MARGALLA FINANCIAL (PRIVATE) LIMITED

ANTI MONEY LAUNDERING (AML)

/

COUNTERING FINANCING OF TERRORISM (CFT)

POLICIES & PROCEDURES MANUAL

DISCLAIMER

The information contained herein is subject to change without prior notice. While every effort is made to ensure accuracy and completeness of information contained, Margalla Financial (Pvt) Limited makes no guarantee and assumes no liability for any errors or omissions of information. No person can use the information for any claim, demand or cause of action.

GLOSSARY

AOF	Account Opening Form
AML	Anti-Money Laundering
BOD	Board of Directors
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
CIF	Customer Information File
CNIC	Computerized National Identity Card
CO	Compliance Officer
CTR	Cash Transaction Report
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FMU	Financial Monitoring Unit
ML	Money Laundering
NADRA	National Database and Registration Authority
NICOP	National Identity Card for Overseas Pakistanis
OFAC	Office of the Foreign Assets Control
PEP	Politically Exposed Persons
PF	Proliferation Financing
POC	Pakistan Origin Card
PSX	Pakistan Stock Exchange
RO	Reporting Officer
RMA	Relationship Management Application
SBP	State Bank of Pakistan
SDD	Simple Due Diligence
SECP	Securities and Exchange Commission of Pakistan
SNIC	Smart National Identity Card
STR	Suspicious Transaction Report
TF	Terrorist Financing
UN	United Nations
UNSC	United Nations Security Council

Table of Contents

INTRODUCTION

Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) are economic crimes that threaten the integrity of financial systems of a country. In order to prevent and protect itself from the menace of ML and TF, Margalla Financial (Private) Limited has prepared and implemented clear and well defined AML and CFT policies.

OBJECTIVES

- The AML/CFT policies have been designed to comply with regulations as defined in the Anti Money Laundering Act of 2010 ("the Act") and the Securities and Exchange Commission of Pakistan's (SECP) AML/CFT Regulations, 2020.
- To mitigate the threats and vulnerabilities as highlighted in the National Risk Assessment 2019.
- To Implement best practices as established by FATF
- To establish the qualifications and define the role of Compliance Officer to ensure adherence to the AML/CFT policies and procedures
- To prepare policies to identify customers and determine monitoring requirements based on risk assessments
- To Implement a Risk Based Approach to assess and apply measures to prevent or mitigate ML and TF.
- To educate and train all employees to create awareness and to understand their responsibilities in preventing, detecting and detecting ML and TF

ROLE AND COMMITMENT OF SENIOR MANAGEMENT

- The senior management including the Board of Directors and Senior Managers shall be fully committed to the goal of ML/TF prevention.
- AML/CFT will be a priority and will include active supervision and monitoring
- The senior management will educate and keep up to date on AML/CFT regulations and best practices
- The management will provide all resources to the compliance officer to perform his duties
- The management will review the compliance reports and any suspicious activities and assist Compliance officer in investigation and reporting
- The management will review the AML/CFT policies and procedures on a regular basis and amend them as necessary

COMPLIANCE OFFICER (CO)

The company will designate a Compliance Officer who will be a focal person for all AML/CFT activities. CO must be a person who is fit and proper to assume the role and who:

(1) has sufficient skills and experience to develop and maintain systems and controls (including documented policies and procedures);
(2) reports directly and periodically to the Board of Directors ("Board") or equivalent on AML/CFT systems and controls;
(3) has sufficient resources, including time and support staff;
(4) has access to all information necessary to perform the AML/CFT compliance function;
(5) ensures regular audits of the AML/CFT program;
(6) 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
(7) responds promptly to requests for information by the SECP/Law enforcement agency.

CUSTOMER IDENTIFICATION, ASSESSMENT AND MONITORING

The company will do its utmost to establish the identity of its clients prior to commencing a business relationship with them. Once the identity of the owner is confirmed, a risk assessment will be conducted based on which monitoring requirements will be highlighted.

Identification of 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

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.

Foreign Individuals:
Currently only Pakistani Nationals with identity documents issued by the Government of Pakistan are allowed to open an account with the firm. Due to difficulty in the verification of documents of foreign nationals, which includes Afghan nationals, refugees and other foreigners residing either in Pakistan or abroad, non-Pakistanis will not be entered into a business relationship at this point in time.

Client Identification for Corporations, Partnerships, Trusts and Other Legal Entities

The company shall take reasonable steps to ascertain satisfactory evidence of an entity Client's name and address, its authority to make the contemplated investment. Utmost effort will be made to determine the ultimate beneficial ownership (UBO) of the entity. 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
- Form 45 filed by the company with SECP for UBO declaration
- 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.

Identity Documentation

Following documents will be obtained from the clients for verification purposes:

S No.	Type of Customer	Information/Documentation to be Obtained
1	Individuals	A photocopy of any one of the following valid identity documents; (i) Computerized National Identity Card (CNIC) issued by NADRA. (ii) National Identity Card for Overseas Pakistani (NICOP) issued by NADRA. (iii) Pakistan Origin Card (POC) issued by NADRA. (iv) Alien Registration Card (ARC) issued by National Aliens Registration Authority (NARA), Ministry of Interior (local currency account only). (v) (v) Passport; having valid visa on it or any other proof of legal stay along with passport (foreign national individuals only).
2	Sole Proprietorship	(i) Photocopy of identity document as per Sr. No. 1 above of the proprietor. (ii) Copy of registration certificate for registered concerns. (iii) Copy of certificate or proof of membership of trade bodies etc, wherever applicable. (iv) Declaration of sole proprietorship on business letter head. (v) Account opening requisition on business letter head. (vi) Registered/ Business address.
3	Partnership	(i) Photocopies of identity documents as per Sr. No. 1 above of all the partners and authorized signatories. (ii) Attested copy of 'Partnership Deed'. (iii) Attested copy of Registration Certificate with Registrar of firms. In case the partnership is unregistered, this fact shall be clearly mentioned on the Account Opening Form. (iv) Authority letter from all partners, in original, authorizing the person(s) to operate firm's account. (v) Registered/ Business address.
4	Limited Companies /Corporations	(i) Certified copies of: a. Resolution of Board of Directors for opening of account specifying the person(s) authorized to open and operate the account; b. Memorandum and Articles of Association;

		c. Certificate of Incorporation; d. Certificate of Commencement of Business, wherever applicable; e. List of Directors on 'Form-A/Form-B' issued under Companies Act, 2017, as applicable; and f. Form-29, wherever applicable. (ii) Photocopies of identity documents as per Sr. No. 1 above of all the directors and persons authorized to open and operate the account;
5	Branch Office or Liaison Office of Foreign Companies	(i) A copy of permission letter from relevant authority i-e Board of Investment. (ii) Photocopies of valid passports of all the signatories of account. (iii) List of directors on company letter head or prescribed format under relevant laws/regulations. (iv) A Letter from Principal Office of the entity authorizing the person(s) to open and operate the account. (v) Branch/Liaison office address.
6	Trust, Clubs, Societies and Associations	(i) Certified copies of: a. Certificate of Registration/Instrument of Trust b. By-laws/Rules & Regulations (ii) Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate the account. (iii) Photocopy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body. (iv) Registered address/ Business address where applicable.
7	NGOs/NPOs/Charities	(i) Certified copies of: a. Registration documents/certificate b. By Laws/Rules and Regulations (ii) Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate

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

Note:

(i) The photocopies of identity documents shall be validated through NADRA verisys.

(ii) In case of a salaried person, in addition to CNIC, an attested copy of his service card or certificate or letter on letter head of the employer will be obtained.

(iii) In case of an individual with shaky/immature signatures, in addition to CNIC, a passport size photograph of the new account holder will be obtained.

(iv) In case of expired CNIC, account may be opened on the basis of attested copies of NADRA receipt/token and expired CNIC subject to condition that regulated person shall obtain copy of renewed CNIC of such customer within 03 months of the opening of account. For CNICs which expire during the course of the customer's relationship, regulated person shall design/ update their systems which can generate alerts about the expiry of CNICs at least 01 month before actual date of expiry and shall continue to take reasonable measures to immediately obtain copies of renewed CNICs,

whenever expired. In this regard, regulated person are also permitted to utilize NADRA Verisys reports of renewed CNICs and retain copies in lieu of valid copy of CNICs. However, obtaining copy of renewed CNIC as per existing instructions will continue to be permissible.

(v) In case the CNIC does not contain a photograph, regulated person shall obtain the following:

a) duly attested copy of either driving license, service card, nikkah nama, birth certificate, educational degree/certificate, pension book, insurance certificate.

b) A photograph duly attested by gazette officer/administrator/office of regulated person.

c) A copy of CNIC without photograph duly attested by the same person who attested the photograph

(vi) The condition of obtaining Board Resolution is not necessary for foreign companies/entities belonging to countries where said requirements are not enforced by their laws/regulations. However, such foreign companies will have to furnish Power of Attorney from the competent authority for establishing Business Relationship to the satisfaction of the regulated person.

(vii) The condition of obtaining photocopies of identity documents of directors of limited companies/corporations is relaxed in case of Government/Semi Government entities, where regulated person should obtain photocopies of identity documents of only those directors and person who are authorized to establish and maintain business relationship. However, regulated person shall validate identify information including CNIC numbers of other directors from certified copies of 'Form-A/Form-B' and 'Form 29' and verify their particulars through NADRA Verisys. The Verisys reports should be retained on record in lieu of photocopies of identity documents.

RISK ASSESSMENT

A risk assessment shall be done on the basis of information obtained at the time of account opening i.e. customer's identity, nature of income, source of funding, location of customer etc. and shall be updated on the basis of information obtained during the relationship and doing business with the customer.

Following factors categorize the customer into High Risk Category:

a. Non-resident customers;

b. Legal persons or arrangements including non-governmental organizations ("NGOs")/not-for-profit organizations ("NPOs") and trusts/ charities;

c. Customers belonging to countries where KYC/CDD and anti-money laundering regulations are lax or if funds originate or go to those countries;

d. Customers whose business or activities present a higher risk of money laundering such as cash based business;

e. Customers with links to offshore tax havens;

f. High net worth customers with not clearly identifiable source of income;

g. There is a reason to believe that the customer has been refused brokerage services by another brokerage house;

h. Non-face-to-face/on-line customers;

i. Establishing business relationship or transactions with counterparts from or in countries not sufficiently applying Financial Action Task Force ("FATF") recommendations; and

j. Politically Exposed Persons ("PEPs") or customers holding public or high profile positions.

- Politically Exposed Persons ("PEPs") include individuals in prominent positions such as senior politicians, senior government, judicial or military officials, senior executives of State Corporations and their family members and close associates.

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' Clients should be directed to the Compliance Officer.

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.

Simplified Due Diligence

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

1) reasonable monetary threshold; and
2) 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:

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

INTERNAL RISK ASSESSMENT

The Internal Risk Assessment (IRA) will be conducted with the aim of identifying the inherent ML/TF threats and vulnerabilities. Emphasis will also be placed on transnational threats that have been highlighted by the NRA 2019. Better understanding of the threats and vulnerabilities will allow the company to create and implement robust policies and procedures to mitigate ML/TF.

The methodology for Internal Risk Assessment will refer to the following concepts as defined by the FATF:

A **threat** is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy, etc. In the ML/TF context this includes

criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities.

Vulnerabilities comprise those things that can be exploited by the threat or that may support or facilitate its activities. In the ML/TF risk assessment context, looking at vulnerabilities as distinct from threat means focusing on, for example, the factors that represent [weaknesses in AML/CFT systems or controls or certain features of a country. They may also include] the features of a particular sector, a financial product or type of service that make them attractive for ML or TF purposes. Note: this revised NRA focuses on inherent vulnerabilities, so we have put the reference to weaknesses in AML/CFT in brackets.

Inherent risk: refers to ML/TF risk prior to the application of AML/CFT controls.

Consequence refers to the impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally.

Likelihood of ML/TF: the likelihood of ML/TF threat actors exploiting inherent vulnerabilities.

A Risk Based Approach (RBA) will be employed in the risk assessment. The following four areas will be analyzed

i. Customers including Beneficial Owners

Special emphasis is to be taken to identify the clients and based on their ratings assess the exposure to ML/TF/PF risks from the following type of customers in particular

(1) PEP

(2) HNWI

(3) Foreign Clients

ii. Products offered by the entity
Assessment of the active products offered by the company and the potential of these products to be used for ML/TF/PF purposes

iii. Geography in which the company operates
Assessment of geography of the customers must be taken into high consideration. The border areas of Balochistan and KPK have porous borders with Afghanistan and Iran and are therefore highly exposed to geographical

vulnerability. These borders are frequently used for smuggling, cash movement, illegal business activities and border crossing. Border areas of Sindh with India are also highly vulnerable. Customers from these areas and jurisdictions identified as high risk by FATF will be marked in the high risk category.

iv. Delivery Channels
Cash, Wire transfers, online payment transaction, payments through credit card/debit cards and internet-based payments solutions increase ML risks. Use of proper banking channels mitigates delivery channel risks.

MONITORING AND REPORTING

Basis of Monitoring

Continuous monitoring is an essential ingredient of an effective AML/CFT program and the extent of monitoring should be according to the risk sensitivity of the account.

Monitoring and Identifying Suspicious Activities

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 RP should put "on enquiry". RPs 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.

ii. Where the enquiries conducted by the RP 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. Where cash transactions are being proposed by customers, and such requests are not in accordance with the customer's known reasonable practice, RPs will need to approach such situations with caution and make further relevant enquiries. Depending on the type of business each RP conducts and the nature of its customer portfolio, each RP may wish to set its own parameters for the identification and further investigation of cash transactions.
v. Where the RP has been unable to satisfy that any cash transaction is reasonable, and therefore should be considered as suspicious. RP 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.

vi. Customers who are unknown to the broker and verification of identity / incorporation proves difficult;
vii. Customers who wish to deal on a large scale but are completely unknown to the broker;
viii. Customers who wish to invest or settle using cash;
ix. Customers who use a cheque that has been drawn on an account other than their own;
x. Customers who change the settlement details at the last moment;
xi. Customers who insist on entering into financial commitments that appear to be considerably beyond their means;
xii. Customers who accept relatively uneconomic terms, when with a little effort they could have a much better deal;
xiii. Customers who have no obvious reason for using the services of the broker (e.g.: customers with distant addresses who could find the same service nearer their home base; customers whose requirements are not in the normal pattern of the service provider’s business which could be more easily serviced elsewhere);
xiv. Customers who refuse to explain why they wish to make an investment that has no obvious purpose;
xv. Customers who are introduced by an overseas agent based in a country noted for drug trafficking or distribution
xvi. Customers who carry out large numbers of transactions with the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction, particularly if the proceeds are also then credited to an account different from the original account;
xvii. Customer trades frequently, selling at a loss
xviii. Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments;
xix. Customers who wish to maintain a number of trustee or customers’ accounts which do not appear consistent with the type of business, including transactions which involve nominee names;
xx. Any transaction involving an undisclosed party;
xxi. transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral; and
xxii. Significant variation in the pattern of investment without reasonable or acceptable explanation

xxiii. Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting thresholds.
xxiv. Transactions involve penny/microcap stocks.
xxv. Customer requests a securities provider to execute and/or clear a buy order and sell order for the same security or similar or correlated securities (and/or on behalf of the same beneficial owner), in close chronology.

xxvi. Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
xxvii. Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.
xxviii. Customer invests in securities suddenly in large volumes, deviating from previous transactional activity.
xxix. Customer conducts mirror trades.
xxx. Customer closes securities transaction before maturity, absent volatile market conditions or other logical or apparent reason.

Reporting of Transactions (STRs/CTRs)

When a suspicious activity is identified, it will be reported to the Compliance officer. The compliance officer will investigate the matter and document his reasoning. If CO cannot justify the activity, he will file an STR/CTR with the FMU and inform the senior management as well.

TARGETED FINANCIAL SANCTIONS (TFS) OBLIGATIONS UNDER UNSC RESOLUTIONS

TFS obligations are provided under the following legal instruments:
a) United Nations (Security Council) Act, 1948 (UNSC Act)
b) United Nations Security Council (Freezing and Seizure) Order, 2019
c) Statutory Regulatory Orders (SROs) issued under UNSC Act
d) Anti-Terrorism Act, 1997 (ATA)
e) Notifications issued under ATA
f) AML Act, 2010 and rules, regulations and directives issued thereunder.

(1) The company shall undertake TFS obligations under the United Nations (Security Council) Act 1948 and/or Anti-Terrorism Act 1997 and any regulations made there under, including:
(a) develop mechanisms, processes and procedures for screening and monitoring customers, potential customers and beneficial owners/associates of customers to detect any matches or potential matches with the stated designated/proscribed persons in the SROs and notifications issued by MoFA, NACTA and MoI.

(b) If during the process of screening or monitoring of customers or potential customers the company finds a positive or potential match, it shall immediately:
i. freeze the relevant funds and assets without delay the customer's fund/ policy or block the transaction, without prior notice if it is an existing customer in accordance with the respective SRO.
ii. prohibit from making any funds or other assets, economic resources, or financial or other related services and funds in accordance with the respective SRO
iii. Reject the transaction or attempted transaction or the customer, if the relationship has not commenced.

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

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

(2) The company is prohibited, on an ongoing basis, from providing any financial services to proscribed/ designated entities and persons or to those who are known for their association with such entities and persons, whether under the proscribed/ designated name or with a different name. The company will monitor its business relationships with the entities and individuals on a continuous basis and ensure that no such relationship exists directly or indirectly, through ultimate control of an account and where any such relationship is found, the company shall take immediate action as per law, including reporting to the FMU.

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

DATA RETENTION

- The Company shall maintain the relevant documents obtained through the application of KYC/CDD procedures, especially those pertaining to identification of the identity of a

customer, account files and correspondence exchanged for a minimum period of five years.

- The Company shall ensure that the customer records are updated with due care and proper documentation must be done and sufficient information is obtained regarding any significant change in the customer profile.

- Suspicious Activities are to be documented along with any in-house investigation

- A record of STRs and CTRs including all related evidences should be kept

TRAINING

The Company shall conduct employees' training sessions, from time to time, to ensure that the employees understand their duties and are able to perform the same on a satisfactory level.