DOCUMENT CONTROL SHEET

Title of Policy	Muhammad Salim Kasmani Securities (Pvt.) limited AML/CFT policies and procedure
Associated Key Risks	Money Laundering, Combating Financing of Terrorism, Proliferation Financing
Policy Owner	MUHAMMAD SALIM KASMANI SECURITIES (PVT.) LTD
Review Frequency	Annual and when needed
Frist Approval Date	JULY 2018
Current Review Date	MAY 2020
Nest Review Date	MAY 2021
Version	4.0
Prepared By	COMPLIANCE OFFICER
Approved by	BOARD OF DIRECTORS

TABLE OF CONTENTS

Glossary

AML	**Anti-Money Laundering**
AOF	**Account Opening Form**
BOD	**Board of Directors**
CCO	**Chief Compliance Officer**
CDD	**Customer Due Diligence**
CDD	**Customer Due Diligence**
CFT	**Countering Financing of Terrorism**
CIF	**Customer Information File**
CNIC	**Computerized National Identity Card**
CTR	**Cash Transaction Report**
EDD	**Enhanced Due Diligence**
FATF	**Financial Action Task Force**
FMU	**Financial Monitoring Unit**
IMS	**Intermarket Securities Limited**
ML	**Money Laundering**
MSK	**Muhammad Salim Kasmani Securities (Pvt.) ltd.**
MSB	**Money Service Business**
NADRA	**National Database and Registration Authority**
NICOP	**National Identity Card for Overseas Pakistanis**
OFAC	**Office of Foreign Assets Control**
PEP	**Politically Exposed Person**
PEPs	**Politically Exposed Persons**
POC	**Pakistan Origin Card**
PSX	**Pakistan Stock Exchange**
RMA	**Relationship Management Application**
RO	**Money Laundering Reporting Officer**
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**

Muhammad Salim Kasmani Securities (Pvt.) Ltd. AML/CFT Policy Statement.

MSK is a small equity brokerage house which caters to select clientele. To limit AML/CFT risk of MSK one product is offered (equity brokerage in ready deliver counter) to only two categories of clients. Individuals (natural person) and Private limited Companies registered in Pakistan (legal person) which have 100% local beneficial ownership. Within natural person no walk-in client is accepted and clients with only reference of existing clients are accepted. MSK will also not accept any clients from countries or jurisdiction which have weak AML/CFT compliance regime and regulatory environment, including countries on the Black list of FATF and any other countries identified by Agencies worldwide.

No employee of any organization which accepts donation is taken as a client due to high risk on money laundering as identified in Pakistan National Risk Assessment 2019. Risk based approach to AML/CFT is adopted where MSK has very limited risk of being used for ML/TF/PL due to limited categories of client, single product, focus on long term investment and low volumes.

In case of clarification or enquiries required please contact our compliance officer (usmansalims@gmail.com)

Introduction, Purpose and Scope

i Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") regime requires financial institutions to understand their Money Laundering ("ML"), Terrorist Financing ("TF") and Proliferation Financing ("PF") risks, adopt and effectively implement an appropriate risk-based ML/TF/PF control framework. By aligning Pakistan's AML and CTF control framework with FATF recommendations,
Pakistan's integration into the global financial system will be facilitated. This is an essential contribution that all RPs can make to the lawfulness, transparency, and long-term solid growth of Pakistan's financial sector supported by strong a capital market and the economy as a whole.

ii Securities and Exchange Commission of Pakistan ("SECP"), in order to maintain the integrity of its regulated financial sector that includes the brokers, insurers, NBFCs and Modarabas notified the Securities and Exchange Commission of Pakistan AML/CFT Regulations, 2018 ("the Regulations"). The SECP AML/CFT Regulations require SECP Regulated Persons (RPs) to establish policies, systems and internal controls to detect and combat ML and TF for preventing the abuse of their financial products and services.

Obligation of MSK in Establishing an Effective AML /CFT Governance and Compliance Regime

i. MSK should understand their ML/FT/PF risk exposure and their obligation of establishing an effective AML/CFT regime to deter criminals from using their financial system for illicit purposes. MSK has develop their own risk-based AML/CFT compliance program to comply with all relevant and applicable laws and obligations.

ii. MSK Board of Directors and senior management are engaged in decision making on AML/CFT policies, procedures and controls, and take ownership of their risk-based compliance program. They are aware of the level of ML/TF/PF risk that MSK is exposed to and evaluate whether it is equipped to mitigate that risk effectively. Directors and senior management guide MSK with respect to appropriate actions and changes needed in the risk control environment for adequately mitigating ML/TF/PF risks identified.

iii. MSK gives due priority to establishing and maintaining an effective AML/CFT compliance culture with written AML/CFT policies. MSK will train its staff to identify suspicious activities and adhere with the internal reporting chain and procedures that needs to be followed.

iv. To oversee the compliance function, MSK will appoint a Compliance Officer ("CO") at the management level. Compliance officer shall have all necessary powers and access to information and will be the point of contact both internally in Compliance matters as well as with the supervisory authorities, including the Commission and the Financial Monitoring Unit ("FMU").

Program and Systems to prevent ML/TF/PF

i. MSK will establish and maintain programs and systems to prevent, detect and report ML/TF/PF. The systems will be appropriate to the size of the MSK and the ML/TF/PF risks to which it is exposed and include

   (a) Policies and procedures to undertake a Risk Based Approach ("RBA")
   (b) Internal policies, procedures and controls to combat ML/TF/PF, including appropriate risk management arrangements
   (c) Adequate systems to identify and assess ML/TF/PF risks relating to customers, products/services, delivery channels and geography (such as higher risk countries or regions within a country)
   (d) Customer due diligence measures (enhanced or simplified due diligence) including identifying customers, beneficial owners and politically exposed person and verifying their identity;
   (e) Ensure screening against all applicable sanctions lists
   (f) Ongoing monitoring of customers and transactions
   (g) Record keeping procedures
   (h) Audit function to test the AML/CFT system
   (i) Screening procedures when hiring employees
   (j) An appropriate employee-training program.

Applying a Risk Based Approach (RBA)

i. MSK will analyse the risk environment of their business to estimate the likelihood of ML/TF/PF occurring based on sub-factors such as customers, products and services and distribution channels.

ii. The RBA will enable MSK to ensure that AML/CFT measures are commensurate to the risks identified and enables efficient allocation of resources. As a part of the RBA, MSK will:
   (a) Conduct a risk assessment to identify and determine the ML/TF/PF relevant to MSK
   (b) Develop and implement a programme containing the procedures, policies and controls used to manage and mitigate those risks.

iii. Under the RBA, where there are higher risks, MSK will take enhanced measures to manage and mitigate those risks; and where the risks are lower, simplified measures will be used.

iv. The process of ML/TF/PF risk assessment has four stages:

   (a) Identifying the area of the business operations susceptible to ML/TF/PF;
   (b) Conducting an analysis in order to assess the likelihood and impact of ML/TF/PF;
   (c) Managing the risks; and
   (d) Regular monitoring and review of those risks.

Risk Assessment of the Entity

i. MSK will create and updated AML/CFT Risk Assesment that describes its current assessment of its ML/TF/PF risk in light of the latest National Risk Assessment. This document will be formally approved by the management and board of directors of the MSK and provide a list of proposed actions if any, needed to address any deficiencies in risk mitigants, controls processes and procedures identified by the assessment. In addition, the document will include a view on the AML/CFT risks with respect to its customers, products, delivery channels, geography and the quality of the MSK risk mitigants, such as controls processes and procedures involving more detailed steps.

ii. The ML/TF/PF risk assessment is not a one-time exercise and will be carried out annually (or as directed by SECP). Further, the MSK management will review the risks w.r.t to new products or services, opening or closing accounts with high-risk customers and mergers and acquisitions.

iii. Risk Assessment will be used to develop Risk Matrix that grades customers, products, geography, and delivery channels into risk categories. Each customer will receive an initial AML/CFT risk rating at the beginning of the business relationship, and it must be kept current based on updates and changes in the relationship. For example, if a customer is inactive over a longer period of time, his risk rating may need to be revised.

Monitoring AML/CFT Systems and Controls

i. MSK will monitor the AML/CFT risks as they may change or evolve over time due to certain changes in risk factors, which may include changes in customer conduct, products offered and their characteristics, development of new technologies in the markets or there use by the MSK itself and new sanctions.

ii. MSK will assess the effectiveness of their risk mitigation procedures and controls, identify areas for improvement and update their systems as appropriate to suit the change in risks. This will allow MSK to manage their AML/CFT risk effectively. For this purpose, MSK will monitor;
   (a) changes in customer profile or transaction activity/behaviour in the normal course of business including incidents related to suspicious transactions and terrorist financing sanctions (TFS);
   (b) changes in risk relative to countries and regions to which the MSK or its customers are exposed;
   (c) the potential for abuse of products and services because of their size, unusual patterns, ambiguity and complexity;
   (d) deficiencies in internal cooperation and coordination mechanisms, and employee awareness of their roles in AML/CFT compliance and other functions/areas; and
   (e) the selection, training and performance of agents, intermediaries and third parties who are in any way involved in the AML/CFT processes of MSK

New Products and Technologies

i. MSK in coordination with compliance function will have systems in place to identify and assess ML/TF/PF risks that may arise from new and pre-existing product such as:
   (a) New products, markets or sales channels;
   (b) New internal organization or new offices and departments;
   (c) New data and transaction screening systems and verification of documentation:

ii. MSK will 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. MSK will update policies and procedures to prevent the misuse of technological development in ML/TF schemes, and avoid or mitigate all technologies that favour anonymity. Limitations on the use of non-face to

face business, or on virtual business, may be adequate to avoid opening up of alternative possibilities for ML/TF and fraud, especially in industries of higher risk according to National Risk Assessment, such as brokerage.

iv. Use of modern technology can strengthen AML/CFT measures, being a small house with limited resources MSK will try to implement software where feasible to reduce time consumed for AML/CFT regime and also to introduce a paperless culture to keep up with latest trends.

Customer Due Diligence (CDD)

i MSK will take steps to know who all their customers are. MSK will not keep anonymous accounts or accounts in fictitious names. MSK will take steps to ensure that their customers are who they purport themselves to be.

ii MSK will 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.

iii MSK shall try to verify the identification of a customer using reliable independent source documents, data or information which may inclue verification of CNICs from NADRA Verisys/Biometric. MSK will make maximum effort to identify and verify the customer's beneficial owner(s) to ensure that MSK understands who the ultimate beneficial owner is.

iv MSK shall try to identify and verify the identity of any person that is purporting to act on behalf of the customer. MSK shall ascertain the reason for such authorization and obtain a copy of the authorization document.

v When performing CDD measures in relation to customers that are legal persons or legal arrangements, MSK will collect documents to identify and verify the identity of the customer and understand the nature of its business, and its ownership and control structure.

vi MSK will assess each customer's risk to allow for correct application of enhanced due diligence, standard, simplified or special measures for PEPs and other designated categories as per the Regulations. Necessary minimum customer risk rating categories are:

(a) High
(b) Moderate
(c) Low
(d) PEP

vii MSK is entitled to ask customers all relevant CDD questions and may refuse business if the necessary questions are not answered, or the necessary data and documents are not provided.

viii If MSK has doubts about the veracity or adequacy of the information provided, it will not start a business relationship, or provide a financial service, and will consider making a suspicious transaction report (STR).

Timing of Due Diligence

a) Establishment of a Business Relationship

i. Customer Due Diligence and verification will be undertaken when establishing the business relationship and before any financial service or transaction occurs.

ii. MSK may complete verification after the establishment of the business relationship as soon as is practicable where the risks of ML/TF/PF are low.

iii. Examples of the types of circumstances where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business, include:
(a) Non face-to-face business;
(b) Securities transactions. In the securities industry, intermediaries may be required to perform transactions very rapidly according to the market conditions at the time the customer is contacting them and the performance of the transaction may be required before verification of identity is completed.

iv. When MSK unable to complete and comply with CDD requirements as specified in the Regulations, it will not open the account, commence a business relationship, or perform the transaction. If the business relationship has already been established, MSK shall terminate the relationship. Additionally, MSK shall consider making a STR to the FMU depending on the circumstances

b) Due Diligence of Existing Customers

i. Existing customers are to be assigned a risk rating based on the Risk Matrix which MSK (based on guidelines by SECP) has created together with MSK Risk Assessment in its Risk based Approach.

ii. MSK will apply CDD measures to existing customers on the basis of materiality and risk and will conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken, and the adequacy of data obtained.

iii. The CDD requirements entails that if MSK has a suspicion of ML/TF/PF 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.

iv. MSK is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information.

v. MSK will consider filing a suspicious transaction report if there are any indicators that support such an action.

c) Tipping-off and Reporting

If MSK form a suspicion of ML/TF/PF while conducting CDD or ongoing CDD, they will take into account the risk of tipping-off when performing the CDD process. If MSK believes that performing the CDD or on-going process will tip-off the customer, it may choose not to pursue that process and may file a STR. MSK will ensure that their employees are aware of these issues when conducting CDD or ongoing CDD.

Beneficial Ownership (BO)

i The Beneficial Owner is the natural person at the end of the chain who ultimately owns or controls the customer. The definition of BO in the Regulations is as below:
"beneficial owner" in relation to a customer of a regulated person means, the natural person who ultimately owns or control a customer or the natural person on whose behalf a transaction is being conducted and includes the person who exercise ultimate effective control over a person or a legal arrangement".

ii For legal persons or arrangements, it is essential to understand the ownership and control structure of the customer. This may be done based on plausibility and records. In any case of lack of transparency or doubt, or higher risk, verification is needed. For legal persons, the primary source for verification of ultimate beneficial ownership is the Register of Ultimate Beneficial Ownership.

iii MSK will adopt a risk-based approach to the verification of beneficial ownership of a customer. Identifying beneficial ownership of a customer is an obligation that must be satisfied, regardless of the level of risk associated with that customer.

iv MSK will assess different levels of money laundering/terrorism financing risks posed by their customers' beneficial owners. For example, MSK will consider whether a beneficial owner is a politically exposed person or has links with a high-risk country or region.

v If MSK has doubts about the veracity or adequacy of the information provided, it will not start a business relationship, or provide a financial service, and will consider making a suspicious transaction report to FMU.

Enhanced CDD Measures ("EDD")

i. Where the risks of ML/TF/PF are higher, or in cases of unusual or suspicious activity, MSK will conduct enhanced CDD measures, consistent with the risks identified. In particular, MSK will increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

ii. In all cases where the connection between a customer and his source of income or wealth is very disparate, consider whether the customer is acting on his own behalf or may be a close associate acting for another party, e.g. a PEP. This is particularly relevant for any person with no discernible source of income and a high living standard, such as housewives, children or students. Close Associate is defined as:
"Close Associates" means any natural person who is known to hold,-
(i)joint ownership or control of a legal instrument with a politically exposed person, or
(ii) any other close business or personal relationship with a politically exposed person, or
(iii) ownership or control of a legal instrument or a person which is set up for the benefit of a politically exposed person.

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

(a) Obtaining additional information on customer (e.g. occupation, intended nature of business, volume of assets, information available through public databases, internet, etc.);
(b) Updating more regularly the identification data of applicant/customer and beneficial owner.
(c) Obtaining additional information on the intended nature of the business relationship, source of funds or source of wealth, reasons for intended or performed transactions;
(d) Obtaining the approval of senior management to commence or continue the business relationship.

a) Source of Funds and Source of Wealth

i. MSK will try to establish that the transaction is within the financial means of the customer. The information that should be obtained should give an indication as to the volume of wealth the customer is reasonably expected to have, and how it was acquired.

ii. Once the client's net worth is established, information may be obtained as to where it came from i.e. inheritance, employment, business, investment etc. MSK may rely on publicly disclosed information if such information is available to verify the information.

iii. Understanding the customer's source of funds and their overall financial situation does not mean full proof of all monies, but it does mean that the MSK has asked and tried to validated the financial position. The same applies to housewives and students, where the income of the person or family that sustains them must be documented, otherwise the due diligence is not complete.

iv. For PEPs, and other HNWI, as well as higher risk customers, the requirement covers source of wealth. This means that not only the source of the funds for the current specific transaction should be understood, but that the overall wealth of the customer needs to be understood. This means a view of the overall ownerships and earnings of the client, to understand his assets and holdings in a complete overview, and be able to estimate his total wealth to some extent.

Special Cases of Higher Risk & Enhanced Due Diligence

a) **Politically Exposed Persons (PEPs)**

i. PEPs are defined in the Regulations, inter-alia, as heads of state, ministers, influential public officials, judges and military commanders and includes their family members and close associates.

ii. Business relationships with PEPs holding important public positions may expose MSK to significant reputational and/or legal risk. In addition, PEPs because of their position, may expose MSK and their business partners to a high degree of public expectation and scrutiny.

iii. Family members of a PEP are individuals who are related to a PEP either directly or through marriage. Close associates are individuals who are closely connected to PEP, either socially or professionally. Close associates have in many cases been used to provide a cover for the financial activities of a PEP, and may not be in any way connected to the PEP in an official capacity. The CDD done by MSK on the source of funds or source of wealth of a customer may be the first clear documentation of a close association.

iv. The AML/CFT National Risk Assessment of Pakistan has determined the risk of corruption and therefore the risk of providing financial services to PEPs is high. This means that all domestic PEPs must be scrutinized, particularly for their source of funds wealth and assets.

v. MSK is obligated to ascertain whether their customer is a PEP. In assessing the ML/TF risks of a PEP, MSK shall consider factors such as whether the customer who is a PEP:
   (a) Has prominent public functions in sectors known to be exposed to corruption;
   (b) Has business interests that can cause conflict of interests (with the position held);
   (c) Has been mentioned in media related to illicit financial behaviour; and
   (d) Is from a high-risk country.

vi. In very low risk scenarios declaration may be sufficient. In higher risk scenario, a search of publicly available information, such as internet public sources or commercial databases is necessary.

vii. The PEP red flags that MSK shall consider include:
   (a) The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;
   (b) A family member of a PEP without own financial means is transacting with the MSK without declaring the relationship to a PEP, or the origin of the funds transacted;
   (c) The PEP is associated with, or owns, or signs for, complex legal structures that are commonly used to hide Beneficial Ownership;
   (d) Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;
   (e) A PEP uses multiple bank accounts for no apparent commercial or other reason;

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

viii. MSK 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 RPs should consider include:
(a) the level of (informal) influence that the individual could still exercise; and
(b) 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, or through continued strong ties within a party, family or institution).

ix. MSK shall stay vigilant in relation to domestic PEP. MSK in addition to performing normal due diligence measures should also:
(a) have appropriate risk management systems to determine whether the customer is a PEP;
(b) obtain senior management approval for establishing business relationships;
(c) take reasonable measures to establish the source of wealth and source of funds; and
(d) conduct enhanced ongoing monitoring of the business relationship.

b) **Non-Profit Organizations (NPOs)**

As already defined in AML/ CFT policy statement MSK will not accept as client any NPO or an employee of NPO due to high risk of money laundering they pose, which is also mentioned in Pakistan National Risk Assessment

c) **High Net Worth Individuals (HNWI)**

i. High net worth individuals can expose the MSK to higher risk of financial transactions that may be illicit. MSK shall consider clients with investment portfolio higher than 150 million Pak Rupees as high net worth individuals.
ii. MSK will scrutinize HNWI customers to determine, whether they carry a higher risk of ML/TF/PF and require additional due diligence measures. Such scrutiny must be documented and updated as part of the Risk Assessment of the RP.

d) **High-Risk Countries & Higher Risk Regions within a country**

i. Certain countries, or regions within countries have a specific higher AML/CFT risk profile. Examples are border regions, large goods transit points such as ports, or regions experiencing social unrest, that can be associated with specific crime patterns such as cash or people smuggling, drug trafficking, violent crimes, fraud and corruption, and consequently pose a higher potential risk to the RP. Conducting a business relationship with a customer from such a country/region exposes the RP to risk of channelling illicit money flows.
ii. Certain Regions in our country have a specific higher AML/CFT risk profile such as western border region of Pakistan and some areas of south Punjab (based on Pakistan National Risk Assesment). List of these areas with higher risk will be developed and updated annually and clients from these areas will be treated as high risk of AML/CFT.
iii. Individuals clients from countries which are black listed by FATF will not be accepted as clients by MSK
iv. Individual clients from countries which have weak AML/CFT oversight will not be accepted as a client by MSK. This will be decided on a case to case basis by the senior management based on the recommendation of compliance officer and only after conducting enhanced due diligence
v. MSK will consider among the other sources, sanctions issued by the UN, the FATF high risk and non-cooperative jurisdictions, the FATF and its regional style bodies (FSRBs) and Transparency International Corruption Perception Index (TI CPI).
vi. MSK will only consider natural persons with Pakistan decent to become clients. MSK will not accept any foreign Legal Person as client to reduce AML/CFT risk.

Simplified Due Diligence Measures (SDD)

i. MSK will conduct SDD in case of lower risks identified by MSK in line with latest National Risk Assessment. While determining whether to apply SDD, MSK will consider the level of risk assigned to the relevant sector, type of customer or activity as mentioned in the latest National Risk Assessment.

ii. Using SDD measures may include:
   (a) reducing the frequency of customer identification updates;
   (b) reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold;
   (c) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transaction or business relationship established;
   (d) undertaking verification after establishment of the business relationship;
   (e) less stringent steps to verify the Beneficial Owner.

Reliance on Third Parties

i. When another domestic financial sector entity, e.g. a bank or an RP, has already established a relationship with a customer, MSK may rely on the CDD performed by that other party. This only applies if the information and CDD is shared directly between MSK and the other entity.

ii. MSK may rely on the initial CDD information provided by another financial institution in Pakistan, where the third party is regulated and supervised by SPB or SECP and where MSK can immediately obtain necessary information from the third party.

iii. The ultimate responsibility for the CDD and the other AML/CFT obligation remains with the MSK for the business they conduct with the customer, and covers all other obligations mentioned in this guideline.

On-going Monitoring of Business Relationships

i. Once the identification procedures have been completed and the business relationship is established, MSK will monitor the conduct of the relationship to ensure that it is consistent with the nature of business stated, when the account was opened.

ii. In all cases, the transactions of the customers will be monitored, scrutinizing the transactions undertaken throughout the course of the business relationship by recognizing unusual patterns or large transactions and unusual money flows.

iii. MSK will try to ensure that CDD data or information is kept up-to-date by undertaking routine reviews of existing records. MSK will update customer CDD records within the 2 years based on the level of risk posed by the customer or on the occurrence of a triggering event, whichever is earlier. Examples of triggering events include:
   (a) Material changes to the customer risk profile or the way that account usually operates;
   (b) MSK lacks sufficient or significant information on a particular customer;
   (c) Where a significant transaction takes place;
   (d) Where there is a significant change in customer documentation standards;
   (e) Significant changes in the business relationship;
   (f) Transaction restructuring to circumvent the applicable threshold.

iv. Annex 1 and 2 gives some examples of potentially suspicious activities or "red flags" for ML/TF/PF, enabling MSK to recognize possible ML/TF/PF schemes. 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.

v. In case a customer has no active business with MSK, and cannot be reached, or refuses to engage in updating because there is no active business, account should be marked inactive with the instruction that relationship cannot be re-activated without full CDD.

vi. In case due diligence cannot be updated, a formal ending of the relationship would be done by following the legal process for ending a customer relationship under the applicable laws.

vii. MSK will apply ongoing CDD measures to existing customers on the basis of materiality and risk, and will conduct due diligence on such existing relationships at appropriate times, taking into account CDD measures previously undertaken, and the adequacy of data obtained.

viii. Transaction of all clients of MSK will be monitored on a daily basis by the compliance officer and the support staff to detect any unusual activity which warrant further review for ML/TF/PF risk.

Record-Keeping Procedures

i. MSK will ensure that all information obtained in the context of CDD is recorded. This may includes:
   (a) Documents provided to the MSK when verifying the identity of the customer or BOD
   (b) Verification of CNIC through NADRA Verisys/ Biometric;
   (c) Transcription into the MSK own IT systems of the relevant CDD information.

ii. MSK will maintain, for at least 10 years after termination of the business relationship, all necessary records on the customer and their 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.

Reporting of Suspicious Transactions

i. MSK will 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. Activities requiring further enquiry may fall into one or more of the following:
   (a) any unusual financial activity of the customer not in line with the customer's profile;
   (b) any unusual transaction in the course of some usual financial activity;
   (c) any unusually-linked transactions;
   (d) any unusual method of settlement;
   (e) unexplained unwillingness to provide the information requested.

ii. Where the enquiries conducted by the MSK do not provide a satisfactory explanation of the transaction, it may be concluded that there are grounds for suspicion requiring disclosure and escalation of matters to the CO who will decide whether to file a suspicious transaction report based on the above. If it decides not to file, reasons must be documented for this decision.

iii. MSK will refuse business that they suspect, might be criminal in intent or origin. Where a customer is hesitant/fails to provide adequate documentation, filing a STR will also be considered. Also, where an attempted transaction gives rise to knowledge or suspicion of ML/TF/PF, that attempted transaction will be reported to FMU

iv. If MSK decides that a disclosure should be made, STR will be reported to the FMU without delay through GoAML portal of the FMU.

v. After concluding an internal enquiry, or making an STR, the MSK will decide whether to close the enquiry, take additional steps such as higher risk rating of customer, or ending the business relationship. This decision will be documented with an explanation for the reasoning behind it.

vi. MSK will report total number of STR filed to commission on bi-annual basis within seven days of close of each half year

vii. MSK will maintain record of AML/CFT reports of internal enquiries and reporting to FMU. Such documentation may include:
   (a) the report itself and all its attached information / documents in copy;
   (b) the date of the report;
   (c) the person who made the report and the recipient;
   (d) any decision based on the STR for the specific customer or a group of customers;
   (e) any updating or additional documentation taken based on the report; and
   (f) the reasoning underlying the decisions taken.

Implementation of UN Security Council Resolutions

i. Sanctions are prohibitions and restrictions put in place with the aim of maintaining or restoring international peace and security. They generally target specific individuals or entities, or particular sectors, industries or interests. They may be aimed at certain people and targets in a particular country or territory, or some organization or element within them.

ii. MSK will 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.

iii. The United Nations Security Council's (UNSC) relevant Committee established in pursuance of Resolution 1267 (1999) and successor resolutions concerning ISIL (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities, approves the addition, amendments and deletion of individuals and entities subject to assets freeze, travel ban and arms embargo as set out in the UNSC resolutions adopted under Chapter VII of the UN Charter.

iv. The Government of Pakistan under the United Nations (Security Council) Act, 1948 gives effect to the decisions of UNSC whenever the Consolidated List maintained by the relevant Sanctions Committee is updated. The Ministry of Foreign Affairs issues Statutory Regulatory Orders (SROs) to provide legal cover for implementing sanction measures under UNSC resolutions. These SROs in respect of designated individuals/ entities require assets freeze (including funds and other financial assets or economic resources), travel ban and arms embargo, in addition to other measures in accordance with the UNSC resolutions. These SROs are available at the following links:
   (a) http://mofa.gov.pk/unsc-sanctions/
   (b) http://www.secdiv.gov.pk/page/sro-unscr-sanctions

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

vi. MSK will immediately scan its customer data bases and their Beneficial Owners /associates for any matches with the stated designated/proscribed person(s)/entity(ies) on the receipt of notifications; issued by the Ministry of Foreign Affairs on United Nations Security Council Resolutions or intimation from National Counter Terrorism Authority/Law Enforcement Agencies/ Home Departments of Provinces/Ministry of Interior regarding updates in list of proscribed persons under the Anti- Terrorism Act, 1997. In case of a true match or suspicion of a proscribed/designated person the following actions shall be immediately taken by MSK

(a) if it is an existing customer, freeze without delay the customer's fund and other financial assets or economic resources / policy or block the transaction, without prior notice;
(b) Reject the customer, if the relationship has not commenced;
(c) Lodge a STR with the FMU, and simultaneously notify SECP and the Ministry of Foreign Affairs in case that person is designated under United Nations Security Council Resolutions, or the National Counter Terrorism Authority ("NACTA") in case that person is designated under the Anti-Terrorism Act, 1997

vii. MSK will ascertain potential matches with the UN Consolidated List to confirm whether they are true matches to eliminate any "false positives". MSK may 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 for suspicion that customer/ funds belong to sanctioned entity/ individual, MSK may consider raising an STR to FMU.

viii. MSK will make their sanctions compliance program an integral part of their overall AML/CFT compliance program. When conducting risk assessments MSK will, take into account any sanctions that may apply (to customers or countries).

ix. MSK will not provide any services to proscribed/ designated entities and individuals or their associated persons as required under the Regulations. For this purpose, necessary measures will be taken including but not limited to the following controls:
(a) In case of entity accounts, it should be ensured that their beneficial owners, directors, members, trustees and authorized signatories are not linked with any proscribed/ designated entities and individuals, whether under the same name or with a different name.
(b) The association of individuals/entities with proscribed/designated entities and individuals may be determined on the basis of appropriate screening of sanctions lists, publicly known information or linkages (on the basis of Government or regulatory sources, reliable media information, etc.)
(c) While opening new accounts or extending services to customers, any similarity between the identifying information of the customer and that of proscribed/ designated entities and individuals including national identification number, address, etc. may be viewed with suspicion and properly investigated for necessary action as per requirements.
(d) MSK will monitor their relationships on a continuous basis and ensure that no such relationship exists. If any such relationship is found, immediate action shall be taken as per law, including reporting to the FMU.
(e) MSK will report to the FMU and the Commission immediately, all attempted or rejected transactions or account opening requests pertaining to proscribed/ designated entities and individuals and their associates.
(f) MSK will maintain up to date data of all frozen assets/ funds, attempted or rejected transactions or account opening requests, and the same shall be made available to the Commission as and when required.

x. MSK will try to carry out checks on the names of potential and new customers, as well as regular checks on the names of existing customers, beneficial owners, transactions, and other relevant parties against the names in the abovementioned lists, to determine if the business relationship involves any sanctioned person/entity, or person associated with a sanctioned person/entity/country.

xi. MSK will try to keep track of all the applicable sanctions and where the sanction lists are updated, shall ensure that existing customers are not listed. The Consolidated Lists available at NACTA's and the UNSC Sanctions Committees' websites, are regularly updated and can be accessed at the following links:
(a) https://www.un.org/securitycouncil/content/un-sc-consolidated-list
(b) https://scsanctions.un.org/search/
(c) https://www.un.org/securitycouncil/sanctions/1267
(d) https://www.un.org/securitycouncil/sanctions/1988
(e) https://www.un.org/securitycouncil/sanctions/1718
(f) https://www.un.org/securitycouncil/content/2231/background
(g) https://nacta.gov.pk/proscribed-organizations-3/
(h) https://nacta.gov.pk/pp/
(i) https://nfs.punjab.gov.pk/

xii. MSK will inform and educate their customers that in case of wrongful or inadvertent freezing, they may apply in writing for de-listing to Federal Government through relevant Ministry or to the UN's Ombudsman, as the case may be.

Internal Controls (Compliance Function, Audit Function, Employee Screening, Ongoing Training Program and Outsourcing)

i. MSK will develop systems and controls that are comprehensive and proportionate to the nature, scale and complexity of their activities and the ML/TF/PF risks identified. MSK will establish and maintain internal controls in relation to:
   (a) compliance management arrangements;
   (b) screening procedures to ensure high standards when hiring employees;
   (c) an ongoing employee training programme; and
   (d) audit function to test the system.

ii. MSK will establish the following three lines of defence to combat ML/TF/PF

iii. **a) First line of defence: Sales and Back office**

Sales, Back Office and settlement is the first line of defence, where for each decision or approval, they need to determine and ensure that sufficient resources are provided for carrying out policies and procedures related to AML/CFT due diligence.

As part of first line of defence, management must create and approve policies and procedures that are clearly specified in writing, and communicated to all employees. They should clearly describe obligations and instructions for employees, as well as guidance on compliance with the Regulations. There should be internal procedures for detecting, monitoring and reporting suspicious transactions.

b) Second line of defence*:* Compliance Officer and Compliance Function

Compliance Officer, back office, internal control, risk management functions and technology are the second line of defence.

As part of second line of defence, the Compliance Officer has the authority oversee the effectiveness of MSK AML/CFT systems. His responsibilities include compliance with applicable AML/CFT legislation, reporting of suspicious and currency transactions, and providing guidance in day-to-day operations of ~~theAML~~the AML/CFT policies and procedures, including freezing of accounts/funds if subsequently identified on proscribed lists. Compliance Officer must be a person who is fit and proper to assume the role and who:

(a) has sufficient skills and experience to develop and maintain systems and controls (including submitting written policies and procedures for management's approval);
(b) reports directly and periodically to the Board of Directors, Chief Executive or equivalent competent authority on AML/CFT systems and controls;
(c) has sufficient resources and access to all information and data within the RP necessary for performing the AML/CFT compliance function;
(d) ensures independent audit of the AML/CFT program;
(e) maintains or ensures maintenance of various logs, as necessary, with respect to declined business/rejected transactions, internal investigations, suspicious transaction reports, and freezing or blocking of payments under Sanction Regime;
(f) responds promptly to requests for information by the SECP/LEAs.

c) Third line of defence: Internal Audit Function

Given the overall size of MSK equity brokerage operation and limited resources available, it not feasible to establish a independent internal audit function. The internal audit function will be performed by the compliance officer through the use of technology and will be on a continuous basis throughout the year. The compliance

officer will conduct AML/CFT inspections to evaluate the effectiveness of compliance with AML/CFT policies and procedures

iii. **Employee Screening**

(1) MSK will screen prospective and existing employees to ensure high ethical and professional standards.

(2) Employee screening will be conducted periodically where a suspicion has arisen as to the conduct of the employee. MSK will try to 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, following factors would be considered.

- references provided by the prospective employee at the time of recruitment;
- employee's qualifications, employment history, and professional memberships;
- details of any regulatory actions or actions taken by a professional body and the existence of any relevant criminal convictions.

(3) MSK will screen all employees periodically against proscribed and Targeted Financial Sanctions lists.

iv. **Employee Training**

(1) MSK will ensure that all concerned staff receive training on ML/TF/PF prevention on a regular basis, at least annually or more frequently where there are changes to the regulatory requirements or where there are significant changes to the MSK business operations or customer base. MSK will ensure that all staff fully understand the procedures and need for compliance with the regulations.

(2) Senior management (including Board of Directors and Compliance Officer) would receive a higher level of training covering all aspects of AML/CFT procedures, including the offences and penalties arising from non-compliance with relevant laws.

v. **Outsourcing to Third Parties**

(1) MSK will conduct due diligence on the proposed service provider and also ensure that the service provider (OSP) is fit and proper to perform the activity that is being outsourced.

(2) MSK will ensure that a written outsourcing agreement clearly sets out the obligations of both parties, including contingency plan to exit the arrangement in case OSP fails to perform outsourced activity.

(3) The OSP will report regularly to the MSK within the timeframes as agreed upon with MSK. MSK will have access to all the information or documents relevant to the outsourced activity maintained by the OSP.

Risk Assessment and Applying a Risk Based Approach - (Based on SECP Policy Guidelines April 2020):

MSK will conduct AML/CFT Risk Assessment and Compliance Assessment based on the Guidelines provided by SECP mentioned below (including Risk Assessment Tables and Compliance Assessment Check lists.)

Identification, Assessment and Understanding Risks

i. Before undertaking an ML/TF/PF risk assessment, MSK will consider the following guidance material to determine the level of risk involved in relation to customers, products/services, delivery channels and countries/regions:
   (a) Latest National Risk Assessment;
   (b) Sector Risk Assessment guidance by the SECP;
   (c) Any applicable guidance by relevant authorities (such as FMU, SBP, MoFA, NACTA etc.);
   (d) information and guidance published by international organisations such as the FATF, APG;
   (e) MSK business experience in relation to certain risks.

ii. As part of assessing risk, MSK will identify inherent risks which are ML/TF/PF risks present before any controls and mitigations. MSK may assess residual risk (the risk after your controls and mitigations) as part of risk assessment.

The first step in assessing ML/TF/PF risk is to identify the risk categories, i.e. customers, countries or geographical locations, products, services, transactions and delivery channels that are specific to the MSK. The significance of different risk categories may vary from institution to institution, i.e. MSK may decide that some risk categories are more important to it than others.

iii. In the second stage, MSK will assess and analyse the ML/TF/PF risks that can be encountered as a combination of the likelihood that the risks will result in an ML/TF/PF event taking place and the impact of cost or damages resulting from the event. The impact can consist of financial loss to the MSK from the crime, monetary penalties from regulatory authorities or the cost of enhanced mitigation measures.

Approach to Risk Assessment

i. The size and complexity of your business plays an important role in how attractive or susceptible it is for ML/TF/PF risk. For example, because a large business is less likely to know its customers individually, it could offer a greater degree of anonymity than a small business. Likewise, a business that conducts complex transactions across domestic and international jurisdictions could offer greater opportunities to money launderers.

ii. For low risk environment, RPs may want to assess risk by only considering the likelihood of ML/TF/PF activity. This assessment should involve considering each risk factor that has been identified, combined with business experience, and guidance available through SECP, latest National Risk Assessment (NRA) for Pakistan, and international organizations such as the FATF. The likelihood rating could correspond to:
   (a) Unlikely - There is a small chance of ML/FT/PF occurring in this area of the business;
   (b) Possible - There is a moderate chance of ML/FT/PF occurring in this area of the business;
   (c) Almost Certain - There is a high chance of ML/FT/PF occurring in this area of the business

Notwithstanding the low risk environment the RP may have identified that one of its products is vulnerable to ML/TF/PF due to the potential for cross- border movement of funds. The risk assessment highlights this product as being easily accessible and is being used by many customers in higher -risk jurisdictions. Combined with domestic and international guidance, the RP assesses that the inherent risk rating of this product is high. The AML/CFT Compliance officer/department should then address this likely risk with appropriate control measures. MSK will need to do this with each of the identified risks.

Applying the Risk Assessment

i. The risk assessment should help rank and prioritize risks and provide a framework for managing those risks. The risk assessment must enable RPs to prepare a comprehensive program for meeting relevant obligations under the regulations, including obligations to conduct CDD, monitor accounts and activities and report suspicious activity. For instance, RPs may consider unexpected international activity of a domestic-based customer unusual, especially if it involves a high-risk jurisdiction, and should submit an STR.

ii. RPs must conduct ongoing CDD. The risk assessment will help target and prioritize the resources needed for ongoing CDD. For instance, RPs may want to undertake ongoing CDD on high-risk customers on a more regular basis than on lower-risk customers.

iii. RPs must undertake account monitoring. The risk assessment will help you design the triggers, red flags and scenarios that can form part of account monitoring. For instance, you may want the activity of a high-risk customer in a high-risk jurisdiction (as identified in the risk assessment) to be subject to more frequent and in-depth scrutiny.

New and Developing Technologies and Products

i. New and developing technologies and products can present unknown ML/TF risks and vulnerabilities. In addition, new methods of delivery may be able to bypass existing AML/CFT measures to allow anonymity and disguise beneficial ownership. The risk assessment should consider whether the business is, or may exposed to customers involved in new and developing technologies and products. The program should detail the procedures, policies and controls that RPs will implement for this type of customer and technology.

Material Changes and Risk Assessment

i. The risk assessment should adapt when there is a material change in the nature and purpose of the business or relationship with a customer. A material change could present an increase, or decrease in ML/TF/PF risk.

ii. Material change could include circumstances where MSK introduce new products or services or have customers (or their beneficial owner) based in new jurisdictions. Material change can include when MSK starts using new methods of delivering services or have new corporate or organizational structures. It could result from deciding to outsource CDD functions or changing the processes for dealing with PEPs. In these circumstances, MSK may need to refresh their risk assessment.

iii. MSK will document their risk assessment in order to be able to demonstrate their allocation of compliance resources. An effective risk assessment is an ongoing process. Risk levels may change as new products are offered, as new markets are entered, as high-risk customers open or close accounts, or as the products, services, policies, and procedures change. MSK will therefore update the risk assessment every 12 months to take account of these changes and will have appropriate mechanisms to provide risk assessment information to the Commission, as required.

Examples of Risk Classification Factors

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

i. **Customer risk factors**: The institution must list and describe all types or categories of customers that it provides business to and should make an estimate of the likelihood that these types or categories of customers will misuse the RP for ML/TF/PF and could be considered to be high risk. Risk factors that may be relevant when considering the risk associated with a customer or a customer's beneficial owner's business include:
   (a) The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the RP and the customer).
   (b) Non-resident customers.
   (c) Legal persons or arrangements
   (d) Companies that have nominee shareholders.
   (e) Business that is cash-intensive.
   (f) Ownership structure of the customer appears unusual or excessively complex given the nature of the customer's business such as having many layers of shares registered in the name of other legal persons.
   (g) Politically exposed persons.
   (h) shell companies, especially in cases where there is foreign ownership which is spread across jurisdictions.

(i) trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets.

(j) NGO
(k) Requested/Applied amount of business does not match the profile/particulars of client.
(l) Designated Non-Financial Business and Professions: real estate dealers, dealers in precious metal and stones, accountants and lawyers/ notaries.

ii. **Country or geographic risk factors**: These may arise because of RPs business location and location of its branch offices together with its customer's geographic presence and jurisdiction in which the customer is operating. The factors that may indicate a high risk are as follow:
(a) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports by international bodies such as the FATF, as not having adequate AML/CFT systems.
(b) Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
(c) Countries identified by credible sources as having significant levels of corruption or other criminal activity.
(d) Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.
(e) Jurisdictions in which the customer and beneficial owner are based;
(f) Jurisdictions that are the customer's and beneficial owner's main places of business.

iii. **Product, service, transaction or delivery channel risk factors**: A comprehensive ML/TF/PF risk assessment must take into account the potential risks arising from the products, services, and transactions that the RP offers to its customers and the way these products and services are delivered. In identifying the risks of products, services, and transactions, the following factors should be considered:
(a) Anonymous transactions (which may include cash).
(b) Non-face-to-face business relationships or transactions.
(c) Payments received from unknown or un-associated third parties.
(d) Products with a surrender value.
(e) International transactions, or transactions involving high volumes of currency (or currency equivalent) transactions
(f) New or innovative products or services that are not provided directly by the RP, but are provided through channels of the institution;
(g) Products that involve large payment hor receipt in cash; and
(h) One-off transactions.
(i) Complex transactions that involves multiple parties or multiple jurisdictions.
(j) Any introducers or intermediaries the RP might use and the nature of their relationship with the RP.
(l) Physical presence of the customer for identification purposes. If they are not present, has the RP used a reliable form of non-face-to-face CDD (Has it taken steps to prevent impersonation or identity fraud).
(m) The customer being introduced by another part of the same financial group and to what extent can the RP rely on this introduction as reassurance that the customer will not expose the firm to excessive ML/TF/PF risk (what has the RP done to satisfy itself that the group entity applies CDD measures).

iv. **Risk Analysis**

In assessing the risk of ML/TF/PF, RPs are to establish whether all identified categories of risks pose a low, medium, high or unacceptable risk to the business operations. The RPs must review different factors, e.g., number and scope of transactions, geographical location, and nature of the business relationship. In doing so, the RPs must also review the differences in the manner in which the RP establishes and maintains a business relationship with a customer (e.g., direct contact or non-face-to-face). It is due to the combination of these factors and the variety of their combinations, that the level of money laundering and terrorism financing differs from institution to institution. The geographical risk should be seen in correlation with other risk factors in order to come up with an assessment of the total money laundering and terrorism financing risk. Thus, for example, a low-risk product in combination with a customer from a high-risk country will present a higher risk.

v. **Risk Management**

MSK has the appropriate policies, procedures and controls that enable them to manage and mitigate effectively the inherent risks that they have identified, including risks identified in the latest National Risk Assessment. MSK will continuously monitor the implementation of the controls and enhance them, if necessary. The policies, controls and procedures approved by the board of directors and senior management, and the measures taken to manage and mitigate the risks are consistent with legal and regulatory requirements.

Annexure 1: ML/TF Warning Signs/Red Flags

The following are some of the warning signs or "red flags" to which MSK should be alerted. The list is not exhaustive, but includes the following:

Brokerage Houses

(1) Customers who are unknown to the broker and verification of identity / incorporation proves difficult;
(2) Customers who wish to deal on a large scale but are completely unknown to the broker;
(3) Customers who wish to invest or settle using cash;
(4) Customers who use a cheque that has been drawn on an account other than their own;
(5) Customers who change the settlement details at the last moment;
(6) Customers who insist on entering into financial commitments that appear to be considerably beyond their means;
(7) Customers who accept relatively uneconomic terms, when with a little effort they could have a much better deal;
(8) 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);
(9) Customers who refuse to explain why they wish to make an investment that has no obvious purpose;
(10) Customers who are introduced by an overseas agent based in a country noted for drug trafficking or distribution
(11) Customer trades frequently, selling at a loss
(12) Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments;
(13) 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;
(14) Any transaction involving an undisclosed party;
(15) transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral;
(16) Significant variation in the pattern of investment without reasonable or acceptable explanation
(17) Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting thresholds.
(18) Transactions involve penny/microcap stocks.
(19) 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.
(20) Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
(21) Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.
(22) Customer invests in securities suddenly in large volumes, deviating from previous transactional activity.
(23) Customer conducts mirror trades.

Annexure 2: Proliferation Financing Warning Signs/Red Alerts

Following circumstances where customers and transactions are more vulnerable to be involved in proliferation financing activities relating to both DPRK and Iran sanctions regimes:

(a) customers and transactions associated with countries subject to sanctions;

(b) instruments that could particularly be used to finance prohibited transactions, such as certain trade financing products and services;

(c) customers involved with and/or transactions related to items, materials, equipment, goods and technology prohibited by UNSCRs;

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

(a) significant withdrawals or deposits of bulk cash that could potentially be used to evade targeted financial sanctions and activity-based financial prohibitions;

(b) opening of banking accounts by DPRK diplomatic personnel, who have been limited to one account each under relevant UNSCRs (including number of bank accounts being held, holding of joint accounts with their family members);