



**SUPREME SECURITIES LIMITED
REGD. OFFICE: 3rd FLOOR
R D CHAMBERS, 16/11, ARYA SAMAJ ROAD
KAROL BAGH
NEW DELHI-110005**

POLICY FRAMEWORK AND GUIDELINES ON
KNOW YOUR CUSTOMER AND ANTI MONEY LAUNDERING AND
COMBATING THE FINANCING OF TERRORISM MEASURES FOR MONEY
TRANSFER SERVICE SCHEME

| | |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Name & Designation of the Principal Officer | Mr. Rishi Tomar |
| Tel No / Cell No | 011-28755841/7838171778 |
| E Mail Id | rishitomar@supremesecurities.com |
| Office Address | Supreme Securities Limited Regd Office :3rd floor R D chambers 16/11,Arya Samaj Road Karol Bagh New Delhi-110005 |

Regulatory Reference: RBI Circular No 18 (A.P DIR Series) dated November 27, 2009

| S NO | Contents | Page No |
|------|-----------------------------------------------------------|---------|
| 1 | Company Policy Statement | 1 |
| 2 | Money Laundering - Introduction | 2 |
| 3 | Money Laundering - Process | 3 |
| 4 | Objectives of KYC/AML/CFT Guidelines | 4 |
| 5 | Customer Data Confidentiality/Security/Integrity | 5 |
| 6 | KYC Policy - Customer Identification | 5 |
| 7 | Customer Acceptance Policy | 6 |
| 8 | Customer Profile | 7 |
| 9 | Risk Categorization | 7 |
| 10 | Customer Identification Procedures | 8 |
| 11 | Documents Requirements from Customer | 9 |
| 12 | Customer Identification Requirements | 10 |
| 13 | Monitoring of Transaction | 10 |
| 14 | Risk Management | 11 |
| 15 | Principal Officer | 13 |
| 16 | Maintenance/Preservation of Records of transactions | 14 |
| 17 | Cash and Suspicious Transactions Reports | 16 |
| 18 | Red Flag Indicators | 17 |
| 19 | Types of Frauds | 18 |
| 20 | Reporting to Financial Intelligence Unit-India (FIU-IND) | 20 |
| 21 | Fraud Detection Guidelines | 21 |
| 22 | Customer Education/Employee's Training/Hiring | 23 |

Company Policy Statement

All Authorized Persons (APs) authorized under Section 10 (1) of the Foreign Exchange Management Act 1999 , have been brought under the purview of the act , Rules and Regulations.

Supreme Securities Limited being an Authorized person and an Indian Agent for Cross border inward Remittance under Money Transfer Service (MTS) Scheme duly licensed by the Reserve Bank Of India under the Foreign Exchange Management Act 1999 is fully committed to comply with the Know Your Customer (KYC) norms , Anti Money Laundering (AML) standards , Combating the financing of Terrorism (CFT) and obligation of the Authorized person as directed by the Reserve Bank Of India (the RBI) OR any other person / competent authority under the Prevention of Money Laundering Act (PMLA) ,2002 as amended by the Prevention of Money Laundering Act ,2009 , and the Prevention of Money Laundering (Maintenance of Records of the nature and value of the transaction, the procedure and manner of maintaining and time for furnishing information and verification and maintenance of the identity of Clients of the banking companies /* financial institutions) Rules 2005 , and all other rules , regulations , notifications and Circulars issued by the Government of India from time to time in that behalf in respect of cross border inward remittance under Money Transfer Service Scheme (MTSS)

The Company will support and encourage its Employees, business Partners and Customers to achieve the highest standards of Compliance integrity.

This Policy document will provide all the employees, business Partners and Customers of the company, a fair and reasonable understanding of KYC norms, AML Standards and CFT measures.

MONEY LAUNDERING

(A) INTRODUCTION

Money laundering is the Process of taking the proceeds of Criminal activity and making them appear legal. It is the process of concealing the source of obtained money.

OR, it may be defined as Clearing of the dirty money obtained from legitimate or illegitimate activities, including drugs trafficking, terrorism, fraud and other criminal activities with the objective of hiding its original source.

Money laundering is a major threat to financial institutions and the economic stability of the entire Country .Governments worldwide have introduced legislation to prevent it ,including specific money laundering offences and legally imposed requirements on institutions operating in their jurisdictions.

Section 3 of the Act defines the term offences of Money Laundering as Under:

“Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property, shall be guilty of offence of laundering.

Supreme Securities Limited consider it as its moral , social and economic responsibility to prevent the misuse of its financial system for laundering proceeds of criminal activities and to Co-ordinate the global war against the Money Laundering .

(B) MONEY LAUNDERING – PROCESS

Money laundering consists of three steps:

PLACEMENT

Placement is the depositing of funds in the financial institutions or the physical immersion of criminally derived funds into the financial system.

LAYERING

Layering involves carrying out complex financial transactions in order to camouflage the illegal source. The purpose of layering is to disassociate the illegal monies from the source and perpetrator of the crime by purposely creating a complex web of financial transactions aimed at concealing any audit trail.

INTEGRATION

Integration is finally acquiring wealth, generated from the transactions of the illicit funds. It is the stage where the money is integrated into the legitimate economic and financial system and is assimilated with all the other assets in the system.

(C) Objectives ,Scope and Application of the Policy of KYC / AML / CFT GUIDELINES

Anti-Money laundering and compliance regulations are the primary weapons used to prevent the system of cross border Inward Remittance under Money Transfer Service Scheme, from being used intentionally or unintentionally, by criminal elements for money laundering, terrorist financing, drugs and other illegal activities.

KYC procedures also enable Authorized Persons who are Indian Agents under MTSS to know / understand their customers and their financial dealings better, which in turn help them manage their risk prudently.

Purposes proposed to be served by the Policy are:

- (i) To prevent criminal elements from using our branches and sub-agents for money laundering activities
- (ii) To enable the branches and sub-agents to know/understand the customers and their financial dealings better which, in turn, would help to manage risks prudently
- (iii) To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures
- (iv) To comply with applicable laws and regulatory guidelines.
- (v) To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures.
- (vi) To develop and implement an effective AML ,CFT and anti-fraud compliance program in the network

This Policy is applicable to all branches/offices and sub-agents of Supreme Securities Limited and is to be read in conjunction with related operational guidelines issued from time to time.

DEFINITION OF CUSTOMER

For the purpose of KYC policy a customer is identified as :

a person who receives occasional / regular transactions

one on whose behalf the transaction is made (i.e. the beneficial owner)

an entity that has a business relationships with Authorized person

GUIDELINES

(1) Customer's Data security/ Integrity/ Confidentiality

The information collected from the customers while making payment of cross border inward remittances is to be treated as confidential. No information can be released to the third person without written direction i.e. court order or an order from Government authority.

Enough safeguards should be there in system to ensure that personal information is protected to prevent unauthorized access & use.

(2) KNOW YOUR CUSTOMER (KYC) POLICY –IDENTIFICATION OF CUSTOMER

The KYC policy sets standards to be adopted by the company to comply with the requirements of the rules and regulations. It includes following four key elements.

- A. Customer Acceptance Policy
- B. Customer Identification Procedures
- C. Monitoring of transactions
- D. Risk Management

Customer Acceptance Policy (CAP)

- (a) Company will develop a clear customer Acceptance policy laying down explicit criteria for acceptance of customers i.e.
 - i) No transactions should be received in anonymous or fictitious / benami names.
 - ii) based on risk perception ,parameters are clearly defined in terms of the nature of business Activity, location of customer, volume of turnover can be categorized in three categories1). Low level 2). Medium level 3). High level. Politically exposed persons can be categorized even higher.

(iii)

DOCUMENTATION requirements and other information's to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of Prevention of Money Laundering Act (PMLA) 2002 as amended by PMLA act 2009.

(iv)

PROHIBITION on making payments of any remittance where the company is unable to apply Customer due diligence measures i.e. unable to verify the identity and/or obtain documents required as per the risk categorization due to non-Cooperation of the customer or non-reliability of the data/information furnished to the company.

(v)

Identification of beneficial owner

Circumstances in which a customer is permitted to act on behalf of another person/entity should be clearly spelt out, the beneficial owner should be identified and all reasonable steps should be taken to verify his identity.

(b) Customer Profile

Based on the business relationship the company shall prepare the profile for each customer containing the information i.e Customer name, Address, social & financial status, nature of business activity.

The customer profile is a confidential document and should not be divulged for cross selling or any other purposes.

(C) RISK CATEGORISATION

Based on Risk perceptions the customer can be categorized in three categories :

1.

Low Risk Customer includes Customers whose financial and social status is known to the company, and is satisfactory, whose wealth can be easily identified

2.

Medium Risk Customers : Customers not falling in low or High Risk category .

3.

High Risk Customers Includes NRI's , Politically Exposed persons ,Foreign Nationals , high net worth individuals , trusts , charities and NGO's receiving donations , customers from countries that do not apply the **FATF** standards i.e. Iran , Democratic Republic of Korea, Myanmar

However the company should keep in mind that the adoption of customer acceptance policy and its implementation should not become too restrictive and must not result in denial of Cross Border Inward Remittance under Money Transfer Service Scheme to general public.

Customer Identification Procedures (CIP)

Customer identification means identifying the Customer and verifying his/her identity by using reliable, independent source documents, data or information. For customers that are legal persons or entities the company should verify the legal status of the person through proper and relevant documents, verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person.

In some typical cases, the company may however frame its own internal guidelines based on their experience of dealing with such customers. Some close relatives e.g. Wife/son/daughter/parents who live with their husband/father/mother and son ,as the case may be , may find it difficult to get the amount as the utility bill required for address verification are not in their name. In such cases company along with accepting Identity document of the customer may accept the address proof of the relative with whom the customer is staying along with the declaration from the relative that the said person wish to undertake the transaction is a relative and is staying with him/her.

Sufficient documents and due diligence should be done to verify the identity and the address /location of the customers.

Documentary Requirements from Customers

1.

Following identification should be verified and a copy should be retained while making payment to the customers:

| | |
|---------------------------|-------------------------------------------------------------------------------|
| Identity Proof | Valid Passport Aadhar Id Voter's Identity Card Valid Driving License |
| Correct Permanent Address | Telephone Bill Bank Account Statement Electricity Bill Ration Card |

2. A cap of USD 2500 has been placed on individual remittances under the scheme.
3. Amount up to Rs 50,000/- may be paid in cash . Any Amount exceeding the limit shall be paid only by means of A/C Payee Cheque / DD / or credited directly into the beneficiary's bank account.
4. However in exceptional cases, where the beneficiary is a foreign tourist, higher amount may be disbursed in cash.
5. Only 30 remittances can be received by a single individual during a calendar year.
6. No Commercial transactions, donations to charitable institutions are allowed under MTSS.
7. PAN Id / Form 60 and a recent customer photograph should be taken along with other OVD
8. Redaction of first 8 digits of Aadhar Number should be done where Aadhar Id is taken as a proof of KYC from the customer

Customer Identification Requirements

i) Transaction by Politically Exposed Persons (PEP's)

Politically exposed persons are those individuals who are or have been entrusted with prominent public functions in a foreign country e.g. Heads of States or of Governments , Senior Politician , Senior Government/Judicial/Military officers, Senior Executives of State –owned corporations .Sufficient information should be collected on any person of this category intending to undertake the transaction. The company should verify the identity of such person and try to ascertain the source of funds. Enhanced monitoring is required in all such cases.

Monitoring Of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. Company should have an understanding of the normal and reasonable activity of the customer to control and reduce the risk of such transactions that fall outside the regular pattern of activity.

Company to pay special attention to all complex, unusually large transactions, and all unusual patterns which have no apparent economic or visible lawful purpose . Company to set key indicators for such transactions ,taking note of the background of customers , such as country of origin , sources of funds , the types of transaction involved and other risk factors. Company to carry out periodically review of risk categorization of customers.

Transaction monitoring is done on regular basis and proper Records of the monitoring done are maintained.

Attempted Transactions

Transaction should not be undertaken in the Cases where company is unable to apply appropriate KYC measures due to non-furnishing of information and/or non-Cooperation by the customer. In such cases a Suspicious transaction report should be made and reported to FIU-IND (Financial Intelligence Unit- India) ,even if the transaction is not put through.

Risk Management

- a) The Company shall ensure that an effective KYC programme is put in place by establishing appropriate procedures and also ensure effective implementation of the same.
- b) The internal audit and compliance functions of the company play important role in evaluating and ensuring adherence to the KYC policies and procedures. The Concurrent auditors should check all MTSS transactions to verify that they have been undertaken in compliance with the anti money laundering guidelines. In case of any non-compliance the matter should be reported to the management. A certificate from the statutory Auditors on the compliance with KYC / AML / CFT guidelines should be obtained and kept on record.

Introduction of New Technologies

The Company will endeavour to pay special attention to any money laundering threats that may arise from new or developing technologies that might favor anonymity and take proper measures.

Combating Financing of Terrorism

The Company should develop suitable system or automated alert generated system for enhanced monitoring of suspicious transactions and report the same to the Financial Intelligence Unit-India (FIU-IND) on priority.

Special attention is to be given on the risks arising from the deficiencies in AML /CFT regime of certain jurisdictions viz. Iran, Democratic People's Republic of Korea, Myanmar as identified in the **FATF** statement issued from time to time, while dealing with individuals or businesses from these jurisdiction.

Sub Agents Management

The Company has been appointing sub-agents strictly in compliance with the guidelines of RBI. Since the KYC/AML/CFT guidelines are also applicable to the sub-agents, we have put in place a system of periodical audit of sub agents.

RBI has issued guidelines for MTSS business which includes guidelines for appointment, audit and furnishing of certain information/documentation etc on sub agents. The guidelines are strictly followed during the MTSS Agent appointment process.

Due diligence of the sub agent is conducted prior to their appointment which includes following checks:

Owners name, Complete address, Date of birth, Country of birth, Identification Number etc., provide Mtss guidelines, Training of the sub agent.

Due diligence of the location and Compliance review is conducted once in a year which includes review of the Mtss transaction done ,physical verification of the location ,KYC check by the Compliance team to analyse the adherence of the sub agent of Compliance policies and procedures, training of the sub agent. Records are maintained for all the process .

Regular updates on MTSS guidelines are communicated to the sub agents through the branches.

Sub Agent Duties/Obligations

Mtss Sub Agents are appointed strictly in compliance with the guidelines of RBI . It is the duty of the Sub agent to conduct Mtss business strictly in accordance with the Mtss guidelines and RBI Regulations. For each Mtss transaction conducted complete KYC should be done. The Mtss records should be available with the Sub Agent in case of audit/Inspection done by the Overseas Principal's/ Main Agent or by the Regulators. No Service should be offered from unauthorized locations/premises.

The Front Line Associates (FLA) must be trained periodically with the latest amendments/updation in the guideline. An acknowledgment of the Training sheet with the staff's signature should be maintained as a record. Only suitably trained employees should be permitted to perform the Money Transfer Service.

The Sub agent is required to maintain the Mtss records for the period of 5 years from the date of Mtss transactions done. The confidentiality of the Mtss records/KYC should be maintained and information cannot be released to a third party or to anybody. The Sub Agent can not release any customer information without written direction such as court order or from a government authority.

Sanctions Compliance

Supreme Securities Limited Anti-Money Laundering (AML) Sanctions Compliance Policy, as set forth in the Supreme Securities Limited Code of Conduct, to full compliance with all applicable laws and regulations. Based on assessed inherent risks, Supreme Securities Limited has implemented and administers the Policy to ensure that Supreme Securities Limited conducts its business in compliance with these laws and regulations. The company requires all its employees Sub Agents that act on its behalf to adhere to the Policy to effectively:

- Prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities;
- Ensure that it does not engage in any business in any sanctioned countries or with any blocked individuals/entities on applicable regulatory sanctions list including OFAC's; and
- Report violations and suspicious activities to applicable regulatory and law enforcement agencies, as required by laws and regulations.

Principal Officer

The Company has appointed a senior management officer designated as 'Principal Officer' located at head/corporate office of the company and shall be responsible for monitoring, reporting , prevention and identification of all transactions and sharing of information as required under law. Principal officer will also be responsible for developing appropriate compliance management arrangements across the full range of AML/CFT areas (e.g CDD ,record keeping).He will maintain close liaison with enforcement agencies, company , and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

Principal Officer responsibility also includes Employees/Agent training on Mtss guidelines and fraud and RBI rules and regulations to prevent conduct of any fraudulent activity/ transaction in the network and to suspend/terminate any such locations which are found conducting fraud/suspicious transactions.

To enable the Principal Officer to discharge his responsibilities, it is advised that the Principal Officer and other appropriate staff should have timely access to customer identification data, CDD information, transaction records and other relevant information. AML system should be installed for monitoring of the Mtss transactions.

Further the company should ensure that the Principal Officer should work independently and report directly to the senior management.

The Principal Officer will be responsible for timely submission of CTR and STR to the FIU-IND.

INDEPENDENT REVIEW

An independent review ensures that the SSL AML/CFT Compliance and Anti Fraud Program is effective and adequate for the money services products provided. The independent review will be conducted by either a legal professional or other trained AML/ CFT consultant. As the Compliance Officer cannot conduct this review, It is important that the independent reviewer accurately tests AML/CFT Compliance and Anti Fraud Program of Principal Officer for its ability to detect, prevent, deter and report suspicious activity and the unique risks that may be present at the locations . The review must be completed on an annual basis and a report detailing the findings must be issued by the auditor. This report will be presented to the board during its regular meetings. After the independent review, if there are corrective actions required, it is the duty of the Principal Officer to complete these required items, document the outcome of the corrective action and retain the completed checklist in accordance with the policies and procedures. In certain jurisdictions, the Independent Review may be conducted by the regulator.

Maintenance of records of transactions/Information to be preserved/Maintenance and preservation of records/cash and suspicious transactions Reporting to Financial Intelligence Unit –India (FIU-IND)

i) Maintenance records of the transactions

The company to introduce a system of maintaining proper record of the transactions as mentioned below –

- a) all cash transactions of the value of more than Rupees Ten lakhs or its equivalent in foreign currency.
- b) All series of cash transactions integrally connected to each other which have been valued below Rupees Ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and aggregate value of such transactions exceed rupees ten lakhs.
- c) All suspicious transactions whether or not made in cash and by way of as mentioned in the rules.

ii) Preservation of Information

The company to maintain the following information in respect of the transactions –

- a) the nature of the transactions
- b) the amount of the transaction and the currency in which it was denominated
- c) the date on which the transaction was conducted
- d) the parties to the transaction

Maintenance and Preservation of Records

- a) the company to take appropriate steps to develop a system for proper maintenance and preservation of transaction information in a manner for easy and quick retrieval of data whenever required or requested by the competent authorities. The company should maintain the records for the period of five years from the date of the transaction between company and the customer .
- b) the company will ensure that records pertaining to the identification of the customer and his/her address (e.g. copies of documents like Passport, Voter Id, driving license, Pan card) obtained while undertaking the transactions are properly preserved for the period of five years from the date of cessation of the transaction and should be made available to the competent authorities on request.
- c) For monitoring of transaction the company will pay special attention to all complex , unusual large transactions and all such transactions which have no apparent economic or lawful purpose. The background of these transactions should be examined and finding at the branch aswell as Principal Officer's level should be properly recorded. These records are required to be preserved for the period of five years.

Sub Agent Identification Records

The Company will establish policies and procedures to collect and maintain the records regarding the identities of the Sub Agent using reliable, independent source documents and in line with the RBI KYC Policy .The Company will maintain records for its sub agents and make those records available to Regulators / Overseas Agent, subject to local legal prohibitions or restrictions. The company will also ensure that an sub agent does not have a family relationship with an Owner/Proprietor or Associate who has been suspended/terminated due to fraud .

Cash and Suspicious Transactions Reports

Cash Transaction Report (CTR)

- i) The cash transaction report (CTR) to be submitted to the FIU-Ind by the due date as mandate by regulations.
- ii) While filing CTR, details of individual transactions below Rs 50000/- need not be furnished
- iii) CTR should contain the transactions carried out by the company on behalf of its customers
- iv) A cash transaction report as a whole to be compiled by the Principal Officer of the Company every month in physical form as per the format specified.

Suspicious Transaction Report (STR)

Suspicious transactions involve funds derived from illegal activities. Suspicious transaction report (STR) will be furnished within the period mandated by regulations upon arriving at a conclusion that any transactions are of suspicious nature. Such report should be made available to the competent authorities on request.

Red Flag Indicators or Indicators for Suspicious transactions

Following are the Red flag Indicators to keep a check on suspicious transactions

Customer makes enquiry about the Kyc requirement

Unrelated Transactions (Receiver-Sender seem to be not related)

Customer is hurried and nervous

Customer Id is not clear or is tampered

Customer is accompanied by unrelated Individuals

Customer makes inquiries or tries to convince staff to avoid reporting

Single Receiver receiving money from multiple Senders

Multiple Receivers receiving money from Single Sender

Receiver is receiving transactions just below Rs 50000/- to avoid any bank entry

Receiver presents multiple Id's to receive transactions

Transactions originating from High Risk countries

Customer could not explain the source of funds satisfactorily

The amount or frequency of the transaction does not make sense for the particular customer

Any Individual approaching the location with photocopy of the Id and not original one.

Types of Frauds

Following are the types of ongoing frauds and Supreme Securities Ltd has effective AML software to monitor such fraud activities, has taken a stand against Scams and educate its own Employees and Agent network regularly on frauds.

Employment Fraud

Customers are tricked into believing that they have found their dream job working part time from home and are asked to send the processing fee through money transfer service.

Loans and Investment Scams

A customer tries to get a loan or invest money to get the high returns is unaware that the company they have contacted is Fraud. The customers are told to send the money through money transfer service to pay processing fee.

Person In need Scams

Individuals are told to send the money to any unknown person who poses himself as a distant friend or Relative, through money transfer service.

Internet Purchase Scams

Customers believe they are purchasing an item from a company /seller on the internet. The customer purchases an item on the internet and is told to make the payment through money transfer service. The fraud company receives the money but no items are received by the customer.

Lottery Scams

Individuals receive E-mails that they have won a lottery prize even though they have not purchased a ticket for the lottery .Victims are notified by e-mail that their e-mail address is selected as the winner of the lottery .In order to receive the winnings the customer must send money to pay fees for processing ,insurance ,customs ,etc

Romance Scams

There are various forms of Romance Scams known as on-line dating, Social networking and mail bride services. All of these scams involve tricking the customer into providing funds to a person the customer believes he/she has a relationship with.

Fraud Transactions

Individuals approaching the locations for payout of the fraud transactions .Such person carry Fake Id's or photocopy of the Id's which are altered with false information on it.Locations which payout such transactions are at risk and are subject to termination of their agency as well as legal action against them.

Reporting of transactions

All branch staff are provided training on the Mtss guidelines and are briefed on the reporting of the transactions of the suspicious /fraudulent nature to the Compliance officer.

All Sub Agents are briefed on monitoring of suspicious transactions / Fraudulent activities and to report to their respective mapped branches in case any such transaction is noticed .

Red flag indicators to analyse the suspicious transactions are available in the Policy document. On the basis of Red flag Indicators the staff/Sub agent can do the transaction analysis and report the suspicious transaction.

On the basis of the branch staff reports MLRO analyse the transaction and report it to Financial Intelligence Unit of India – FIU-IND .

In case of any fraudulent activity /transaction the same should be reported to the Overseas Principal .

Supreme Securities Limited prohibits the use of any of its Overseas Principal's IMT products, services, and systems to be used for payment by sellers or telemarketers. In case the employees / sub agents / FLA's suspects that the consumer / the receiver of funds might be a telemarketer, transaction is not processed and is reported to the mapped Branch staff and then onward to the Principal officer who in turn report the same to respective Overseas Principal's compliance for appropriate action.

Reporting to Financial Intelligence Unit-India (FIU-IND)

In terms of the PML Rules ,the company should submit the Cash Transaction Report (CTR) for each month by 15th of the succeeding month and Suspicious Transactions Report (STR) within 7 days of arriving at a conclusion that any transaction ,whether cash or non-cash or a series of transactions integrally connected are of a suspicious nature to Financial Intelligence Unit – India (FIU – IND)

Website: <http://fiuindia.gov.in>

Fraud detection guidelines

CONSUMER FRAUD

You should understand & recognise what consumer fraud is & take precautions to prevent our customers becoming victims of it.

Consumer fraud is the potential or actual theft of funds from a consumer by means of; Deceit, Trickery or Manipulation

Signs to detect fraud are:

- ☒ There is no apparent family connection between the sender & receiver
- ☒ Customer is sending money to a person they have not actually met, to pay for travel
- ☒ One receiver is using different IDs
- ☒ Customer has forged or false IDs
- ☒ One receiver picking up multiple transactions from many senders

If you are suspicious of the transaction, ask questions. If you have reason to believe the customer is a victim/organizer of fraud - DO NOT process the transaction.

How do you identify Receive side consumer fraud?

For every victim of consumer fraud, there is an individual on the receive side of the transaction, picking up the money fraudulently...

- ☒ An individual repeatedly picks up transactions from multiple senders' in multiple locations
- ☒ An individual who attempts to pick up a transaction in a city other than where it was intended to be sent
- ☒ There does not appear to be a family connection between the receiver & the sender (different last names)
- ☒ There does not appear to be a business purpose for the transaction
- ☒ There are so many senders that it seems unlikely that the receiver actually knows that number of people

Some Key Points to Respond to Consumer Fraud

- Know your customer
- Ask questions if you are suspicious about the activity
Advise the customer to never disclose any of the details of the transaction especially reference numbers to any third party
- DO NOT process the transaction if you believe that the customer may be a victim of consumer fraud or a Receiver of fraudulently acquired funds
- Reporting consumer fraud to your Principal Compliance Officer.

Consumer Protection

Customer can lodge their grievances/complaints on Supreme Securities Limited Centralised Customer care number 8447592904 . Our complaints handling procedure reflects commitment to valuing complaints. It seeks to resolve customer dissatisfaction as close as possible thorough, impartial and fair investigations of customer complaints

Customer Education / Employees training / Employee's Hiring / Recruitment

Customer Education

The company shall prepare specific literature/pamphlets etc., so as to educate the customer of the objectives of the KYC programme .The employees should be trained while dealing with the customers.

Employee Training

New Joinee Training – AML/CFT/ Anti Fraud training is given to all new staff / sub agents as part of onboarding training prior to commencement of processing transactions

Ongoing Training – The company should run Employee/Sub Agent training programme on a regular basis so that the staff/Sub Agent should be adequately trained and aware of the KYC policies and procedures related to prevention of money laundering and can differentiate between the genuine and the suspicious transaction.

Sufficient systematic assessment should be put in place by the company as an integral part of its recruitment/hiring process of personnel to ensure high standards.

The company to conduct suitable background checks on potential recruits prior to offering employment with the company to avoid any risk.

The company should run Employee training programme on a regular basis so that the staff should be adequately trained and aware of the KYC policies and procedures related to prevention of money laundering and can differentiate between the genuine and the suspicious transaction. All staff/ sub agents are required to complete periodic training to ensure they have complete and updated knowledge of the product as well as its procedure/rules & regulations .

The employees handling the business shall have full knowledge of the product as well as its procedure/rules & regulations. Necessary class room training besides theoretical training shall be provided to the employees at all levels. Necessary reading material in the form of Manuals of Instructions have been made available to the employees both in soft copy and hard copy form to enable them to read, understand and update their knowledge. Further, the employees shall be given refresher training from time to time so as to update them with the changes in the rules and regulations..

Updated Mtss guidelines should be communicated to all the employees on regular basis.

Hiring / Recruitments of Employees

Sufficient systematic assessment should be put in place by the company as an integral part of its recruitment/hiring process of personnel to ensure high standards.

The company to conduct suitable background checks on potential recruits prior to offering employment with the company to avoid any risk.