ANTI-MONEY LAUNDERING AND COMBATING FINANCING OF TERRORISM (AML / CFT) POLICY

1) POLICY STATEMENT

It is the policy of the Eastern Exchange Establishment (hereinafter called Company) to comply with the Qatar Central Bank AML/CFT regulations and other applicable laws. This policy forms an integral part of the Company's AML/CFT Program, which includes procedures and personnel responsible for complying with this policy and applicable laws.

2) OBJECTIVES

(i) The purpose of this policy is to enhance the Company's compliance with anti-money laundering laws and regulations, to assist law enforcement in combating illegal money laundering, and to minimize the risk of Company resources being used for improper purposes.

(ii) To ensure implementation of policies, procedures, system and controls for prevention, detection, control and report of money laundering and terrorist financing in accordance with FATF 40 + 9 recommendations on AML/CFT.

(iii) The company is under statutory obligation to follow Law 4 of 2010 on Anti Money Laundering and Combating the financing of Terrorism and provisions of these regulations.

(iv) To maintain, enhance and protect the company's credibility, integrity and reputation.

3) PRINCIPLES

(i) To ensure that the policies, procedures, systems and controls are adequately addressed.

(ii) To adopt a risk based approach.

(iii) To know our customers based on their risk profiles.

(iv) To ensure proper internal and external reporting of suspicious transactions.

(v) To ensure adequate screening procedure while appointing employees and provide appropriate training programme for all our employees on AML / CFT

(vi) To provide documentary evidence on compliance with the AML / CFT regulations.

4) **RISK BASED APPROACH**

While establishing a business relationship with a customer, our exchange company is considering the following 4 risk elements ;

- Customer Risk
- Product Risk
- Interface or Delivery Channel Risk
- Jurisdiction or Geographical Area Risk

Customer Risk :

The company is taking the following measures to minimize the customer risk.

- Ensure to assess and document the risks of money laundering, terrorist financing and other illicit activities by different type of customers such as Individuals, Legal entities (Companies, Partnership, Trusts, Nominees shareholders & Power of Attorney holders and Politically Exposed Persons etc.

- Ensure to obtain prior approval from the Management Committee before entertaining business relationship with non profit organizations or with customer's requiring enhanced customer due deligence measures.

- Ensure to obtain prior approval from the Management Committee before entering into business relationships with Politically Exposed Persons (PEP)

- Ensure enhanced customer due diligence and on going monitoring if the company suspects that a customer is

an individual, a charity, non profit organization, legal entity that is associated with, or involved in, terrorist acts, terrorist financing activities.

The above policy guidelines are being followed by the counter staff while performing their duties.

Product Risk :

- Our Company is offering various products/services to its customers by way of Bank to Bank Transfer (web based package), E-Money (Instant Cash payment facility), Issuing DDs for customer account etc., to various countries.

- The company has a system to assess and document the risks of money laundering, terrorist financing and other illicit activities posed by the products above mentioned that are offering to its customers.

- Policies, procedures, systems and controls are in place to address specific risks of ML, TF and other illicitly activities posed by different types of products offered by us (as an agent) to the customers.

- The company is not allowing any of its products which is fictitious, false or when no name or the customer is not identified.

- The company is having Correspondent Banking relationship with various FI / Banks in a Foreign Jurisdiction and before establishing the Correspondent Banking relationship, it has ensured the following;

1. Obtain all information on the respondent FI/Bank to understand the nature of its business, ownership structure and management.

2. Obtain all information on major business activities of the respondent and its location as well as the location of its parent branch office.

3. Assess the respondent FI's AML / CFT policies, procedures, systems and controls.

4. Obtained Management Committee Approval before establishing correspondent banking relationship.

- The company also considers the following aspects before establishing Business Relationship with the Foreign FI/Banks.

    1. The financial position of the respondent FI/Bank.

    2. Whether the respondent FI has been subject to any investigation, or civil or criminal proceedings relating to ML /FT.

    3. Whether the respondent FI is regulated and supervised by a regulatory or governmental authority equivalent to the authority in home jurisdiction.

    4. Suitable clause has been incorporated in the Agreement signed by both the parties that outlines the respective responsibilities and obligation of each institution in relation to money laundering detection and monitoring responsibilities.

5. Ensure not to establish or continue business relations with FIs/Banks which have not physical present or “mind Management” (Shell Banks)

6. Ensure to submit Suspicious Transaction Report (STR) to the FINANCIAL INFORMATION UNIT (FIU) in the event that we are approached by a shell bank or any institution that the FI has reason to suspect that it is a shell bank.

Wire Transfers :

Wire transfer for QR4000 or equivalent in foreign currencies at the relevant time, whether sent or received by the Exchange company, product risk shall not be applied under the following;

- When a transaction is carried out using a credit or debit card, when the card number accompanies all transfers flowing from the transactions and the card is not used as a payment system to effect money transfer.

- When a transfer is from one FI to another FI and the originator and recipient are both FI’s acting on their own behalf.

Outgoing Transfers :

While remitting funds, Company shall ensure obtaining all the following required details of the originator

- Name of the Originator
- Account number or reference number in the absence of an account.
- ID or Passport Number
- Address and
- Details of Beneficiary's Name, Account Number, Bank Details and purpose.

Incoming Transfers :

The company has effective system to compare the details of originator and beneficiary submitted by the customer with the system generated report. The company shall refuse to make payment to the beneficiary for the reason for not submitting the full details such as copy of ID, difference in the name of the receiver as per ID and incoming transfer.

Interface or delivery channel risk:

- The company has proper systems and controls to address specific risk of Money Laundering, Terrorist Financing and other illicit activities posed by the different types of interface and technological developments through which business relationships are started, conducted and maintained.

Jurisdiction Risk

The company will ensure that proper policies, procedures, system and controls are in place to address specific risk of ML, TF and other illicit activities posed by different jurisdictions.

5) POLICY, PROCEDURES SYSTEMS AND CONTROLS

(i) Customer due diligence measures and on going monitoring.

(ii) Detection of suspicious transactions.

(iii) Comply with the internal and external reporting obligations.

(iv) Record making and retention.

(v) To assess and document the risks of money laundering, terrorist financing and other illicit activities by different type of customers such as Individuals, Legal Entities, PEPs etc.

(vi) To obtain prior approval from the Management Committee before entertaining business relationship with non profit organizations or with a customers requiring enhanced CDD measures.

(vii) To obtain prior approval from the Management Committee before entering into business relationships with Politically Exposed Persons (PEP).

(viii) To evaluate all financial transactions and take all necessary steps to comply with anti-money laundering laws and regulations.

(ix) To ensure that all the employees are conversant with the requirements of AML / CFT Law and regulations.

6) KNOW YOUR CUSTOMER (KYC)

Objectives:

(i) To establish procedures to verify the bonafide identification of individuals.

(ii) Establish systems for conducting due diligence and reporting of such activities.

(iii) To establish process and procedures to monitor high value transactions and suspicious transactions.

The focus of KYC is 'back to back basics' where elaborate standard for obtaining detailed information regarding new customers at the initial stage and that of existing customers over a period of time would be achieved. This would help in establishing the genuineness and bonafides of customers and keeping a watch over transactions, particularly those of a suspicious nature, and reporting these to the FIU/law enforcers.

Customer Identification and Profile

(A) Accounts of Individuals:

Identification of clients or their representatives according to legal identification documents and registration of these identifications when entering with them in business relations, deals or presenting services including making financial remittance or other banking and financial works and services.

Example: National Identification Card, Passport, Driving License, Health Card etc.

As per the latest guidelines of QCB, Eastern Exchange undertakes to preserve such ID card details in the system for future reference if any.

(B) Other than Individual Accounts:

For any business dealing done by firms, companies etc, the company shall check for the existence of the client and its legal situation by documents establishing the establishment/company such as commercial registration, license from the government, memorandum and articles of association and what information it includes to understand the objectives of the client.

Check the authorization given to the person representing the company via ID details.

Obtain full information regarding the correct identity, origin and head quarters of the firm.

It shall also be ensured that KYC guidelines are made applicable to new and existing customers.

Customer Due Deligence :

- As an internal control measures for high value transactions any remittance exceeding Qr 50000, the counter staff has been advised to bring it to the notice of Manager / Officer so that the manager / officer can interact with the customer for obtaining a copy of Bank

Statement / Declaration / letter from the customer's sponsor.

- Company shall ensure real time transmission of remittance data to QCB through onling connectivity with particulars of ID of the remitter.

- Eastern Exchange Establishment ensures the prompt reporting of the suspicious transactions as enumerated by QCB and other regulatory authorities.

- Company shall have the inbuilt program in the operating system to enforce the counter staff and back office officials to input the needed details of the remitter as per QCB guidelines and the stipulations given by various correspondents.

- Company shall insist the counter staff to verify the identity of the remitter duly verifying the ID Card and also the person.

- Latest procedural guidelines like verification of the remitter even in the case of woman remitter shall be strictly adhered to by the Eastern Exchange Est.

- Company shall ensure Prompt submission of reply on suspicious transactions queries raised by the various governmental authorities like QCB, Financial Information Unit (FIU), CID etc.

- Company shall adhere to the AML guidelines of the agents like Western Union money transfer, xpress money transfer and Prabhu Money Transfer with whom the

company has got a tie up for providing money transfer services to various countries.

Transaction of suspicious nature :

For identification of suspicious transaction, Company shall take the precautions which would be exercised by a man of normal prudence.

It will be desirable to eliminate the possibility of accepting as customers, persons, institutions or parties where there may be reasonable apprehension that the transaction could be used for money laundering or other anti social activities. As a preventive and as a prudential measure the Company shall not allow transactions in the following circumstances :

- Where the customer's identification is not established to the satisfaction of the company;

- Where there is reasonably reliable information that the Prospective customer has a doubtful past;

- Accounts of terrorist individuals/organizations/persons related/connected to/with them.

7) THE IMPORTANCE OF KYC GUIDELINES TO EMPLOYEES

- The employees will conduct themselves in accordance with the highest ethical standards and in accordance with the extant regulatory requirements and laws. Staff should not provide advice or other assistance to individuals who are indulging in money laundering activities.

- Money laundering activities cover not only the criminals who try to launder their ill-gotten gains, but also the financial institutions and their employees who participate in those transactions and have knowledge that the property is criminally derived. “Knowledge” includes the concepts of “conscious avoidance of knowledge.

- Arrangements shall be made to ensure that correspondents advise the Bank of any local exchange control regulations and restrictions on international transfers. Similarly, it shall be ascertained whether correspondent bank themselves are regulated for money laundering prevention in their country and if so, whether the correspondent is required to identify their customers in comparable standards

- Beneficiary is an acceptable person (Natural or legal)

- Establishment of prima facie connection or locus standing between remitter and beneficiary.

- Purpose; the underlying transaction or motive behind the transaction is not illusory or vexatious. End use of funds with reference to beneficiary bears out well with documents produced and the status of remitter.

- Transaction is borne by complete set of documents or any other formality, Company requires the remitter to fulfill, is complied with without haphazardness or any haggling and irrational references.

- Pattern of the remittances commensurate to customer’s nature of business

8) PROCESS AND PROCEDURES TO MONITOR SUSPICIOUS TRANSACTIONS AND RESPONSIBILITY OF MONEY LAUNDERING REPORTING OFFICER (MLRO)

- An exclusive compliance officer has been employed at the management level having sufficient seniority, experience and authority to carry out his responsibilities independently.

- MLRO will report directly to the Management Committee.

- MLRO / Compliance Officer will be the key and focal person in implementing the company's AML/CFT strategies.

- Compliance officer will ensure that the company's wider responsibility for preventing money laundering and terrorist financing is addressed centrally.

- The main duty of the compliance officer / MLRO will be to receive, investigate and assess the internal suspicious transaction report of the company and making STRs to FIU wherever applicable.

- MLRO will act as central point of contact between the company, FIU, the Regulator(s), and State authorities in relation to AML and CFT issues.

- MLRO shall execute his duties and responsibilities honestly, reasonably and independently, particularly while receiving, investigating and assessing internal STRs and deciding whether to make a STR to FIU.

- External auditor shall be employed for ensuring the adequacy and the compliance of the policy and procedure framed for onward submission to QCB by the auditor

- Staff will record and report all transactions of suspicious nature in deposit and remittances accounts etc., with full details to the compliance officer / Manager.

- The company undertakes to report Suspicious Transactions or any such attempt by criminal elements to Financial Information Unit (FIU) under the provision of Article 14 & 18 of law of 2010.

The procedure followed shall be as under:

- It shall be a prudent practice to segregate after scrutiny, the large sized transactions and satisfy ourselves about such transactions. Accordingly, the threshold limits (wherever specified in the policy)would be put in place for all concerned departments to scrutinize such entries and to satisfy themselves about the genuineness of the same.

- On receipt of the internal reports from the officers or employees of the company, the MLRO should properly and appropriately document the report and acknowledge the same together with a reminder of the provisions relating to tipping off.

- Consider the internal report in the light of all other relevant information available with the FI and decide whether the transaction is suspicious and furnish a

notice to the officer or employee of the decision of the Money Laundering Reporting Officer.

- When the company has a reasonable ground to know or suspect that the funds are proceeds of criminal conduct, or related to Terrorist Financing or linked or related to, or are to be used for terrorism, terrorist act or by terrorist organization, Company is obligated to make a report to FIU.

- The company should immediately make a STR to FIU and ensure that any future or proposed transaction relating to the report does not proceed without consultation with FIU.

- In consultation with Solicitors to take up the matter with the appropriate law enforcing authorities designated under the relevant laws governing such activities.

- In case the name of any banned organization appears as Payee/endorsee/applicant, it shall be endeavor of the Company to ensure that the system must throw a caution. Reporting of such transactions as and when detected shall be as above.

- Company shall submit monthly statements to FIU for monitoring purposes or as and when it is demanded.

- Tipping off is prohibited under the provisions of Article 39 of Law (4) of 2010.

- Company shall ensure that its officers and employees are aware of and sensitive to the issue surrounding and consequences of tipping off.

- Company is taking all precautionary measures to ensure safeguarding information relating to internal Suspicious Transaction Report(STR).

- Company staff has been advised, not to disclose the internal STRs to any person, other than members of the Management Committee, without the consent and permission of the MLRO.

- The MRLO shall not accord permission or consent on disclosure of information relating to internal STR to any person, unless MLRO is satisfied that such disclosure would not constitute tipping off.

- The MRLO shall maintain a record for the consent given to disclose the information relating to internal STR.

9) RETENTION OF RECORDS:

- Records of remittance transactions for specified periods are required to be maintained.

- Company shall undertake to preserve at the end of business relationship with the customer, which in any case shall not be less than 15 years the hard copies of ID and other relevant papers in respect of transactions, which have been reported for suspicious activities.

- Regarding the transactions executed for customers who do not hold any account at the bank or financial institution (occasional customers), documents and records related to any transaction should be kept for a period of fifteen years at least from the date of executing the transaction.

- Reports made to government authorities concerning suspicious customer activity relating to possible money laundering or other criminal conduct together with supporting documentation should be kept for a period of fifteen years at least or until a judgment, in case of any judicial involvement or final decision is rendered with regard to the transaction, whichever is longer.

- Training records should be retained for a period of five years.

- Any other documents required to be retained under applicable money laundering laws/regulations.

- All financial transactions records are to be retained for at least 15 years after the transaction has taken place and are to be made available for scrutiny of Law enforcing agencies, Audit functionaries as well as Regulators, as and when required.

10) TRAINING

- Staff would undergo ongoing training programme on AML/CFT for strict implementation of KYC guidelines and AML measures.

- Training programme would envisage that the officers and employees of the company understand :

  (A) The legal and regulatory responsibilities and obligations under AML/CFT law and regulations.

  (B) Their role in preventing ML and TF and the liability devolving on Officers and employees and company due to their involvement in ML or TF and failure to comply with AML/CFT law and regulations.

11) DUTIES/RESPONSIBILITIES

The duties and responsibilities at branches are as under:

- Officer/Counter staff of the branch shall be vested with the authority to make relevant enquiries from the potential /existing customer

- To verify the introductory reference/customer profile.

- To exercise due diligence in identifying suspicious transactions.

- To ensure against initiating transaction in the name of terrorist/banned organizations.

- To comply with the guidelines issued by the Qatar Central Bank from time to time in respect of conduct of exchange business.

- Manager shall scrutinize and satisfy himself the information furnished by the customer are in strict compliance with KYC guidelines before authorizing the transaction.

- To certify regarding compliance with KYC guidelines and report suspicious transactions to FIU.

- Manager shall be vigilant in computerized and non-computerized transactions. He shall keep himself abreast of all latest developments in AML area in other organizations and countries and effect the changes in AML measures suitably to improve AML exercise of the Company. Maintain up-to-date list of high risk countries.

- Manager will also be instrumental in adhering to KYC principle and effective customer identification and should provide necessary guidance to operating staff. He shall arrange to conduct training for staff with latest course material on AML and case studies.

- Auditor will verify and record his comments on the effectiveness of measures taken by branches/level of implementation of KYC guidelines.

12) STAFF ACCOUNTABILITY WITH REGARD TO 'KNOW YOUR CUSTOMER' AND 'ANTI MONEY LAUNDERING':

- It is important to ensure that the guidelines/instructions laid down for 'Know Your Customer' and 'Anti Money Laundering' in this Policy is followed in letter and spirit. Therefore, the staff entrusted with this responsibility is

- In the event of any discrepancies or deviations observed it is important to ascertain the possible consequences thereof and set the position right within a short time frame and to avoid any adverse repercussions. At the same time it is also necessary to analyze such cases and to determine whether the same were caused by any shortcomings in the exercise of due diligence on the part of the Company's officials/staff. For the purpose the Manager Operation shall examine all such cases as he may consider appropriate and submit the same to Management Committee with his findings as to the causes, responsibility and consequences of the deficiencies or deviations which will turn examine the same, take a view and initiate such action as may be appropriate including with regard to staff accountability.

13) REPORTING

Any unusual or inconsistent transaction by a customers known legitimate business and risk profile, by itself does not make it a suspicious transaction. In this regard company shall consider the following:

(i) Whether the transaction has no apparent or visible economic or lawful purpose.

(ii) Whether the transaction has no reasonable explanation.

(iii) Whether the size and pattern of the transaction is not similar to the earlier pattern or size of same or similar customers.

(iv) Whether the customer has failed to furnish adequate explanation or information on the transaction.

(v) Whether the transaction is made from a newly established business relationship or is a one-off transaction.

(vi) Whether the transaction involves off-shore accounts, companies etc that are not supported by the economic needs of the customers.

(vii)Whether the transaction involves unnecessary routing of funds through third parties.

The list is only indicative and company may consider any other relevant issue to assess if the transaction is unusual or inconsistent.

Internal Reporting requirements:

1. Company shall have clear and effective policies, procedures, systems and controls for internal reporting of the known or suspected instances of ML & TF,

2. These policies, procedures, systems and controls for internal reporting should enable the company to comply with the AML/ CFT law, regulations and also enable prompt making of internal suspicious transactions report to the Money Laundering Reporting Officer.

3. The company shall ensure that all officers and employees

have direct access to the Company's Money Laundering Reporting Officer and also that the reporting hierarchy between the officers and employees are short.

4. All officers and employees of the company should make an internal STR to the Money Laundering Reporting Officer. On making such an internal STR to Money Laundering Reporting officer, the officer or employee should promptly report all subsequent transactions details of the customer until required by the Money Laundering Reporting Officer.

Obligation of Money Laundering Reporting Officer on receipt of internal reports:

1. On receipt of the internal reports from the officers or employees of company, Money Laundering Reporting Officer shall :

(a) properly and appropriately document the report

(b) furnish a written acknowledgement to the officer or employee, together with a reminder of the provisions relating to tipping off

(c) consider the internal report in the light of all other relevant information available with the company and decide whether the transaction is suspicious and furnish a notice to the officer or employee of the decision of the Money Laundering Reporting Officer.

External Reporting requirements:

1. Company shall have clear and effective policies, procedures, systems and controls for reporting all known

or suspected instances of ML of TF to FIU.

2. These policies and procedures of company should be able to comply with AML/ CFT law, regulations in relation to making STRs to FIU promptly and also to cooperate effectively with FIU and law enforcement agencies in relation to STRs made to FIU.

14) GENERAL GUIDELINES

- Any suspicious transactions observed shall not be disclosed to the clients.

- In such case the manager shall hold the money received in an intermediate account such as Sundry deposit

- After confirmation of the genuineness of the transaction the amount held in the sundry deposit shall be remitted to the beneficiary account/person.

- If the genuinety of the transaction cannot be established the same shall be reported to the FIU / QCB for further action by the appropriate authorities.

- Formats specified by the QFIU only shall be used for reporting suspicious transactions and shall be addressed to public department, banking affairs and issuance department at QCB.

- Special attention shall be given to transactions with financial companies and establishments operating from countries which do not implement stringent anti money laundering laws.

- Eastern Exchange shall review this policy from time to time incorporating the latest changes/developments as per the legislation of the Qatar regulators.

****

Annexure

SUSPICIOUS TRANSACTIONS

- Behaviour which to the eye of the observer appears to be unusual or out of context in the circumstances within which it is observed.

- Money launderers involve many types of transactions while disguising the dirty money and layering it. So it is difficult to define a suspicious transaction. However, it may be one that is inconsistent with a client's known business, profession or activity/trade he/she carries on. The key to detect such suspicious transactions is to knowing sufficiently about client to recognize that a transaction/or series of them is unusual.

- Availing exchange for business trips which is disproportionate to the duration of stay and not befitting the status of the business executive of the company.

- Cash being tendered for availing foreign exchange by corporate customers.

- Customers who receive various remittances frequently from centers abroad and make various remittances frequently abroad.

- Frequent visits to same destinations by a large number of officials who draw disproportionately high amount of exchange.

- Receipt of international remittances from services irrelevant to customer's business/profession or from

- Money activities of customers, which show sudden and disproportionate growth in volumes.

- Customer or his representative reluctant to give information relating to customer's activities.

- Customer's account exhibiting large deposits through tender of currency bearing the labels of other banks.

- A single cash deposit of substantial amount comprising of large component of high/low denomination notes.

- Unlimited applications/requests for drafts/pay orders against cash.

- Customers requiring exchange of small denominations of notes for larger denominations and vice versa.

- Several cash deposits/withdrawals below a specified threshold limit to avoid filing a report. These may be necessary in case of transactions above the threshold level, i.e. initial splitting of transactions.

- Individual/group that induces or attempts to induce the Company's employee/s to avoid filing reports/or any other forms.

- Request for wire transfers, out of country, financed by multiple banker's cheques (just below threshold limit).

- Customer receiving wire transfers and converting the balances in monetary instruments favoring third parties. The amount is very large, or just below the specified threshold limit decided by the legislation.

- Transactions are repeated.

- Risk based monitoring of transactions (Automatic/Manual) shall be undertaken and accordingly guidance will be provided to employees who interact with customers, carry out their instructions or effect transactions.

****