Know your Customer/Customer Due Diligence, Anti-Money Laundering, Countering Financing of Terrorism and Proliferation Financing Policy

Arif Habib Limited

ARIF HABIB LIMITED

APRIL 22, 2025

Table of Contents

ARIF HABIB LIMITED

1. INTRODUCTION

The Securities and Exchange Commission of Pakistan has issued comprehensive guidelines on Know Your Customer/Customer due Diligence, Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing standards in the context of the recommendations made by the Financial Action Task Force (FATF) and has advised all financial institutions to establish proper KYC / AML framework in line with requirements of AML/CFT/CPF Regulations, 2020 and the related Guidelines.

This Policy introduces the general framework for the fight against ML/TF and other financial crime. The standards set out in this Policy are minimum requirements based on applicable Laws and Regulation. These requirements are intended to prevent, our organization and employees from being misused for ML/TF and deploy mitigating measures to effectively manage the risk of Money Laundering and Terrorist Financing (ML/TF) faced by our Company

All the definition and terms used in this policy are referred from the aforementioned Regulations and Guidelines.

2. OBJECTIVES

The objective of KYC/AML policy is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities. The policies and procedures set forth in this Policy Manual shall also enable the Arif Habib Limited to know and get better understand of its Clients and its financial dealings better which in turn will help it to effectively manage its ML/TF risks. Thus, the AML/CFT/CPF policy has been framed by the AHL for the following purposes:

- Comply with all Anti - Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing Rules & Regulations and guidelines applicable on us.
- Maintain an effective compliance culture within organization
- Ensure that every member, officer, director, and employee (each, an Employee") is familiar with applicable laws and regulations
- And are aware of their reporting obligations in case of any suspicious activity found.
- Ensure Adequate trainings are provided to its employees for detecting suspicious activities and reporting to the Compliance Officer by following established internal control procedures.

3. CLIENT IDENIFICATION PROCEDURES

Client identification means identify the Client and verify the information provided by using independent and reliable sources. The company shall undertake identification and verification process at the time of commencement of business relationship and/or when there is doubt about the veracity of already obtained information.

Client Identification Procedures for Natural Person:

In order to confirm the identity of the Client, following documents shall be obtained and retained for AHL's records:

- Duly filled and signed Know Your Customer form and Customer Relationship form
- Attested copies of CNIC, SNIC, NICOP, ARC or POC, Passport or other official government-issued identification documents; where CNIC/SNIC/NICOP shall be validated through NADRA Verisys or biometric verification will be conducted where applicable.
- Power of attorney, where applicable, along with identification documents of the attorney.
- Address Details of the Applicant including documentary evidences such as Bank statement or utility bill; or other residential identifying information
- Details concerning Annual Income, Source of Income, Occupation and name of Business/Employer with documentary evidences.
- In case of foreign clients, all documents provided shall be attested by notary public and/or Counsel general of Pakistan.
- Any other information/documentation in accordance with Annexure I of SECP AML/CFT/CPF Regulation, 2020.

For due diligence purpose, at the minimum following information shall also be obtained, verified and recorded on Client profile:

- Nature and purpose of Account
- Details of Bank Account
- Details of Investor Account maintaining with CDC and Details of Sub Account maintaining with other Broker(s)
- Qualification, Number of Dependents, Employment/Business Duration, NTN Status, Account opened with any other broker (Active/Inactive/closed status)
- Knowledge of stock Market and Investment experience
- Normal or expected mode of transaction and Expected Monthly Turnover

All offline/online clients shall be required to perform biometric verification at the time of account opening and in case the account is opened through online digital platform, Customer Care Officer may required to video call the client for face to face verification purpose. For every new account, particulars of client, nominee, beneficial owner, authorized person shall be matched with

proscribed persons'/organization list (as notified by UNSCR, NACTA, OFAC or any other regulatory body) maintained in AHL Information Management system.

AHL will confirm 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, AHL will also confirm the identities of the underlying third parties and/or beneficial owner and will obtain all aforesaid necessary documents.

The Company shall establish and maintain risk-sensitive internal policies, procedures and controls to determine whether a customer, connected party, agent, beneficial owner is a PEP, an immediate family member of a PEP or a close associate of a PEP when conducting CDD on their customers

Politically Exposed Person:

A PEP is an individual who is or has been entrusted with a prominent public function either domestically or by foreign country such as heads of state or government, ministers, senior public officials, judges and military commanders, political party officials; including their family members and close associates

To determine if a customer/agent/connected party/beneficial owner is a PEP, the Company will ensure that the CDD information is up to date so that they can monitor the business relationship for a change in PEP status. To do that, the Company may use the internet and media as sources for determining, monitoring, and verification of information in relation to PEP. Alternatively, self-declaration by a customer of their PEP status can also be accepted. However, the Company will not solely rely on such self-declarations and will engage the customers and obtain information pertinent to the different elements of the PEP definition.

For such customers and beneficial owners identified as a PEP, the Company shall take reasonable measures to establish the overall source of wealth and source of funds such as obtaining tax returns, bank statements etc. and obtain senior management approval for establishing/continuing business relationships. The Company shall perform ongoing monitoring of such client on regular intervals

Account shall not be opened or business relationship shall be declined/ceased if client fails to provide valid identity documents or where due diligence cannot be performed adequately.

Client Identification Procedures for Legal Person:

For legal person such as Corporations (local and international), Retirement funds, NGO/NPO, Waqf, Government owned entities etc. following documents shall be obtained to understand nature of Client business, control structure and ultimate beneficial ownership and retained for AHL's records:

- Duly filled and signed Know your Customer and Customer Relationship Form
- Registration Documents such as Certificate of Incorporation and Certificate of Commencement of business (if any)

- Copy of Latest Form-A/Form-B and Form 29 filled with SECP
- Articles of Memorandum and Articles of Association, or any other constitutive registration documents such as trust deeds, bye laws, etc.
- Copy of resolution of Board of Directors/ any other Executive Committee constitute for this purpose to open the account and granting the Directors/Principals authority to open and operate the account
- List of Directors/Members/Trustees/Authorized Signatory/Senior Management/Nominated persons to operate the account on business letterhead with their attested CNIC/NICOP/Passport copies
- Audited Financial statements
- Details of Ultimate Beneficial Owner along with identification document
- For Foreign entities, all above mentioned documents shall be duly verified and attested by notary public or consul general of Pakistan having jurisdiction over the Client .
- Business profile/organogram with control and ownership structure
- Any other document deemed necessary for identifying Client and its ultimate beneficial owner.

All documents provided by local corporate clients shall be duly attested by company or by notary public where applicable. The Company shall screen the identity information of all directors/Members/Trustees/Authorized persons to open and operate the account/Senior management/Beneficial owners for any possible match with proscribed individuals/entities list (as notified by UNSCR, NACTA, OFAC or any other regulatory body) maintained in AHL Information Management system. The Company shall also verify the CNIC copies provided through NADRA Verisys system.

UBO information shall be:

- Verification of UBO identity using reliable sources
- Reviewed periodically based on risk classification
- Updated whenever there is a trigger event (change in ownership, capital structure, control persons, etc.)

High Risk Instances and Enhanced Procedures to be adopted:

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 due diligence measures on such client:

- A Political Figure, any member of a Political Figure's Immediate Family, and any Close Associate of a Political Figure; Senior management of state owned organization, judicial or military officials.

- Any Client who gives the Compliance Officer any reason to believe that its funds originate from, or are routed through, an account maintained at an "offshore bank", or a bank organized or chartered under the laws of a Non-Cooperative Jurisdiction; and
- Any Client who gives the Compliance Officer any reason to believe that the source of its funds may not be legitimate or may aid terrorist activities such as NGO/NPO, trust, charitable organizations etc.
- Non-resident/Foreign Clients, HNWI clients
- Cash-intensive Business, unusual or excessively complex ownership structure of the company.
- Entities operating in sectors such as dual-use goods, shipping, logistics, chemicals, metallurgy
- Clients located in or dealing with high-risk jurisdictions (Internal List maintained by Company and updated as and when required)
- Use of intermediaries, consultants, or trading companies with unclear economic purpose
- Business relationships and transactions with high risk country known for drug trafficking, high levels of organized crime, vulnerability to corruption or terrorist activity, lax Anti Money Laundering/ Combating the Financing of Terrorism (AML/CFT/CPF) regime or which does not apply or insufficiently applies the Financial Action Task Force (FATF) recommendations or higher risk regions within a country as identified in National Risk Assessment report.

Enhanced Identification Procedures include but are not limited to:

- Assessing the Client's business reputation through review of financial or professional references, generally available media reports or by other means
- Verification of ownership structure and controlling interests
- Understanding the nature of business, supply chains, and cross-border linkages
- 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.
- 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.
- Obtaining additional documentation relating to source of funds and source of wealth
- Obtaining the approval of Senior Management to commence the business relationship.
- Such relationships shall be reviewed at least annually based on client transaction activity.

4. ONGOING MONITORING AND REPORTING PROCEDURES

On-going due diligence is important part of effective and sound ML/TF risk management. Company can only effectively manage its risk if the Company and its employees have

understanding of the normal and reasonable securities market activity of the Client, which enables a company to identify attempted unusual transactions which falls out of the regular pattern of the brokerage business or the nature of business stated by Client at the time of account opening.

Ongoing monitoring is required to be conducted in relation to all business relationships and transactions, but the extent of monitoring is dependent on:

- The results of risk identified in the initial risk assessment at the time of Client identification step (Sample selected based on transaction/trading activity of client during the period as per mechanism defined in AML/CFT/CPF procedures and policy)
- Client identity, type of business and assets, or the Client is reluctant or refuses to reveal any information concerning business activities or its beneficial owner, or the Client furnishes unusual or suspect identification or business documents
- When Client activity significantly deviates from its risk profile and applied threshold's.
- Frequent requests for modification of address, mobile number etc.
- Client (or a person publicly associated with the Client) is the subject of news reports indicating possible criminal, civil or regulatory violations
- Client attempts to make or requests transactions in cash or cash equivalents.
- The customer with a significant history with the brokerage house abruptly liquidates all of his or her assets in order to remove wealth from the jurisdiction
- The customer refuses to identify a legitimate source for funds or provides the brokerage house with information that is false, misleading, or substantially incorrect
- Accounts where authorization to operate the account and issue payment instructions are given to a third party and who has never/rarely visited or contacted the brokerage house
- The customer's address is associated with multiple other accounts that do not appear to be related
- Company has a long period of inactivity following incorporation, followed by a sudden and unexplained increase in financial activities
- Company is registered at an address that is also listed against numerous other companies or legal arrangements, indicating the use of mailbox service
- Company beneficial owners, shareholders or directors are also listed as beneficial owners, shareholders or directors in multiple other companies

AHL requires any Employee who detects suspicious activity or has reason to believe that suspicious activity is taking place are required to immediately inform the Compliance Officer.

In case where Client has no activity performed since last one year and could not be reached, account should be marked dormant with the written instruction on client profile that CDD is required to be performed for reactivation process.

Transaction Monitoring:

The Employees of AHL at front line and second line of defense have to effectively understand the normal and practicable activities of the Client so that they have the means of identifying transactions that have no economic sense or fall outside the regular pattern of client activity.

All complex, unusually large transactions and patterns which have no apparent economic or visible lawful purpose shall be subject to ongoing due diligence. Compliance officer shall prescribe threshold limits of each client and particular attention will be given to the transactions which exceed these limits. Other instances requiring monitoring maybe:

- Client attempts, with unusual frequency (taking into account the differences between Individual and Intermediaries as appropriate), to make investments / withdrawals, or purchases financial or monetary instruments
- The purchase of long term investments followed by a liquidation of the accounts shortly thereafter, regardless of fees or penalties.
- High turnover which is inconsistent with the means of the Client or its previous history may indicate that funds are being 'washed'.
- Frequent/multiple transaction involving parties with the same beneficial owner, which did not make economic sense.
- Large or frequent cash-based transactions, which do not commensurate with the stated business profile/ activities of the Client
- The Client makes a large purchase or sale of a security, or option on a security, shortly before news is issued that affects the price of the security
- Two or more unrelated accounts trade an illiquid or low priced security suddenly and simultaneously.
- Transaction where one party purchases securities at a high price and then sells them at a considerable loss to another party. This may be indicative of transferring value from one party to another
- The securities account is used for payments or outgoing wire transfers with little or no securities activities
- Attempts to open accounts using intermediaries, shell companies, or nominee directors with no clear business justification.
- Requests for changes in beneficial ownership shortly after account opening
- Upon inquiry for justification of inconsistent transactions conducted in the account, apparently vague explanations are provided and no supportive documentary evidence is presented to the company.
- 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
- Co-mingling of business and personal funds without any plausible reason
- Export / Import proceeds and other receipts and payments from/ to unrelated counterparties, which are not in-line with the legal person's business nature

ARIF HABIB LIMITED

- Round Tripping pattern of transactions that confuse the legitimate trading of business and apparently do not provide any economic benefit to the legal person
- Repeated funding of accounts by unrelated third parties or offshore entities without documented justification
- Clients operating in sectors linked to procurement or shipment of dual-use items.
- Use of accounts as pass-through for third-party transfers
- Securities movements between unrelated parties without economic reason

Monitoring of transactions falling below threshold limits shall also be performed as there could be instances where transaction has been restructured to circumvent the applicable threshold.

All identified red flags shall trigger enhanced review, documentation, escalation to Compliance, and when required, reporting to FMU.

Update of KYC Information and Risk Profile:

Based on the risk rating of Clients, Clients of AHL shall be asked on periodic basis to update their KYC profile along with updated information/documentation as an evidence.

This exercise shall also be performed in the light of changes in Company business environment, any change in technologies, products/services offered and relevant new threats emerge.

5. ROLES AND RESPONSIBILITIES

AHL shall enforce the concept of "three lines of defense" as a way to promote compliance culture at all levels in organization by structuring roles, responsibilities and accountability to effectively manage the risk and apply risk based controls.

First Line of Defense:

These are Client facing teams such as Client Service, sales team, Operations department. They are primarily responsible for identifying and controlling the risk by adhering to internal control system and policies and procedures of Company. Employees at this stage must be aware of their legal obligations to recognize and report suspicious activity.

Second Line of Defense:

These are Compliance, risk management departments and others who provide support to first line of defense in compliance matters and continuous staff trainings. They are responsible for developing and implementing policies and procedures, monitoring and reporting to department with the highest accountability on complete company's exposure to risk.

Compliance officer is a part of second line of defense. The Compliance officer shall be responsible to oversee the effectiveness of overall AML/CFT/CPF system including implementation of

policies and procedures and provide guidance to first line of defense regarding compliance of Rules, Regulations, policies and procedures of AML/CFT/CPF.

Responsibilities of Compliance Officer Includes:

- Ensure that operations and business transactions follow all relevant legal and internal controls applied and report the status of effectiveness of AML/CFT/CPF systems and controls to Board of Directors on periodic basis.
- Develop and implement a compliance program to ensure the organization operates in accordance with all applicable Laws and Regulations.
- Create and manage effective action plan in response to audit discoveries and compliance violations
- Perform compliance audits to determine whether establish protocols are being followed and where they can be improved
- Evaluate business activities to assess ML/TF risk and conduct entity wide risk assessment.
- Provide training to employees on regulations and industry practices and address employee concerns or questions on compliance matters
- To liaise with and assist external auditors and inspectors when necessary and responds promptly to requests for information by the Apex Regulators.
- Enterprise-Wide Risk Assessment (EWRA): The Compliance officer shall conduct an enterprise-wide ML/TF/PF risk assessment annually, covering:
    - Customer risks
    - Product/service risks
    - Delivery channel risks
    - Geographic risks
    - Securities-specific risks
    - PF-specific exposure (DPRK/Iran, dual-use sectors)

    The EWRA must be documented, approved by the Board or a designated Committee, and used to update controls and risk classification methodologies.

Third Line of Defense:

The last line of defense is Internal Audit function/Audit Committee. They provide a representation of the overall risk management framework implemented throughout the organization and advice on all matters related to the achievement of objectives and effectiveness of control implemented to the board.

It shall be the responsibility of Internal Audit team to conduct audit of AML/CFT/CPF/PF to evaluate the effectiveness of compliance with regards to AML & CFT policies. In case where any deficiency in the implementation of specific management measures is identified, the internal audit

function should periodically report to the Audit Committee for review, and provide such information to serve as reference in employee training.

6. EMPLOYEE TRAINING PROGRAM

AHL shall ensure that all employees are provided with training they need to perform their jobs safely at all times. The training provided to employees shall include all activities which aim to assist staff to maintain, update and enhance their knowledge, skills as well as professional skepticism which includes a questioning mind and a critical assessment of the appropriateness and sufficiency of information provided by client.

The Company shall ensure that all relevant staff receives training on AML/CFT/CPF/PF regulations and internal control procedures on periodic basis and whenever there are changes in Laws and regulation or Company's business operations.

Training requirements will vary subject to staff roles and job responsibilities and span of employment with the Company. Training course should be tailored to an employee's specific role to ensure that the employee has sufficient knowledge and information to effectively implement the AML/CFT/CPF policies and procedures. Newly hired must attend training sessions as soon as possible after being hired. Revision sessions should be provided to ensure that staff are fully aware of their obligations and have up to date knowledge and expertise.

The Client facing teams shall be provided regular formal and informal trainings to recognize and deal with Clients and transactions which may be related to ML/TF, as well as to identify and report to Compliance officer anything that gives grounds for suspicion. At a minimum training shall cover the following areas;

- AML red flags
- Explaining the relevant law and regulations and placing them in the context of the company's business activities
- Conducting Know your Client/Client due diligence. And Enhanced measures to be adopted where industries and services considered higher than normal risk (e.g. import and export services, Charitable organisations, cash intensive businesses etc.)
- how to deal with suspicious transactions/activities
- Tipping off
- Record keeping

All employees, including front-facing, operations, settlements, risk management and IT staff shall receive:

- Annual TFS/TF/PF training
- Training on sanctions handling, escalation duties, and asset freezing procedures
- Mandatory refreshers upon major regulatory changes

Copies of training materials, including training manual, presentations, attendance register and any other accompanying material such as training log that documents and records the nature of the training undertaken, the date of completion, attendance, employee assessment results, and details of scheduled training shall be retained. Company shall obtain undertaking from its staff confirming that they have attended the AML/CFT/CPF training sessions and understands their obligation to report the suspicious activities under AML/CFT/CPF regulations and that they fully understand the training materials.

Company shall ensure that Compliance officer undergoes a more rigorous and comprehensive program of AML/CFT/CPF training than a regular employee. Training should cover all aspects of the Laws and Regulations applicable on Company, relevant internal control policies, reporting of suspicious activities, and on new trends of criminal activity.

A higher level of training shall be provided to Senior management and Board of directors covering all aspects of risk of ML/TF/PF faced by business, AML/CFT/CPF regulations and internal policies and penalties arising from the non-compliance of relevant laws and regulations.

The Company shall ensure that all member of staff participate in the appraisal / personal development review process with their manager, at least annually, and to take up opportunities that are provided in support of their learning and development needs.

To ensure the continued adherence to AHL's anti-money laundering policies and procedures, all Employees are required to reconfirm their awareness of the contents of this Policy Manual by signing the acknowledgement form annually, or more frequently, as required by the Compliance Officer.

7. RECORDS RETENTION

Company will ensure that all documents pertaining to Client accounts are retained for at least five (5) years or longer where law requires after termination of business relationship to comply swiftly with information requests from the competent authorities. The records so maintained must be sufficient to permit reconstruction of individual transactions (identification of any unusual pattern), so as to provide, if necessary, to law enforcement agencies for investigation or as an evidence in legal proceedings.

AHL will keep all documents obtained during identification procedure of Client, CDD/EDD measures, records of ongoing monitoring, transaction record and all business correspondence including the results of any analysis undertaken for at least five years or longer where law requiredafter relationship is ceased.

AHL shall also maintain records of accounts with whom business relationship is rejected due to non-compliance of Client due diligence process and due to identification in proscribed person/Targeted Financial Sanction.

AHL will retain those records for longer period where Client or transactions relate to litigation or are required by the court of law or by any other competent authority, till such time the company gets permission from those competent authorities to destroy such record.

8. OTHER MATTERS

DORMANT ACCOUNT / BLOCK / SUSPENDED ACCOUNTS:

In case where customer has no activity performed since last five year and could not be reached, account should be marked dormant with the written instruction on client profile that CDD is required to be performed for reactivation process. The Company shall put in place proper controls such that no activity/transaction, deposit and withdrawals performed in dormant account until and unless CDD process has been completed.

Where customer CNIC is expired, fortnightly notices shall be send to its registered email address.

Where customer's identification document such as CNIC/NICOP/Passport not available, account shall be blocked for all withdrawals after one-month prior notice to client

TIPPING OFF:

Tipping-off is the process of letting Client know that he or she is or might be subject of suspicious. Tipping-off can possibly occur at the time of initial contact with client, during transaction processing or when carrying out CDD process for additional information.

AHL, its directors, officers and employees are prohibited by law from intentionally or unintentionally disclosing or "tipping-off" the fact that a suspicious transaction report was or is being filled with the FMU as this can compromise the information gathering and investigation process, and can enable persons to dispose of his/her assets and escape.

All staff of AHL should be aware of their obligations under tipping-off legislation. If the company sufficiently believes that performing the due diligence process will alert or tip-off the Client, it might not pursue the CDD process and directly file the STR with FMU.

Training shall be provided to all members of staff to avoid the circumstances where carrying out CDD process will alert the Client of action being taken by Company. Any unauthorized disclosure of STR will result in Company facing criminal liabilities.

REPORTING OF SUSPICIOUS TRANSACTION REPORT:

Suspicious transaction/activity means that transaction or activity is inconsistent with client risk profile. These unusual large and unjustifiable complex transactions which have no economic sense and gives rise to a reasonable ground of suspicion that it may involve Money laundering and financing of the activities relating to terrorism shall be reported to Compliance officer.

AHL as a reporting entity is required to report suspicious transaction or activity when they suspect or have reasonable grounds for suspicious of ML/TF offence. Reporting of STR is also required in circumstances where a Client fails to provide adequate information/documentation for identification process. AHL shall not form any business relationship with such Clients or shall cease the relationship where there is doubt about the veracity of documents provided and file the STR with FMU.

Where any suspicious transaction/activity is reported to Compliance officer, it is important that Compliance officer put into context AML/CFT/CPF Regulation, Red flag alerts notified by FMU and other factors for assessing such suspicion. All reported transactions shall be evaluated as to whether they seem normal activity of that Client, its business, pattern of previous transaction and other possible connections linking client to client or account to account. Consideration shall be given on the factor that whether transaction is consistent with other business in that specific area or those conducted before.

Some factors which can bring about suspicion or reasonable doubt are as follows:

- Unusual patterns of transactions which have no apparent economic or visible lawful purpose;
- False documents provided to open an account
- Inability or reluctance of a Client to provide necessary information for due diligence purpose;
- Transactions conducted or activity performed or income inconsistent with the Client's profile or source of income provided
- Business transactions connected to a high risk country known for drug trafficking, high levels of organized crime, vulnerability to corruption or terrorist activity, lax Anti Money Laundering/ Combating the Financing of Terrorism (AML/CFT/CPF) regime or which does not apply or insufficiently applies the Financial Action Task Force (FATF) recommendations;
- Unusual / Complex transactions indicative of layering between multiple accounts, individuals and countries.
- A client wants to Settle the debits/margins in cash, the company rejects the transaction
- Two or more one-off transactions seemingly linked
- Client intended to conduct a transaction but subsequent action(s) by company or the client cause it not to be carried out or completed
- The customer makes a large purchase or sale of a security, or option on a security, shortly before news is issued that affects the price of the security.
- The customer is known to have friends or family who work for the securities issuer
- A customer trades in selective scrip just after opening the account and makes sizeable profit in each trade
- A customer trading in small amount of shares suddenly takes a sizable position in a specific scrip and makes a considerable profit on it.
- A Customer earns a sizable profit by generating a considerable portion of market volume in illiquid scrip
- A customer engages in prearranged or other non-competitive securities trading, including wash or cross trades of illiquid or low priced securities
- A customer’s transactions include a pattern of receiving physical securities or receiving incoming shares transfers that are sold with the proceeds wire transferred out of the account
- Two or more unrelated accounts at the brokerage house trade an illiquid or low priced security suddenly and simultaneously.

- Transactions between the same or related parties structured solely so that one side incurs a loss while the other incurs a gain.
- The customer deposits a large number of physical securities at the brokerage house
- The company at issue has experienced frequent or continuous changes in its business structure and/or undergoes frequent material changes in business strategy or its line of business
- The customer's profile does not suggest a legitimate business reason for receiving many third party deposits
- The customer's account is not used for its intended purpose (i.e. used as a depository account).
- An account opened by a person/entity that has the same addresses or contact numbers as of other persons/entities without any apparent economic or plausible reason
- A person/entity maintaining an account apparently associated with a terrorist organization or having similar ideology as of a terrorist organization
- A dormant account suddenly receives a huge deposit or series of deposits followed by cash withdrawals made on regular basis till the funds in the account are reduced to a nominal balance
- The individual conducts a transaction via using a credit instrument or any other negotiable/non-negotiable instrument with a high-risk jurisdiction or a country of specific concern.
- Upon inquiry for justification of inconsistent transactions conducted in the account, apparently vague explanations are provided and no supportive documentary evidence is presented to the company.
- Transactions conducted in the accounts of non-profit or charitable organizations for which there is no apparent economic or plausible reason and the transactions apparently do not match with the regular business activities of the organization
- Use of the accounts of a non-profit organization or charity to collect funds for immediate transfer to a small number of foreign/domestic beneficiaries.
- Movement of funds to/from the areas of frequent military and terrorism activities by non-profit organizations.
- A non-profit organization is involved in charity related activities in the areas of conflict or high-risk jurisdictions
- When any legal person or associated natural person of the legal person is proscribed for terrorism / terrorism financing related activities
- The employee/ director/ signatory/ beneficial owner of the legal person is unusually concerned with the reporting threshold or AML /CFT policies
- Legal Person linked to negative/adverse news or crime (named in a news report on a crime committed or under Law Enforcement investigation/inquiry)
- The complex formation structure that does not commensurate with nature of business activities or where legal person fails to disclose actual beneficial owner
- Frequent/multiple transaction involving entities with the same beneficial owner, which did not make economic sense
- 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.

ARIF HABIB LIMITED

- Clients connected with jurisdictions subject to PF sanctions (notably DPRK and Iran)
- Companies involved in dual-use goods, advanced chemicals, engineering, scientific research, or international procurement

In addition to reporting of STR in above cases, company will also ensure to take appropriate actions such as review of risk rating or entire business relationship itself.

If Company becomes aware that any transaction is conducted by or on behalf of a proscribed individuals/entities and organization, STR will be filled with FMU without delay and such accounts will be freezed. Company will not form any business relationship with the individuals / entities / organizations listed in NACTA or imposed sanctions by UNSCR or other countries.

AHL 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 Compliance officer should ensure prompt reporting in this regard.

AHL shall have internal control system for reporting of suspicious transactions as and when conducted on timely basis. The process for identifying, investigating and reporting of suspicious transactions activities to the FMU is clearly specified in the Company's AML/CFT/CPF standard Operating procedures

SANCTIONS SCREENING AND PROLIFERATION FINANCING CONTROLS

This section outlines the AHL's internal controls, procedures, and responsibilities for preventing, detecting, mitigating, and reporting risks related to Targeted Financial Sanctions (TFS) relating to Terrorism (T), Terrorist Financing (TF), and Proliferation Financing (PF) and ensuring compliance with United Nations Security Council (UNSC) sanctions, SECP AML/CFT/CPF Regulations, Anti-Terrorism Act (ATA) 1997 and internationally recognized terrorism and PF risk-mitigation practices.

The Firm recognizes the vulnerabilities associated with securities brokerage accounts, including transferability, liquidity, and potential cross-border linkages that may be exploited for TF and PF activities.

The Firm strictly prohibits dealing with any customer, counterparty, transaction, or security that is directly or indirectly associated with:

- Persons or entities designated under UNSCRs relating to sanctions and proliferation (notably DPRK and Iran)
- Individuals or entities subject to national designations notified through MOFA/SECP
- Front companies, procurement agents, shell companies, or intermediaries operating for proliferation-sensitive programs and/or Terrorism financing.
- Any activity that may contribute to the acquisition, development, or transportation of nuclear, chemical, or biological weapons, delivery systems, or related materials
- The Firm shall apply risk-based, ongoing, and real-time controls to ensure full compliance with sanctions and PF obligations.

Conducting or attempting any:

- Securities trade, fund movement, settlement instruction, transfer-in/transfer-out, margin deposit, or custodial movement

- If the customer or the counterparty is linked with **TFS-TF or TFS-PF**

Failure to comply with TFS constitutes a violation of law and regulatory directives, and may result in regulatory sanctions, criminal liability, and internal disciplinary action.

SCREENING REQUIREMENTS

- All customers, beneficial owners, authorized persons, directors, trustees, partners, and connected parties shall be screened before the account is opened or activated.
- No account may be approved until Compliance provides screening clearance.
- Periodic screening of the entire customer base shall be conducted.
- Event-Driven Screening Triggered upon: Changes in customer profile, Changes in contact person/authorized person details, New beneficial ownership, Regulatory advisories or updated sanctions lists.

TARGETED FINANCIAL SANCTIONS (TFS) CONTROLS – TERRORISM (TF) AND PROLIFERATION FINANCING (PF)

The Firm shall:

- Ensure mandatory freezing without delay of accounts belonging to individuals/entities designated under UNSCR or ATA.
- Prohibit the provision of any funds, financial services, securities trading or settlement support to designated persons or entities.
- Document the freeze action and maintain an internal freeze register
- Monitor transactions for TF indicators, including:
    - Unusual donations or sudden inflows
    - Third-party payments not aligned with profile
    - Layered securities transactions
    - Pass-through behaviour
    - Accounts used only for funding and immediate withdrawal
- Prohibits account usage by front companies supporting DPRK or Iranian procurement networks
- Prohibits the provision of services to identified clients having Connections with:
    - Maritime/shipping companies under sanctions
    - Dual-use goods manufacturers
    - Logistics chains in high-risk jurisdictions
    - Trading companies with opaque structures
- Securities transfers executed to obscure ownership of PF-linked assets
- Suspicious flows: Large transfers followed by immediate withdrawal, Foreign-linked deposits inconsistent with customer profile or Transactions routed through multiple intermediaries

Where PF/TF suspicion exists, Compliance shall file a STR/SAR to FMU without delay

ARIF HABIB LIMITED

Note: Detailed Due Diligence, Ongoing Monitoring, Risk Mitigation Procedures and other mechanism/matters related to AML/CFT/CPF function are part of Standard Operating Procedures of AML/CFT/CPF Manual.

ARIF HABIB LIMITED