verisys. Similarly, the company shall identify and verify the customer's beneficial owner(s) to ensure that the company understands who the ultimate beneficial owner is.

v. The company shall ensure that the purpose and intended nature of the proposed business relationship or transaction is understood. The company shall assess and ensure that the nature and purpose are in line with its expectation and use the information as a basis for ongoing monitoring.

vi. The company shall identify and verify the identity of any person that is purporting to act on behalf of the customer ("authorized person"). The company should also verify whether that authorized person is properly authorized to act on behalf of the customer. The company shall conduct CDD on the authorized person(s) using the same standards that are applicable to a customer. Additionally, the company shall ascertain the reason for such authorization and obtain a copy of the authorization document.

vii. The company may differentiate the extent of CDD measures, depending on the type and level of risk for the various risk factors. For example, in a particular situation, it could apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa. Similarly, allowing a high-risk customer to acquire a low risk product or service on the basis of a verification standard that is appropriate to that low risk product or service, can lead to a requirement for further verification requirements, particularly if the customer wishes subsequently to acquire a higher risk product or service.

viii. When performing CDD measures in relation to customers that are legal persons or legal arrangements, the company should identify and verify the identity of the customer, and understand the nature of its business, and its ownership and control structure.

ix. The company should identify the customer and verify its identity. The type of information that would be needed to perform this function should be as specified in Annexure 4 of the policy.

x. If the company has any reason to believe that an applicant has been refused facilities by another brokerage house/regulated entity 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.

a) Timing of Verification

i. The best time to undertake verification is prior to entry into the business relationship or conducting a transaction. However, the company may complete verification after the establishment of the business relationship where it is required to perform transactions very rapidly, according to the market conditions and where performance of the transaction may be required before verification of identity is completed.

ii. Transactions such as above can only be performed subject to the approval of the CEO. For the avoidance of doubt, the company should not postpone the verification where the ML/TF risks are high and enhanced due diligence measures are required to be performed. Verification, once begun, should normally be pursued either to a satisfactory conclusion or to the point of refusal. If an applicant does not pursue an application, the staff could consider that this in itself is suspicious, and they should evaluate whether a STR to FMU is required.

iii. Where CDD checks raise suspicion or reasonable grounds to suspect that the assets or funds of the prospective customer may be the proceeds of offences and crimes related to ML/TF, the company should not voluntarily agree to open accounts with such customers. In such situations, the company should file an STR with the FMU and ensure that the customer is not informed, even indirectly, that an STR has been, is being or shall be filed.

b) Existing Customers

i. The company is required to apply CDD measures to existing customers on the basis of materiality and risk, and to conduct due diligence on such existing relationships, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

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

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

iv. Where the company is unable to complete and comply with CDD requirements as specified in this policy, it shall not open the account, commence a business relationship, or perform the transaction. If the business relationship has already been established, the company shall terminate the relationship. Additionally, the company shall consider making a STR to the FMU.

c) Tipping-off & Reporting

The Law prohibits tipping-off. However, a risk exists that customers could be unintentionally tipped off when the company is seeking to complete its CDD obligations or obtain additional information in case of suspicion of ML/TF. The applicant/customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected ML/TF operation. Therefore, if the company form a suspicion of ML/TF while conducting CDD or ongoing CDD, they should take into account the risk of tipping-off when performing the CDD process. If the company reasonably believes that performing the CDD or on-going process will tip-off the applicant/customer, it may choose not to pursue that process, and should file a STR. All concerned employees should be aware of, and sensitive to, these issues when conducting CDD or ongoing CDD.

d) No Simplified Due Diligence for Higher-Risk Scenarios

The company should not adopt simplified due diligence measures where the ML/TF risks are high. The company shall identify risks and have regard to the risk analysis in determining the level of due diligence.

10. On-going Monitoring of Business Relationships

i. Once the identification procedures have been completed and the business relationship is established, the company 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. The company shall conduct ongoing monitoring of their business relationship with their customers. Ongoing monitoring helps to keep the due diligence information up-to-date, and review and adjust the risk profiles of the customers, where necessary.

ii. On-going due diligence includes scrutinizing the transactions undertaken throughout the course of the business relationship with a customer.

iii. Documents, data or information collected during the "Identification" process are kept up-to-date and relevant by undertaking routine reviews of existing records.

iv. The company shall consider updating customer CDD records as a part its periodic reviews (i.e. annually) or on the occurrence of a triggering event, whichever is earlier. Examples of triggering events include:

(1) Material changes to the customer risk profile or changes to the way that the account usually operates;
(2) Where it comes to the attention of the company that it lacks sufficient or significant information on that particular customer;
(3) Where a significant transaction takes place;
(4) Where there is a significant change in customer documentation standards;
(5) Significant changes in the business relationship.

Examples of the above circumstances include:

(6) New products or services being entered into,
(7) A significant increase in a customer's deposit,
(8) A person has just been designated as a PEP,
(9) The nature, volume or size of transactions changes.

v. However, if the company has a suspicion of ML/TF or becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible

vi. For an effective monitoring of accounts, the same shall be achieved through a combination of computerized and through corporate compliance culture, and properly trained, vigilant staff through their day-to-day dealing with customers, effective monitoring mechanism.

11. Simplified Due Diligence Measures ("SDD")

i. The company may conduct SDD for clients with lower risks. However, the company shall ensure that the low risks it identifies are commensurate with the low risks identified by the Commission. While determining whether to apply SDD, the company should pay particular attention to the level of risk assigned to the relevant sector, type of customer or activity. The simplified measures should be commensurate with the low risk factors. SDD is not acceptable in higher-risk scenarios.

ii. Where the company decides to take SDD measures on an applicant/customer, it should document the full rationale behind such decision.

12. Enhanced CDD Measures ("EDD")

i. The company should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, that have no apparent economic or lawful purpose.

ii. Where the risks of ML/TF are higher, or in cases of unusual or suspicious activity, the company should conduct enhanced CDD measures, consistent with the risks identified. The company should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions/activities appear unusual or suspicious.

iii. Examples of enhanced CDD measures that could be applied for high-risk business relationships include:

(1) Obtaining additional information on the applicant/customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.).

(2) Updating more regularly the identification data of applicant/customer and beneficial owner.

(3) Obtaining additional information on the intended nature of the business relationship.

(4) Obtaining additional information on the source of funds or source of wealth of the applicant/customer.

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

(6) Obtaining the approval of senior management to commence or continue the business relationship.

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

iv. In case of accounts where the accountholder has instructed the company not to issue any correspondence to the accountholder's address. Such accounts do carry additional risk to the company, and due caution shall be exercised they should exercise due caution as a result.

a) High-Risk Countries

i. Certain countries associated with crimes pose a higher potential risk to the company (reputational risk and legal risk). Company should exercise additional caution and conduct enhanced due diligence on individuals and/or entities based in high-risk countries.

ii. Caution should also be exercised in respect of the acceptance of certified documentation from individuals/entities based in high-risk countries/territories and appropriate verification checks undertaken on such individuals/entities to ensure their legitimacy and reliability.

iii. The company shall consult publicly available information to ensure that they are aware of the high-risk countries/territories including sanctions issued by the UN, the FATF high risk and non-cooperative jurisdictions (www.fatf-gafi.org), and Transparency international corruption perception index (www.transparency.org)

13. Politically Exposed Persons (PEPs)

i. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose the company to significant reputational and/or legal risk. Such persons, commonly referred to as 'politically exposed persons' (PEPs) includes heads of state, ministers, influential public officials, judges and military commanders and includes their family members and close associates.

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

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

iv. The company shall remain vigilant in relation to PEPs from all jurisdictions, who are seeking to establish business relationships. The company should, in relation to PEPs, in addition to performing normal due diligence measures:

(1) obtain senior management approval for establishing business relationships with such customers;

(2) take reasonable measures to establish the source of wealth and source of funds; and

(3) Conduct enhanced ongoing monitoring of the business relationship.

vi. Senior management approval shall be obtained to continue a business relationship once a customer or beneficial owner is found to be, or subsequently becomes, a PEP.

vii. The Company shall take a risk based approach to determine the nature and extent of EDD where the ML/TF risks are high. In assessing the ML/TF risks of a PEP, the company shall consider factors such as whether the customer who is a PEP:

(1) Is from a high risk country;

(2) Has prominent public functions in sectors known to be exposed to corruption;

(3) Has business interests that can cause conflict of interests (with the position held).

viii. The other red flags that the company shall consider include:

(1) The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;

(2) Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;

(3) A PEP uses multiple bank accounts for no apparent commercial or other reason;

(4) The PEP is from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country.

ix. The company shall take a risk based approach in determining whether to continue to consider a customer as a PEP who is no longer a PEP. The factors that they should consider include:

(1) the level of (informal) influence that the individual could still exercise; and

(2) Whether the individual's previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

14. Record-Keeping Procedures

i. The company should ensure that all information obtained in the context of CDD is recorded. This includes both;
   a. recording the documents the company is provided with when verifying the identity of the customer or the beneficial owner, and
   b. Transcription into the company's own IT systems of the relevant CDD information contained in such documents or obtained by other means.

ii. The company shall maintain, for at least 5 years after termination, all necessary records on transactions to be able to comply swiftly with information requests from the competent authorities. Such records should be sufficient to permit the reconstruction of individual transactions, so as to provide, if necessary, evidence for prosecution of criminal activity.

iii. Where there has been a report of a suspicious activity or the company is aware of a continuing investigation or litigation into ML/TF relating to a customer or a transaction, records relating to the transaction or the customer should be retained until confirmation is received that the matter has been concluded.

iv. The company should also keep records of identification data obtained through the customer due diligence process, account files and business correspondence that would be useful to an investigation for a period of 5 years after the business relationship has ended. This includes records pertaining to enquiries about complex, unusual large transactions, and unusual patterns of transactions. Identification data and transaction records should be made available to relevant competent authorities upon request.

v. Beneficial ownership information must be maintained for at least 5 years after the date on which the customer is dissolved or otherwise ceases to exist, or five years after the date on which the customer ceases to be a customer.

15. Internal Controls (Audit Function, employee Screening and Training)

i. the company shall maintain internal controls and policies (appropriate to the ML/TF risks, and to the size of the company) in relation to:
   (1) an audit function to test the AML/CFT systems, policies and procedures;
   (2) employee screening procedures to ensure high standards when hiring employees; and
   (3) An appropriate employee training program.

a) Audit Function

i. the company should, on annual basis, conduct an AML/CFT audit to independently evaluate the effectiveness of compliance with AML/CFT policies and procedures. The frequency of the audit shall be revisited after the evaluation of the risks identified during the risk assessments. The AML/CFT audits should be conducted to assess the AML/CFT systems which include:
   (1) test the overall integrity and effectiveness of the AML/CFT systems and Controls;
   (2) assess the adequacy of internal policies and procedures in addressing identified risks, including;
      (a) CDD measures;

(b) Record keeping and retention;
(c) Transaction monitoring;

(3) assess compliance with the relevant laws and regulations;
(4) test transactions in all areas of the company, with emphasis on high–risk areas, products and services;
(5) assess employees' knowledge of the laws, regulations, guidance, and policies & procedures and their effectiveness in implementing policies and procedures;
(6) assess the adequacy, accuracy and completeness of training programs;
(7) assess the effectiveness of compliance oversight and quality control including parameters for automatic alerts (if any), and
(8) assess the adequacy of the company's process of identifying suspicious activity including screening sanctions lists.

c) Employee Screening

i. The company shall 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 particular risks associated with the individual positions.
ii. Employee screening should be conducted at the time of recruitment and where a suspicion has arisen as to the conduct of the employee.
iii. The company shall 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, the company 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.

d) Employee Training

i. The company shall 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.
ii. 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 in the company's business operations or customer base.
iii. The company should provide their staff training in the recognition and treatment of suspicious activities. Training should also be provided on the results of the company's risk assessments. Training should be structured to ensure compliance with all of the requirements of the applicable legislation.
iv. 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.
v. All new employees should be trained on ML/TF know the legal requirement to report, and of their legal obligations in this regard.

vi. The company shall obtain an undertaking from their staff members (both new and existing) confirming that they have attended the training on AML/CFT matters, read the company's AML/CFT manuals, policies and procedures, and understand the AML/CFT obligations under the relevant legislation.

vii. 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 considered to be suspicious.

viii. 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.

ix. 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.

16. Reporting of Suspicious Transactions / Currency Transaction Report

i. 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 the company should put "on enquiry". The company shall 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.

ii. Where the enquiries conducted by the company 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.

iii. 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.

iv. The company 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.

v. If the company decides that a disclosure should be made, the law require the company to report STR without delay to the FMU, in standard form as prescribed under AML Regulations 2008. The STR prescribed reporting form can be found on FMU website through the link http://www.fmu.gov.pk/docs/AML_Regulations-2008.pdf.

vi. The company shall report total number of STRs filed to the Commission on biannual basis within seven days of close of each half year. The CO should ensure prompt reporting in this regard.

vii. The company shall should maintain 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.

viii. Where 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.

ix. In addition to reporting the suspicious activity, the company shall ensure that appropriate action is taken to adequately mitigate the risk of the company 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 shall be to escalate the matter to CEO to determine how to handle the relationship, taking into account any other relevant factors, such as cooperation with law enforcement agencies or the FMU.

17. Sanctions Compliance- Implementation of UN Security Council Resolutions

i. The Company shall not form business relationship with the individuals/entities and their associates that are either, sanctioned under United Nations Security Council (UNSC) Resolutions adopted by Pakistan or proscribed under the Anti-Terrorism Act, 1997.

ii. The Company is also required to screen its entire customer database when the new names are listed through UNSC Resolution or the domestic NACTA list.

iii. Where there is a true match or suspicion, the company shall take steps that are required to comply with the sanctions obligations including immediately–

(a) freeze without delay[1] the customer's fund or block the transaction, if it is an existing customer;

(b) reject the customer, if the transaction has not commenced;

(c) lodge a STR with the FMU; and

(d) Notify the SECP and the MOFA.

iv. The company is required to submit a STR when there is an attempted transaction by any of the listed persons.

v. The company must ascertain potential matches with the UN Consolidated List to confirm whether they are true matches to eliminate any "false positives". The company 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 may consider raising an STR to FMU.

vi. The sanctions compliance program shall be an integral part of the overall AML/CFT compliance program.

vii. The company shall document and record all the actions that have been taken to comply with the sanctions regime, and the rationale for each such action.

viii. The company shall keep track of all the applicable sanctions, and where the sanction lists are updated, shall ensure that existing customers are not listed.